MEDIC

Medical Excellence. Compassionate Care.

EMPLOYEE HANDBOOK
Last updated February 1, 2023

Table of Contents

Welcome to the Medic Team!

Whether you join Medic with years of experience or are new to EMS, I want to clarify why we are here. Our purpose, simply stated, is to help people. The Agency exists to care for those in need without bias or prejudice.

I am thankful that you have chosen to join the Agency and work with us toward that goal. The enclosed materials are some of the work rules for all of us while we are here. If you have any questions about them, please contact the Human Resources Department.

Again, welcome, and I hope you enjoy working at Medic as we serve the public in this important work.

Sincerely,

John "JP" Peterson

John “JP” Peterson
Executive Director

Purpose and Introduction to Handbook

This Employee Handbook serves to inform and guide employees in regard to the overall purpose of the Mecklenburg EMS Agency, "the Agency". The Agency is an equal opportunity employer and does not discriminate against employees or applicants in promotion or employment. Positions are filled without regard to race, religion, sex, color, age, national origin, disability, or veteran status. **All employees are expected to read this handbook carefully, and are responsible for being familiar with this information. This handbook is intended to be used for reference only and does not constitute an agreement or contract of employment between the Mecklenburg EMS Agency and the employee.** After receipt of this information, employees will sign the Acknowledgement of Receipt form and return it to the Human Resources Department.

The Agency has prepared this manual to provide employees an overview of the Agency's policies, procedures and benefits. It is intended to familiarize employees with important information about the Agency, as well as information regarding their own privileges and responsibilities. Although it is not a contract or a legal document, it is important that all employees read, understand and follow the provisions of the manual as it may be amended from time to time by the Agency.

It is obviously not possible to anticipate every situation that may arise in the workplace or to provide information that answers every possible question. In addition, circumstances will undoubtedly require that policies, practices and benefits described in this manual change from time to time. Accordingly, the Agency must reserve the right to modify, supplement, rescind or revise any provision of this manual from time to time as it deems necessary or appropriate in its discretion. The Agency also reserves the right to refer to Mecklenburg County's policies and procedures if a specific policy does not exist.

The Agency is constantly striving to improve its policies, the services and products that it provides its customers, and positive relations with its employees. Employees should bring suggestions for improvements to the attention of their supervisors or Human Resources. By working together, the Agency hopes that it will share with its employees a sincere pride in the work place and the services that we are all here to provide.

Amendments, Revisions, and Review of the Employee Handbook

Purpose

To provide an orderly, expedient method for suggesting and issuing amendments to the Employee Handbook.

Policy

1. Suggestions for additions or revisions will be submitted in written form to the Director of Human Resources for review.

2. Amendments, deletions, or other revisions to the handbook will be published and will also be made available on electronic mail for all employees.

Chapter 1 - Employment

1.1 At Will Employment

Effective 1/1/99

Policy

All Agency employees who do not have a written individual employment contract for a specific, fixed term are classified as “at-will” employees. This means that employees may resign at any time, and the Agency may terminate employment at any time with or without notice for any reason or no reason.

1.2 Equal Employment Opportunity

Effective 1/1/99; Revised 2/1/2006; Revised 1/23/2013; Revised 01/01/2022

Purpose

To ensure equal employment opportunity for all Agency employees or applicants for employment.

Policy

Federal and state laws require that there be no discrimination against any employee or applicant for employment because of the individual's race, color, religion, sex, sexual orientation, gender identity or expression, national origin, age, disability status, genetic information, protected veteran status or any other characteristic protected by law with respect to hire, lay off or other terms, conditions, or privileges of employment.

The Agency supports equal employment opportunities for all persons and will apply the Agency's recruitment and employment policies and practices in a manner consistent with state and federal laws.

All employment decisions, including recruitment, selection, assignment, wage determination, classification, training, promotion, demotion, transfer, discipline, benefits, termination and other conditions of employment will be based upon non-discriminatory factors such as the individual's qualifications, merit and professional ability and will conform to all legal requirements.

The Agency will comply with the Americans with Disabilities Act (ADA) and ADA Amendments Act, which both prohibit discrimination on the basis of a disability. The Agency will not automatically exclude from employment individuals with certain medical conditions or disabilities and will, prior to making any employment decisions, consider whether (1) any reasonable accommodations are available to allow the applicant or employee to perform the essential functions of the position, and (2) seek an individualized medical assessment from an Agency appointed physician to determine if the particular applicant or employee would in fact pose a direct threat to the health and safety of him or herself or others.

If any employee has a suggestion, problem or complaint with regard to equal employment, he or she should contact the Human Resources Department. (See also Grievance Policy and Harassment/Sexual Harassment Policy).

1.3 Hiring Procedure
Revised 3/1/05

Summary Statement
The Agency will adhere to hiring practices consistent with local, state and federal regulations.

Applicability
All applicants of Mecklenburg EMS Agency.

Procedures
1. Human Resources will verify the position as an approved position and commence recruitment activity.
2. All applications and resumes on file will be considered for open positions and Human Resources will advertise positions as appropriate.
3. Interviews and/or assessment centers for the most qualified applicants will be conducted. Current job descriptions, performance standards and, when applicable, clinical requirements established by the medical director will be used to evaluate eligibility for employment.

Selection & Offer
1. After all qualified applicants have been interviewed, Human Resources will be notified.
2. Human Resources will complete a background check that may include references, criminal background search, OIG, DMV and any other verification required by the position before any offer of employment is made.
3. Human Resources will notify the Hiring Manager to contact the selected applicant to extend the conditional job offer, including compensation rate, and direction on contacting our Safety Team for a health assessment. Human Resources must receive a health assessment confirmation from the Safety Team before the selected applicant will be allowed to attend new employee orientation.
4. The Hiring Manager, in consult with Human Resources, will notify all applicants interviewed for a position of the final decision regarding their status.

1.4 Employee Introductory Period

Effective 1/1/99

Purpose

The Introductory period is intended to allow the employee and the Agency a period of time to determine if continued employment is in the best interest of both parties. This policy outlines the introductory period.

Policy

1. All new employees shall serve an introductory period at the Agency. The normal introductory period is ninety (90) days. However, this period may be extended due to extenuating circumstances, agreed upon by the Supervisor, Director of Human Resources and the employee.

2. An employee promoted or upgraded to a position with a new job description will also serve an introductory period. This introductory period will last at least ninety (90) days.

3. Employees serving an introductory period are not eligible for promotions or transfers.

4. The employee should receive a performance review prior to the end of the introductory period. This performance review will not include compensation.

    a. Introductory periods should not extend past 180 days.

    b. The introductory period does not guarantee employment for ninety (90) days or any other period of time.

1.5 Background, Reference and Sanction Checks
Effective 6/1/04

Procedure

1. The Agency will perform background checks (including criminal background checks), reference checks and checks against duly authorizing licensing, disciplining and sanctioning authorities on each individual who is a candidate for employment by Mecklenburg EMS Agency. Each individual seeking employment will be checked within 30 days of employment offer. Checks against duly authorizing licensing, disciplining and sanctioning authorities will include reviews at the federal and state level (including the Cumulative Sanction List of the Office of Inspector General) for any sanction, exclusion, debarment, lost of license or other conduct or performance based actions that might impact an individual's ability to perform his or her duties on behalf of the Agency and the patients it serves. The employment application for any position will include an attestation by the candidate relating to whether such candidate has been convicted of a crime or sanctioned by a duly authorized regulatory or enforcement agency of the government. The following language shall appear on all employment applications:

    a. Have you ever been convicted of any criminal violation of law, or are you now under pending investigation or charges of violation of criminal law? If yes, explain.

    b. Have you ever been the subject of any adverse action(s) by any duly authorized sanctioning or disciplinary agency for either conduct-based or performance based actions? If yes, explain.

2. Individuals who are charged with criminal offenses related to healthcare or who have been proposed for exclusion or debarment from any federally funded healthcare program will be removed from direct responsibility for or involvement in any federally funded healthcare program until final resolution of the criminal charges or proposed exclusion or debarment. If the resolution results in conviction, debarment or exclusion of the individual, employment of that individual shall be terminated. The Agency will evaluate any individual or entity that has been the subject of an adverse action for either misconduct or poor performance to determine if such misconduct or poor performance should preclude employment by, or a business relationship with, the Agency.

3. Human Resources will be responsible for making the appropriate agency checks for each candidate for employment in accordance with Section A of this policy to determine if any such individual has been the subject of any adverse action, exclusion, debarment or other sanction. Documentation of the agency check will be maintained properly in the individual's employment file. The Agency's Compliance Director and other administrative directors will take appropriate action regarding any individuals who are found to have been the subject of adverse actions by duly authorized sanction authorities.

4. The Agency's compliance director will ensure on-going sanction checks of all current employees and vendors are conducted at least every six months. All checks are made against the Cumulative Sanction List of the Office of Inspector General and the General Services Administration (GSA) Debarred List. Documentation of these semi-annual checks will be maintained by the compliance director. The Agency's compliance director and other administrative directors will take appropriate action regarding any individuals who are found to have been the subject of adverse actions by duly authorized sanction authorities.

5. It is the responsibility of the department manager who negotiates agreements with independent contractors who provide temporary personnel for either patient care or billing and coding services to the Agency to include the following language in any service agreement:

6. The Service Provider shall maintain and provide upon request to the Agency the following information for any personnel who will provide services for the Agency, prior to the date such personnel begins an assignment:

7. Report of criminal background check in each state where the individual has resided during last 7 years.

8. Report of SBI criminal background check for unlicensed personnel involved with patient care, maintenance and security.

9. Documentation that Office of Inspector General (OIG) Sanction and GSA Debarred List Verification has been completed.

10. All managers responsible for material management or accounts payables shall check all vendors that the Agency uses against the Federal Sanction (OIG) and Debarred List (GSA). They must also maintain documentation of such checks in their vendor files. Any vendor listed on either database must be reported to the compliance director immediately.

11. Annual corporate compliance audits will be conducted by the CHS Chief Compliance Officer, or his designee to verify (i) that appropriate pre-employment checks have been made; (ii) that appropriate semi-annual checks on existing employees and vendors have been made; (iii) that documentation of requested agency checks are available; and (iv) that appropriate actions are taken in cases where individuals are found to have been sanctioned or debarred.

1.6 Charges, Convictions or Sanctions
Effective 6/1/04

Mecklenburg EMS Agency shall be notified by its employees in the event of a criminal charge, conviction or sanction. It is the intent and purpose of this policy to ensure the safety of patients, employees and all other guests, as well as, to enhance and protect the property and reputation of the Agency.

Policy
Any employee who is charged with, or convicted of, a felony or any misdemeanor involving violence, injury to another person, communicating threats, destruction of property, sexual offenses, drug, DWI, theft or fraud including fraudulent checks, shall immediately report such charges or conviction to his/her supervisor.

Employees who drive Agency vehicles as a requirement of their position must report any moving violations or conviction involving a traffic violation where points are placed against their driving record and/or a conviction resulting in a suspension or revocation of their driving privilege.

As part of the annual performance appraisal, a signed attestation of compliance with this policy will be required of all employees.

Charges
Employees must report, in writing, any charge listed above to his/her supervisor the next work day after the charges are filed. Failure to report a charge will be grounds for disciplinary action up to and including termination.

Managers and supervisors who receive a notice of charge must report it to the Director of Human Resources in Human Resources within one (1) business day.

The department manager, in consultation with the Director of Human Resources, and other administrative directors, may issue a suspension for up to 30 days while the charge is being reviewed. Employees will not be paid for time away from work, but may use accrued vacation/holiday time.

Any charges dismissed or dropped, must be reported immediately to the department supervisor/manager.

Conviction
Employees convicted of a charge listed above or sanctioned by a federal or state agency must report the conviction or sanction in writing to his/her supervisor within five days of the occurrence. Failure to report a conviction or sanction will be grounds for termination of employment. Managers or supervisors who receive notice of a conviction or sanction must report it to the Director of Human Resources within one business day.

The department manager, in consultation with the Director of Human Resources, and other administrative directors, will determine if the employee's unlawful conduct is grounds for reassignment or disciplinary action up to and including termination.

In the event of a criminal conviction or federal agency debarment related to healthcare, employment will be terminated.

1.7 Non-Retribution / Non-Retaliation

Effective 12/1/99

Purpose

To promote ongoing, open communication and to encourage employees of the Agency to communicate and report problems, concerns and opinions without fear of retaliation or reprisal.

Policy

No employee of the Agency shall be disciplined solely on the basis that he or she reported what he or she reasonably believed to be an act of wrongdoing or a violation of the Compliance Plan.

Each supervisor shall take measures to assure his or her staff that the Agency truly encourages the reporting of problems and that an employee who makes a report based on his or her reasonable belief that a violation or wrongdoing has occurred or is occurring will not be disciplined as a result of making such report. It is critical that all employees of the Agency realize that retaliation or reprisal against an employee for raising/reporting a problem will not be tolerated.

Employees must also realize that disciplinary action will be taken if the Agency reasonably concludes that the employee's report of wrongdoing was knowingly fabricated by the employee or was knowingly distorted, exaggerated or minimized to either injure someone else or protect himself or herself. In determining what, if any, disciplinary action may be taken against an employee, the Agency will take into account an employee's own admission of wrongdoing.

1.8 Grievances

Effective 1/1/99

Purpose

This policy provides for the settlement of any controversy or claim pertaining to employment actions which may arise between employees and management. It is intended to provide an equitable and timely method for the final disposition of such issues.

Procedure

1. Employees who disagree with decisions involving work philosophies and expectations should first contact the Director of Human Resources to help resolve the matter or may file a grievance under certain circumstances. Such circumstances include decisions on performance increases, transfers, promotions, working conditions (where health and safety are an issue), and equal pay. The grievance process is also available to employees who believe they have been discriminated against or harassed on the basis of age, race, color, sex, national origin, religion or disability.

2. At all stages of this process a Human Resources representative will be available to answer questions regarding procedure and will assist either party with case preparation or advice on matters of policy interpretation.

3. By mutual agreement the time limits provided for in this procedure may be extended. An agreement to extend the limits may be entered into by the employee and Human Resources and should not be denied by either party. Failure by the employee to process a grievance within the time limits shall result in a loss of their right to appeal or otherwise impair the Agency's ability to investigate a grievance and take corrective action.

4. Concerns and complaints regarding policy or performance review decisions are not subject to this policy and should be addressed through the appropriate chain of command.

First Step

An employee who has a complaint must first discuss the matter with his/her supervisor unless the supervisor is the reason for or subject of the complaint, in which case the employee should contact the Director of Human Resources. If the issue cannot be resolved with the supervisor, the employee must state the complaint in writing on a grievance form (available in Human Resources) or in a letter. The written grievance must be delivered to the employee's supervisor or department manager with a copy forwarded to the Administrative Services Department within five (5) working days of the occurrence of the action or event which is the subject of the dispute. A Human Resources representative may accompany the grievant to the initial discussion and any subsequent meetings held by the immediate supervisor. The supervisor or department manager must respond to the grievance within five (5) working days following receipt of the written grievance, either in writing or verbally.

Second Step

If the supervisor or department manager's reply is not acceptable to the employee, he/she may request a hearing before the department manager, Executive Director or his designee, and the Director of Human Resources by submitting the grievance to Human Resources within five (5) working days of the supervisor's reply. Hearing participants will include the employee and the person whose actions are the subject of the grievance, the department manager, the Executive Director or designee and the Director of Human Resources. The hearing will be held at the earliest possible time, and a decision and opinion issued in writing within five (5) working days from the date the grievance hearing was held. Legal and/or personal representatives are not allowed. Any decision of the Executive Director will be considered binding and final except for grievances concerning involuntary terminations.

An employee’s failure to report within 15 minutes of the scheduled time for the hearing without good cause will be deemed a withdrawal of their request, and their rights for appeal will be forfeited.

For harassment related concerns, refer to the Harassment/Sexual Harassment policy.

1.9 Suggestion Program
Effective 1/1/99

Purpose
The Agency encourages employees to present to management constructive suggestions for the improvement of operations. The Agency recognizes all employees whose suggestions are submitted and accepted.

Policy
1. Constructive suggestions by employees should be emailed to the Human Resources general email box. The Human Resources Department will receive all suggestions and will respond in a timely manner. Examples of eligible suggestions include:

    a. A more efficient way to do a job.
    b. Improvement in patient care.
    c. A better method to work with equipment.
    d. Reduction of waste.
    e. Efficient use of materials.
    f. A change in any Agency policy.

2. The management team members will review any suggestions, which improve conditions and ultimately save the Agency financially. Employees will be acknowledged and/or rewarded at the discretion of the Executive Director.

3. Although responses to each question may take research time, the Agency will acknowledge receipt of each question within 10 regular business days.

4. Acknowledgements and responses will not be made possible if sender is anonymous.

1.10 Posting of Job Opportunities

Effective 1/1/99, Revised 7/1/21

Purpose

To afford all employees the opportunity for change in job description or status when openings are available.

Policy

Position opportunities will be posted for a minimum of five (5) days, internally and/or externally as applicable for the position. Opportunities will be posted on the Agency's bulletin boards and website; and other social media means as applicable.

1. If the job is a promotion, it will be made based upon individual qualifications and performance, with seniority taken into consideration when two or more employees possess equivalent qualifications and performance.

2. The employee personnel file, to include disciplinary history, will be reviewed when an employee applies for an internal position. Employees with Level 5 or Level 6 Progressive Disciplinary actions are not eligible to apply for an internal opportunity for one year after issue of action.

Chapter 2 – Employees Responsibilities

2.1 Code of Conduct

Effective 9/1/99

Policy

The Agency is committed to promoting integrity and maintaining the highest standard of ethical and professional conduct. Medic employees have adopted the following Core Values and Standards of Behavior:

Compassion- A deep feeling for and understanding of others without regard to race, age, creed, or social standing. The desire to identify with or sense something of another's experience; a precursor of caring. This includes kindness, generosity, forgiveness, caring, friendship, love, and sharing toward all people.

Customer Advocacy- Commitment to speaking and acting on behalf of our patients and the community. Being informed of community efforts and programs available and communicating the needs of our patients to staff, family members, or community agencies/providers. The process of speaking out on issues of concern in order to exert some influence on behalf of our patients.

Fairness- The absence of bias in specific realms characterized by freedom from prejudice or favoritism.

Honesty- Telling the truth and being worthy of trust

Integrity- A steady and faithful observance of a code of moral values. This includes honesty in word and deed and a sense of right and wrong. Steadfast adherence to high ethical principles or professional standards; truthfulness, fairness, doing what you say you will do, and speaking forth about why you do what you do. Uprightness of character and soundness of moral principle, absolute truthfulness, and honesty.

Responsibility- Being reliable and following through on commitments. Solve problems rather than make excuses, being a reliable team player. Accountable for actions and decisions, following policy and clinical protocol, supportive, reinforcing appropriate behavior as well as consequences when not following policy.

Straight Forwardness- Free from ambiguity or pretence; honest and frank. Manifesting honesty and directness, especially in speech: candid, direct, downright, forthright, frank, open, plainspoken.

As part of the annual performance appraisal, a signed attestation of compliance with this policy will be required of all employees.

2.2 Employee Behavior

Effective 1/1/05

Purpose

It is the policy of the Agency that certain rules and regulations regarding employee behavior are necessary for the efficient operation of the Agency and for the benefit and safety of all employees. This policy outlines such rules and regulations.

Policy

1. Conduct that interferes with Agency operations or is offensive to customers or fellow employees discredits the Agency and will not be tolerated.

2. The following are examples of inappropriate conduct that may subject the employee to disciplinary action, including termination of employment:

    a. Reporting to work under the influence of alcoholic beverages and/or illegal drugs and narcotics. (Refer to Drug and Alcohol Testing Policy)

    b. Using, selling, dispensing, or having possession of alcoholic beverages and/or illegal drugs and narcotics on Agency premises. Agency employees will not consume alcoholic beverages eight hours prior to reporting to work).

    c. Reporting to work impaired (diminished cognitive, interpersonal, social and/or vocational effectiveness).

    d. The use of profanity or abusive language, to include inappropriate radio communication.

    e. The possession of firearms or any dangerous weapons on Agency property.

    f. Insubordination or the refusal by an employee to follow management instructions concerning a job related matter.

    g. Fighting or assault of a fellow employee, patient, or customer.

    h. Theft, destruction, defacement, or misuse of Agency property or another employee's property.

    i. Gambling on Agency premises.

    j. Falsifying any Agency record or report.

    k. Failure to wear assigned safety equipment (i.e., PPE, gloves, goggles) or failure to abide by safety rules and policies.

    l. Failure to comply with uniform policy.

    m. Engaging in any form of harassment, intimidation or discrimination.

    n. Being convicted of a felony. If an employee is charged with a felony, the employee may be suspended until a conviction or an acquittal is rendered.

    o. Loss of driver's license by personnel who have job descriptions which require a valid driver's license to perform their job functions.

    p. Excessive absenteeism and or tardiness. (Refer to Attendance Policy)

    q. Loss of insurability by personnel who have job descriptions, which require valid driver’s license to perform job functions.

    r. Violation of established policies & procedures.

    s. Misuse of Agency computers or e-mail.

    t. Failure to report behavior by others which violates Agency policies.

3. The foregoing list sets forth examples of inappropriate conduct. It is not intended to be all-inclusive. There may be other examples of inappropriate conduct while in the discretion of the Agency, justify immediate disciplinary actions up to and including termination.

2.3 Dress Code

Revised 4/1/03; Revised 1/3/14; Revised 3/5/14; Revised 3/14/14

Purpose

Employees are expected to maintain a standard of dress and personal grooming that creates a professional, favorable, and welcoming appearance for our patients, visitors and the public at-large. Field employees are required to wear designated uniforms as determined by current uniform policy.

Policy

General guidelines for all employees are as follows:

a. Clothing must be clean, pressed, neat and in good repair.
b. Employees should practice good overall personal and oral hygiene to prevent offensive body odor.
c. Employees' hairstyle must reflect professionalism and safety for patients. Hair must be neat and clean and it is preferred that long hair is away from face. No extreme hairstyles and hair dyes. Mustaches must be clean and neatly trimmed. Facial hair must not interfere with proper PPE fit and usage. Facial hair (with exception of clean and neat mustache) is prohibited for employees that at any point in time are required to be in uniform bearing a certification patch.
d. Jewelry must be conservative and professional so that bracelets, necklaces, earrings and rings are not interfering with patient care or operation of equipment. Field employees may wear studded earrings only. Visible pierced jewelry on body parts other than ears (nose, tongue, etc.) are not allowed.
e. No tattoos or brands may be visible when wearing uniforms.
f. Shoes should be clean, professional in appearance and in good repair. Hosiery must be in good repair and be worn at all times, except for female (non-uniformed) administrative personnel who elect to wear open-toe sandals with their appropriate summer attire.
g. Perfume, cologne and other fragrance toiletries are prohibited in patient care areas.
h. All personnel must wear identification badges during working hours.

Acceptable & Professional Attire includes:

a. Dress and skirts in a professional style, length and fit,
b. Tailored suits and pants
c. Shoes in good repair and stockings/hosiery
d. The Agency has adopted Fridays as "Business Casual". Acceptable business-casual attire includes: golf shirts, casual skirts and khaki style pants.

Unacceptable Attire includes:

a. Shorts, sundresses, spandex and leggings
b. T-Shirts, sweatshirts
c. Denim jeans
d. Tennis shoes

This dress code has been adopted for all Agency employees. Supervisors are responsible for seeing that the dress code is enforced. Employees will be excused without pay pending change of attire if they come to work in attire deemed unprofessional. Refusal to comply with the dress code or repeated incidents of inappropriate dress may result in disciplinary action. Exception to the dress code policy for valid medical or religious reasons will be considered on a case-by-case basis.

2.4 Performance Improvement/Progressive Discipline

Effective 1/1/99, Updated 10/1/2018

Purpose

This policy provides guidelines for performance improvement and disciplinary action by the Agency.

Policy

1. When performance improvement or disciplinary action is necessary, supervisors/leaders will follow the appropriate process depending upon employee status as outlined below. However, the Agency may, in its discretion, apply other disciplinary measures, as appropriate, on a case-by-case basis and is not required to follow any prescribed disciplinary procedure.

2. Full-Time Regular Employees

   a. Performance Improvement is used to correct unsatisfactory job performance or behaviors of regular employees who have successfully completed a provisional period.

      Performance Improvement (PI) consists of:
      - Level 1 PI Performance Modification
      - Level 2 PI Performance Modification
      - Level 3 PI Performance Modification
      - Level 4 PI Performance Modification with Work Plan

   b. If Performance Improvement does not succeed, progressive discipline begins.

      Progressive Discipline (PD) consists of:
      - Level 5 PD Written Warning
      - Level 6 Decision-Making Day
      - Termination or resignation, if the issue is not corrected

   c. For conduct, safety violations or serious misconduct, PIPD, may begin at any level in the process to include a Decision-Making Day of Leave and/or termination.

   d. For serious misconduct, an employee may be terminated immediately without any prior PIPD levels.

   e. Absence of two consecutive workdays without notification and proper authorization will be considered a voluntary resignation with no right of appeal.

3. Introductory Employees

   a. Employees who have not attained regular status and are still in the introductory period may be terminated immediately for unsatisfactory job performance or conduct/safety violations without following the progressive discipline process.

   b. There is no right of appeal for introductory employees.

   c. Appropriate documentation of the termination will be included in the employee's personnel file.

4. Part Time Temporary Employees

   a. Employees who are temporary may be terminated immediately without following the progressive discipline process or right of appeal.

5. Performance Improvement and Progressive Discipline

   a. When unsatisfactory behavior and/or job performance are first observed, a Level 1 PI Performance Modification should be initiated to prevent the conduct and/or performance problem from becoming a disciplinary issue.

b. If unsatisfactory behavior and/or performance problems continue, a Level 2 PI Performance Modification should be initiated.

c. If an additional issue occurs a Level 3 PI Performance Modification will be initiated. However, if the same issue has occurred for the third time (the Three Strike Rule) it may escalate to a Level 4 Work Plan developed with the employee by the supervisor. A Work Plan serves as notification to an employee that a level of performance and/or behavior is currently below the standards that are expected. This non-punitive process allows employees to look toward their future with the organization without a strong emphasis on the past. A Work Plan is a method used to help improve performance. It places the responsibility for corrective action(s) on the employee and reminds the employee of the organization's work philosophies and expectations.

d. Three Strike Rule. If an employee commits the same offense or infraction for a third time, one level may be skipped. The three offenses do not need to be consecutive; however, a Level 6 Decision Making Day may not be skipped under the Three Strike Rule.

e. The disciplinary process will begin at Level 5 PD Written Warning. If the employee's performance or behavior has not improved, a Level 5 PD Written Warning will be issued to the employee outlining further corrective action and appropriate time frames necessary to meet expectations.

f. If there are continued deficiencies following the Level 5 PD Written Warning, the next step involves Level 6 Decision-Making Day. The acceptable performance and/or behavior is discussed with the employee, and the supervisor then authorizes a Decision-Making Day of leave. The employee must provide a written response to be included in their personnel file. An employee is paid for this day of leave in an effort to demonstrate management's good faith and continuing commitment to the organization's Standards of Behavior, Values and Guiding Principles, and the Agency Mission. This day is not subject to appeal. The Decision-Making Day serves as a cooling off period; a demonstration of management's seriousness; a time for the employee to consider their responsibilities and the expectations of the supervisor; and a time for the employee to consider future options including returning to their job, reassignment or resignation.

g. If the employee elects to return to the job, the employee must present in writing their plan to solve the specific deficiencies and commit to totally acceptable performance in every area of their job. Employee(s) electing to return from a Decision-Making Day will meet with their supervisor for a performance improvement session. During this session, the employee and supervisor will review the improvement steps and corrective action plan in written form and time period necessary to meet expectations.

h. If the employee believes the problem cannot be effectively resolved and wishes to remain with the Agency, a reassignment to a suitable vacant position may be requested. The decision to approve a reassignment request is at the discretion of the department director and compensation may be affected with such change. If the employee resigns, a letter of resignation must be submitted to the supervisor/leader on the next business day.

i. If the employee elects to resign or request reassignment, this decision should be discussed at this session. Should the employee commit to the improvement plan but fail to complete it satisfactorily, the employee will be terminated according to the procedures outlined in the termination policy.

2.5 Harassment/Sexual Harassment

Effective 1/1/99; Revised 01/01/08

Policy

The Agency is strongly and actively committed to providing safe and pleasant working environment. As such, harassment of employees because of sex, race, religion, age, national origin, disability, sexual orientation, etc., will not be tolerated. Harassment may take the form of physical or verbal conduct, which may lead to, among other things, intimidation, aggression, hostility or unequal treatment. These unwelcome activities create a hostile and abusive work environment.

Prohibited actions include:

1. Harassment – Harassment is verbal or physical conduct that denigrates or shows hostility or aversion toward an individual because of race, color, religion, gender, national origin, age, sex, disability, veteran status, political affiliation, sexual orientation or any statute protected by law which has the purpose or effect of creating an intimidating, hostile, or offensive work environment or interferes with an individual's work performance or otherwise adversely affects an individual's employment opportunities.

   Harassing conduct includes, but is not limited to: epithets, slurs, negative stereotyping, or threatening, intimidating, or hostile acts that relate to race, color, religion, gender, national origin, age, disability or political affiliation. Written or graphic material, which denigrates or indicates hostility or aversion toward an individual or group, is prohibited from display on the employer's premises, or circulation in the workplace.

2. Sexual Harassment - The Agency prohibits sexual harassment of its employees by other employees or outside parties. Sexual harassment affects morale, motivation and job performance. It is inappropriate, offensive, and illegal and will not be tolerated. Sexual harassment includes unwelcome verbal behavior such as comments, suggestions, jokes or derogatory remarks based upon sex; physical behavior such as inappropriate or offensive touching; visual harassment such as posting of sexually suggestive or derogatory pictures, cartoons or drawings, even at one's work station; unwanted sexual advances, pressure for sexual favors and/or basing employment decisions (such as an employees performance evaluations, work assignments, or advancement) upon the employee's acquiescence to sexually harassing behavior in the workplace.

   Any employee who is aware of any instances of sexual harassment or other type of harassment should report the alleged act immediately to his or her supervisor. If the employee is uncomfortable in discussing the matter with the supervisor, or if the supervisor is not available, the employee should report the alleged act immediately to the supervisor's manager and/or the Director of Human Resources. Supervisors, managers and directors who receive a sexual harassment complaint are to contact the Director of Human Resources immediately. Likewise, any employee who believes that another employee is being harassed should report this to the Director of Human Resources immediately.

   Failure to report harassment involving others may subject you to disciplinary action up to and including termination of employment.

   All Complaints will be investigated promptly, impartially and discreetly and, upon completion of the investigation, the appropriate parties will be notified immediately of the findings. Any employee/manager who has been found to have harassed an employee will be subject to appropriate corrective action, up to and including termination. No employee will suffer retaliation for reporting instances of harassment in good faith.

It is expected that employees of the Agency will act responsibly to maintain a professional working environment, free of discrimination, allowing each employee to perform to his or her maximum potential. The Agency encourages any employee to bring questions he or she may have regarding discrimination of this type of the Director of Human Resources.

See Agency Grievance Policy.

2.6 Employees as Representatives of the Agency

Effective 1/1/99

Purpose

To give the employee a guideline concerning Agency representation.

Policy

1. An employee of the Agency will not originate correspondence on the Agency letterhead without authorization.

2. An employee of the Agency will not present himself/herself as an Agency representative when off duty. Employees must be aware of the fact that the public and media may consider them as an Agency representative at any time. Employees should therefore conduct themselves in a fashion or manner that does not adversely impact the Agency's image. Further, employees acting on their own are solely liable for any information they release.

3. An Employee who is off-duty and is confronted with or acts upon an EMS situation shall at all times conduct him/herself in accordance with local medical protocol and departmental policy.

2.7 Employment or Volunteer Work Outside the Agency

Effective 1/1/99

Purpose

The Agency realizes that many employees desire to engage in outside employment, whether paid or unpaid. In an effort to avoid any conflicts, the policy below will be followed.

Policy

1. Agency employees are expected to meet their obligations to the Agency over all other employers or volunteer commitments. These obligations include the employee reporting to work adequately rested and fully prepared to perform their job duties.

2. Employees should not engage in other employment or volunteer work which:

   a. Could be inconsistent with the interests of the Agency.

   b. Could by reason of association adversely affect the reputation of the Agency.

   c. Could require devoting so much time and effort to the job that work efficiency and safety at the Agency would be adversely affected.

   d. Could conflict with Agency employment, because occasionally employees will be required to stay later than their assigned shift. Due to the nature of our business, outside employers should be advised of this prior to your employment. If conflicts occur, this should be relayed to your Supervisor for possible accommodations.

   e. Interferes with on-duty activities.

3. The Executive Director must approve employment outside the Agency. Each employee who wishes to pursue outside employment shall give written notice to the Executive Director specifying the details of all outside employment engaged in or to be engaged in by the employee.

2.8 Professional Licensure/Registration/Certification
Revised 11/1/00

Purpose
To provide employees with information on the necessary professional licensure, registration and certification to maintain employment at the Agency.

Policy
1. Employee in positions identified in the chart below are required to maintain current level of licensure, registration or certifications.

2. Evidence of such licensure, registration, or certification must be submitted to the Human Resources Department prior to initial employment and resubmitted upon renewal and request of the Agency.

3. Failure to submit and maintain current licensure, registration or certification constitutes grounds for disciplinary action up to and including termination of employment.

PARAMEDICS	**EMT-B**
*Valid Drivers License *Maintain insurability with Agency's insurance carrier *EMT-P Certification *BTLS *ACLS/PALS or EMS-C *CPR *All mandatory in-service training *Fit testing *Semi-annual TB testing *Agency approved driving course	*Valid Drivers License * Maintain insurability with Agency's insurance carrier *EMT-B certification *BTLS *CPR *All mandatory in-service training *Fit testing *Semi-annual TB testing *Agency approved driving course

COMMUNICATIONS	**ADMINISTRATIVE**
*EMD *CPR *EMT – didactic *Annual TB testing *All mandatory in-service training	*Annual TB testing

2.9 Attendance Policy

Effective 10/1/02, Revised 10/1/05; 9/15/06; 6/24/08; 8/27/09; 7/1/13; 6/4/14; 10/1/18, 2/1/23

Purpose

The purpose of the attendance policy is to manage attendance in a consistent manner. Regular attendance and punctuality are important elements in our efforts to maintain excellent customer service and patient satisfaction. Being part of a team requires that each person be in the right place at the right time. When staff meets their obligation to report for work punctually, the burden of work is not passed on to co-workers or delayed. Reworking assignments or schedules to accommodate absences/tardiness represents inefficiency and negatively impacts the Agency's mission, vision and values.

Policy

Attendance infractions are managed by Agency's the Performance Improvement, Progressive Disciplinary process (Policy 2.4). All attendance behaviors are addressed with application of Performance Improvement Observations (PIOs) or Performance Improvement, Progressive Discipline documentation (PIPD) by their direct chain of command or appropriate designee.

Part time (temporary) employees will be assessed PIPD triggers for all attendance infractions.

Employees have ability to utilize their sick leave benefits, when following the appropriate call-out procedures and have enough accrued sick leave to cover the entirety of their shift.

Employees have the opportunity to accumulate vacation benefit leave for perfect attendance. This incentive is measured and applied on a calendar quarter basis for eligible employees.

Reporting for Duty

Employees should be ready for work at their assigned location, whether onsite, offsite or remote, for their scheduled shift and are required to clock in by their scheduled start time. Employees are also required to clock out at their scheduled end time. **This includes clocking out and back in between double shifts.** If the employee is in the field when the double shift occurs there is no need to report back to headquarters to clock out and in between shifts.

Reporting Absences or Potential Tardiness

Occasionally there are times when an employee must be absent from work because of illness or other reasons, or may have potential of a late arrival for their shift start time. The employee must personally notify the Agency of their absence or tardiness prior to their shift via the below guidelines (not through spouses, dependents, friends or co-workers). All absences and potential for tardy should be reported as soon as possible. Following the proper call-out policy with enough benefit leave to cover an absence will not be considered an attendance infraction.

Employees are required to follow their specific departmental policies as defined below:

Field Operations

Employees are required to contact the on-duty Operations Assistant **at least** one (1) hour prior to the start of their assigned shift. If the Operations Assistant is not available employees are required to leave a voice mail message **and** then call the on duty CMED Supervisor so that timely adjustments can be made to the schedule.

Communications / Support Services

Employees are required to contact the on-duty Supervisor **at least** two (2) hours prior to the start of their assigned shift. If the on-duty Supervisor is not available, employees are required to leave a voicemail and contact the on-duty Operations Assistant so that timely adjustments can be made.

All Other Departments
Employees are required to contact their immediate supervisor **at least** one (1) hour prior to the scheduled start time or as otherwise established by the department.

Terms
Scheduled Work – All hours that are part of an employee's scheduled work week such as:

- regular scheduled hours
- mandated scheduled hours
- voluntary shift sign ups, overtime/extra shift (outside regular hours)
- scheduled personal swap/duty exchange

Full Time – Employees who earn/accrue benefits

Part Time (Temporary) Personnel – Employees who do not earn/accrue benefits

Absence – Any unscheduled, unplanned or unauthorized time away from work, whereas the employee has not communicated verbally or in written form regarding time away.

High System Demand Period/Mandated Period – Any date/event such as a holiday, major drill, disaster, etc. that has the potential to burden the system due to increased call volume. The Agency reserves the right to freeze scheduled benefit leave during these times. Any unscheduled benefit leave use may be subject progressive disciplinary action, up to and including termination.

Attendance Behavior Infraction – Behavior that requires a documented conversation to prevent reoccurrence. Infractions may accumulate in additional to any other infractions occurred simultaneously. If multiple actions/documentation are due, the highest level will be assessed.

Detailed information related to standard operating procedures associated with the attendance policy can be found on the extranet.

This policy is a guideline only and does not create a guarantee of employment, maintaining an at-will employment status. Notwithstanding this Policy, the Agency reserves the right to discipline or terminate any employee at any time and for any reason not in violation of local, state or federal law.

2.10 Continuing Education

Effective 1/1/99

Purpose

To provide for the provision of high quality continuing educational programs for the development of Agency employees.

Policy

1. Employees must meet the training requirements set by the Agency.

2. The Agency will pay the reasonable costs associated with required training for employees unless otherwise specified.

3. A schedule listing all educational programs will be available through the Medical Services Department or the Medical Services for non-clinical staff members.

2.11 Drug and Alcohol Testing

Revised 11/1/04; 10/1/05

Purpose

To assure employee and applicant fitness for duty and to protect employees, patients and the public from the risks posed by the misuse of alcohol and use of illegal or prohibited substances.

To also assure drug and alcohol tests are collected in a manner that protects the integrity of samples and the dignity of the individuals being tested.

Policy

The Agency recognizes that an employee's on or off the job involvement with drugs and alcohol can have an impact on work productivity and on the ability to provide a work environment free from the effects of substance abuse. It is inappropriate for the Agency to intrude into the private lives of its employees, but employees are expected and required to be in a condition to safely and effectively perform their duties throughout the workday.

The Agency offers an Employee Assistance Program (EAP), which provides 24-hour on-call assistance for employees with problems affecting their job performance or well-being. Employees should contact their supervisor or the Human Resources Department for more information. An employee's voluntary participation in the EAP may be favorably considered in any proposed disciplinary action for previous substance abuse infractions. Employees who are found to have violated the substance abuse policy and are not successfully engaged in a treatment/rehabilitation program may be dismissed.

During regular business hours, Monday through Friday 8:00 a.m.- 5:00 p.m., the Employee Health Nurse or Risk and Safety Specialist in Human Resources will be responsible for collecting urine samples for all urine drug testing and/or breath alcohol testing. An outside contracted service will provide a collection agent on site for testing after regular business hours. See attached for contact information and hours. All testing will be done using appropriate chain of custody procedures to insure accuracy and confidentiality. Samples for urine drug testing will be sent to an approved testing laboratory.

Those employees/applicants whose drug test is verified positive will have seventy-two hours after notification by a Medical Review Officer to request that their original sample be retested. The employee or applicant will pay the cost for the retest.

Pre-placement Testing

All eligible candidates for employment must take a drug test and show a negative result prior to being hired and as a condition of employment. *Testing results will be valid for 30 days from the date of testing.* The Human Resources Department will coordinate this process. Candidates who fail to show up for a test will no longer be considered for employment. There are no exceptions to these conditions. *The Agency may accept a negative drug test at another location provided it was completed less than one (1) month prior to hire date by an approved drug-testing laboratory.* In the event of a positive drug test, the candidate may request a retest of the original sample within 72-hours of receipt of the test result. The applicant will be given the option of choosing a different DHHS/SAMHSA certified laboratory to perform the retest. The retest is at the candidate's expense. If the retest is negative, the Agency will provide reimbursement for the expense. Candidates who test positive for drugs or alcohol will not be considered for employment for at least one (1) year from the date of the positive test.

Reasonable Suspicion Testing

When there is a reasonable suspicion that an employee is impaired and would be incapable of safely performing his assigned duties and responsibilities, the Agency will arrange to verify the reasonable suspicion. Reasonable suspicion is that quantity of proof or evidence that is more than intuition or strong feeling. Such reasonable suspicion must be based on specific

observations concerning the appearance, behavior, speech, and/or body odors of the employee. Factors supporting a reasonable suspicion determination include but are not limited to any one or more of the following:

a. Direct observation of prohibited drug or alcohol use
b. Slurred speech
c. Alcohol beverage odor on breath
d. Unsteady walking and movement
e. An accident involving Agency property
f. Physical altercation
g. Verbal altercation
h. Lapse in cognitive abilities
i. Aggressive, hostile, threatening, disruptive, or unusual behavior
j. A report of drug or alcohol use provided by a reliable and credible source.
k. Evidence that the employee is involved in the use, possession, sale, solicitation, or transfer of prohibited drugs.

These observations (or other factors supporting a reasonable suspicion) must be personally observed and documented by at least one (1) supervisor or manager and reported to the Director of Human Resources. In the event the Human Resources Director is not on duty, the supervisor will review and consult with at least one other supervisor to confirm the decision and process forward. The Human Resources Director shall be notified on the next business day.

The supervisor/manager will direct the employee to a confidential area away from other employees and will verbally inform the employee that a reasonable suspicion test is an obligation and refusal to submit to such testing will result in termination. If the employee agrees to take the test, the employee will be informed that they are suspended from work with pay and will be notified whether or not and under what circumstances they will be permitted to return to work. It is the responsibility of the supervisor/manager to transport the employee to the designated area for testing. If the employee refuses to take the test, the employee will be terminated and will be notified in writing by the department director. Arrangements will be made to have the employee taken home. The employee will not be allowed to drive. If the employee insists on driving, the police will be notified.

Random Testing
From time to time the Agency conducts random drug and alcohol testing of employees. All Agency employees are subject to random testing at any time. Refusal to be tested will be considered grounds for termination. In the event of a positive drug test, the candidate may request a retest of the original sample within 72-hours of receipt of the test. The employee will be given the option of choosing a different certified laboratory to perform the retest. The retest is at the employee's expense.

Illegal Drugs or Alcohol
Employees testing positive for the use of illegal substances or alcohol will be subject to disciplinary action, including termination of employment.

In the event that our provider for after hours drug and alcohol testing needs to report a breath alcohol test that is .020-.039 or above .040, they will be instructed to call 704-943-6226 and ask to speak to the on-duty Operations Supervisor. They will NOT give this information to anyone else at the Agency to be relayed to the Operations Supervisor. Should the Operations Supervisor be occupied with field duties, or otherwise unavailable, the Operations Assistant will make every effort to contact the Supervisor by cell phone or pager. If the provider is unable to reach the Supervisor within 30 minutes, they will be instructed to call the CMED Supervisor, who will, in turn, page the Director of Operations or the Assistant Director of Operations.

A breath alcohol level of .040 or greater is considered positive and the employee shall be terminated. If the reading is between 0.020 and 0.039, the employee shall be placed on disciplinary suspension without pay for a twenty-four (24) hour period and documentation of such event will be placed in the employee personnel file.

The supervisor or manager of the employee being sent home shall assist the employee in getting a ride home. Any supervisor or manager who witnesses an impaired employee operating a motor vehicle will contact law enforcement.

A negative alcohol test result must be provided before returning to work.

2.12 Drug Free Workplace

Effective 1/1/99

Purpose

To ensure a drug free work environment for all employees.

Policy

The use of illegal drugs and misuse of legal substances by a significant segment of the American work force has major adverse effects on the welfare of all citizens and results in the loss of considerable money and productivity each year. Because the safety of its employees and the delivery of service to its citizens are adversely affected by alcohol and substance abuse, the Agency cannot afford to ignore this critical problem.

The Agency is committed to provide, within its means, a healthy, safe, and drug free work environment; to provide the best possible services to citizens; to maintain the public's confidence in its employees; and to protect the Agency from the economic losses that can occur due to substance abuse. To meet each of these issues, the Agency's policy is to:

1. Assure that employees are not impaired in their ability to perform assigned duties in a safe, productive and healthy manner;
2. Create an environment free from the adverse effects of drug abuse and alcohol misuse;
3. Prohibit the unlawful manufacture, distribution, dispensing, possession or use of controlled substances; and

Encourage employees to seek professional assistance through the Employee Assistance Program (EAP) anytime personal problems, including alcohol or drug dependency, adversely affect their ability to perform their assigned duties.

2.13 Physical and Mental Fitness (Fit for Duty)

Revised 9/1/99, 03/25/14

Purpose

The Agency provides a safe and healthy work environment and seeks to promote the health and welfare of its employees. The Agency recognizes the importance of physical and emotional health as it pertains to job performance and overall quality of life. Therefore, the Agency requires all employees to report to work, be fit for duty and to perform assigned duties without any physical or mental impairment, which would unreasonably interfere with the employee's ability to perform the essential functions of the job.

Fit for duty is defined as a physical and mental status that facilitates the performance of duties completely and efficiently without impairment in coordination or skill. Being fit for duty allows employees to perform job responsibilities in a safe and effective manner that does not jeopardize the health and safety of others.

To help promote health and welfare, the Agency provides an Employee Assistance Program (EAP) through Business Health Services 800-237-2251, or www.bhsonline.com code MECKCO, on-site fitness facility and a risk & safety/occupational health department. All employees are eligible for these benefits and are encouraged to seek assistance whenever necessary.

2.14 Severe Weather

Effective 2/1/03, Revised 12/1/09, Revised 10/5/17

Policy

The nature of Medic's role and service to the community mandate continuous operational ability. Employees who work in functions essential to the 24-hour operations of Medic, or in functions determined essential by the department director, must maintain their regular work hours during inclement weather.

For other employees, Medic will observe Mecklenburg County's operating hours during severe weather.

Procedure

During periods of inclement weather, all non-essential employees shall access the official information by calling Mecklenburg County's "Employee News Now" phone line at **980-314-4444** or by monitoring broadcast media.

It is the employee's responsibility to call any time there is a question regarding changes to the Agency's operating hours during severe or inclement weather.

In times of emergencies or declared disasters, the Agency may require non-operations personnel to report to work, in support of the emergency services, even when other local government offices are closed.

When the office hours are modified, the Employees will be paid for hours normally scheduled for that day. To illustrate, if the start of the workday is delayed until 10:00 a.m. employees who normally begin work at 8 a.m. will have 2 hours credit for "inclement weather." If the employee's normally scheduled to begin at 9, there is one hour of credit for that day. If the office is closed for the entire day on a day when the employee normally works 8 hours, the employee is paid for a full day. If the office is closed on a day that is the employee's normal day off, there will be no credit for hours.

If an employee who normally begins work at 8 a.m. reports at 11:00am, they must charge one hour of vacation/holiday leave. If the employee does not come to work on a day that Medic has delayed opening due to inclement weather, the employee must use vacation/holiday hours for the hours that the Agency is open.

For example, if the Agency closes at noon an employee who has not reported to work must charge 4 hours to vacation leave or leave without pay. A non-exempt employee will be in a leave without pay status if there is insufficient benefit accrual. Exempt employees are not subject to leave without pay for partial day absences.

A department may require appropriate medical documentation to verify the use of sick leave. This Policy does not affect employees on vacation, sick or other leave.

2.15 Infectious Disease Policy

Effective 10/28/13; Revised 10/20/14, Revised 01/04/2022

Policy

Medic is committed to providing a safe and healthy environment for all employees and patients. In pursuit of this endeavor, there will be times, such as the influenza season, or a pandemic outbreak, when the Agency will require employees to take action with regard to protection against infectious diseases.

Required employee action will include mandatory vaccination with exception for valid, documented medical or religious reasons. Employees with documented medical or religious exemptions will be required to use personal protective equipment (PPE) as directed.

All employees will be required to comply with all Agency mandated protective measures within the timeframe specified by the Agency. Anyone failing to meet the required standards will be subject to placement in a non-work status and disciplinary action up to and including termination.

The required actions may change as directed by the Agency, and will be based upon a host of factors emanating from various local, state and federal authorities.

2.16 Paramedic Crew Chief Upgrade

Effective 07/01/2016

Policy

The Crew Chief Upgrade process ensures the Agency is able to fill shift vacancies in a timely fashion. Paramedics are required to upgrade to Relief Crew Chief within 365 calendar days* from when the Agency releases the employee to function as a Paramedic. Once upgraded to Relief Crew Chief, the employee will be included in the Crew Chief shift bid process described below.

*Circumstances beyond the employee's control which inhibit this requirement will be evaluated on a case by case basis.

Definitions:

Full Shift Bid – a mandatory process where the full field operations schedule is placed out for bid. All full-time employees are ranked and bid for their upcoming assigned shift.

Crew Chief Upgrade Shift Bid – a mandatory process where paramedic relief crew chiefs are ranked and bid for their crew chief shift. This bid may occur periodically throughout the year based upon Agency needs.

Bid Group – a group of employees that completed crew chief class together.

Procedure

When the Agency determines that a crew chief vacancy exists, the scheduling department will conduct a Crew Chief Upgrade Bid to fill vacant shift(s) within two full pay periods after the vacancy occurs.

The bid process is as follows:

1. All eligible employees will receive notification of the vacancy through a shift bid email.
2. The email will state [P1: Shift Bid – ACTION REQUIRED].
3. The email will include:
    i. Vacant shift(s) detail
        a) Shift name
        b) Start/stop time
        c) Workdays/rotation pattern
        d) Shift calendar for the remaining calendar year
        e) Partner (if any)
        f) Supervisor assignment
    ii. Timeline
        a) Date bid begins
        b) Date bid closes (minimum 7-day span)
        c) Date results will be emailed to all employees
        d) Date in which the assignment(s) begin
    iii. Employee Rank
        a) Each participating group will be considered a bid group for the purpose of rank. All employees within that group will be ranked in order according to their most recent shift bid score.
        b) Employees that become eligible in subsequent bids will also be ranked in order according to their most recent shift bid score, but as a separate group below the previous bid group.
    iv. Online shift selection form link

All employees will be required to select the number of shifts equal to the number available, i.e. if there are 10 shifts available, all employees are required to select 10 shifts in the bid.

If an employee has not submitted an entry within one day of the close date, the scheduling supervisor or designee will email (cc: employees' supervisor) and call the employee for follow-up on the requirement. If the employee does not submit an entry by the deadline, the employee will be subject to being administratively places after the bidding is complete.

Assignment Process:

1. All shift bid entries will be collected and sorted at the close of the bid.
2. Employees will be assigned shifts in order of their ranking.
3. After all assignments have been confirmed, an email will be distributed to all employees that participated in the bid.
4. Scheduling will attempt to honor any previously approved vacation time periods for the new shifts.
5. Scheduling will process PAFs (personnel requisition forms) for the upgrades within one week of the bid close.

Chapter 3 – Benefits

3.1 Employee Benefits

Revised 2/1/05; 8/1/13; 1/3/14

Purpose

To provide eligible employees with a guideline of benefits above and beyond wages. Benefits may be modified by the Agency from time to time in the Agency's discretion without prior notice.

Policy

The benefits listed below are provided to eligible employees. The Agency reserves the right to add, modify or eliminate benefits from time-to-time without prior notice to employees. Please contact your Human Resources Department for a summary of the most updated information on each benefit:

- Health Insurance
- Dental Insurance
- Vision Insurance
- Life and AD&D Insurance
- Worldwide Travel Assistance
- Temporary Disability Insurance (TDI)
- Temporary Long Term Disability Insurance
- Supplemental Life Voluntary Insurance
- AFLAC Voluntary Insurance
- Life, Auto, and Home Voluntary Insurance Program
- Flexible Spending Account & Dependant Care Account
- Employee Assistance Program (EAP)
- NC Local Governmental Employee's Retirement System (NCLGERS)
- 401(k) and Roth 401(k)
- 457 Plan
- NC Association of Rescue & EMS
- Firemen's and Rescue Squad Worker's Pension Fund
- Public Safety Officers Benefits
- Employee Benevolent Fund
- Social Security
- Administrative Leave
- Family and Medical Leave Act (FMLA)
- Extended Medical/Family Leave
- Worker's Compensation
- Military Training
- Sick Time
- Vacation Time
- Holiday
- Bereavement
- Jury Duty
- Relocation Benefit
- Sign-on Bonus- Paramedics
- Sign-on Bonus- EMT's and Dispatchers
- Referral Bonus
- Tuition Reimbursement
- Fitness Room
- County Care Fitness Program
- Aquatic Center
- Discounted Bus Passes
- Credit Unions
- Government Employee Travel Opportunities

3.2 Tuition Reimbursement

Effective 9/1/99, Revised 7/1/03, 7/1/06, 7/1/07, 6/17/15

Purpose

To provide financial assistance to employees who enroll in incidental, academic course work at an accredited educational institution or attend work-related seminars/conferences not mandated by the Agency with prior approval.

Policy

All regular benefit eligible employees are eligible for school tuition and/or approved seminar reimbursement. Reimbursements are based on allocation of funds up to an annual maximum of $750 for school tuition and $200 maximum for approved seminar/conference reimbursement and are provided on a first-come-first-serve basis.

The total amount of reimbursement available for each regular benefit eligible employee applying for both school tuition and seminar/conference reimbursement may not exceed $750.

This benefit is budgeted annually. 50% of the allocated funds will be made available on a semi-annual basis to ensure equal opportunity for all employees throughout the year.

Courses or subject must be job related or lead to a degree that could be utilized at the Agency. Objectives or content of any seminar/conference will be taken into serious consideration before approval is made.

Tuition Reimbursement Forms must be completed **before the start of the class or program.** Forms are available on the payroll portal under electronic forms. Forms can also be submitted through employee documents on the payroll portal.

Expenses eligible for reimbursement are classroom tuition, seminar/conference costs, fees and books.

Expenses not eligible for reimbursement includes tools, and supplies (other than books) retained by the student or participant, travel, meals, lodging, parking and transportation.

To be eligible for tuition reimbursement, all employees must (a) submit tuition reimbursement form, in advance, of the course prior to enrolling (b) obtain a satisfactory grade (i.e., C or “pass”) as established by the educational institution; (c) submit student transcript and/or grade report to the Agency; and (d) submit proof of tuition payment. All documentation (grades and receipts) must be received within 30 days of the conclusion of the course(s) or by June 30th of each fiscal year, whichever is sooner, to be eligible for reimbursement.

3.3 Vacation Benefit Leave
Effective 1/1/99; Revised 8/1/07; Revised 7/1/13, Revised 1/2/18

Purpose
Vacation leave is extended to all eligible employees for the purpose of compensated time away from their regular assignment in order to ensure their physical and mental well-being. It is designed to encourage advance scheduling of vacation leave in order to provide for optimum staffing.

Policy
Vacation Leave accrues from the first day of service and is granted with pay to all full-time (and existing permanent part-time) regular employees after the initial ninety (90) calendar days of employment. Temporary employees are not eligible for vacation benefits. Maximum accrual of benefits is based on the employee's scheduled hours of work annually. Eligible employees accrue vacation on a bi-weekly basis determined by the length of service (aggregate date in the N.C., Retirement System). The accrual rates are as follows:

40-HOUR WORK WEEK EMPLOYEES:

Length of Service	**Accrued hours per pay**	**Annual Accrual**
Under 2 years	3.07	79.82
2- up to 5 years	3.69	95.94
5 – 10 years	4.61	119.86
10 – 15 years	5.53	143.78
15 – 20 years	6.46	167.96
Over 20 years	7.38	191.88

Vacation leave accrued in excess of 240 hours during the calendar year will be converted to sick leave at the end of the calendar year. Only a maximum of 240 hours may be carried over into the new calendar year. Employees who leave the employment of the Agency will be paid for accrued vacation time up to a maximum of 240 hours.

Four (4) hours of vacation leave shall be awarded to the accumulated benefits of all employees eligible to receive vacation leave who do not use sick leave and/or leave without pay for a period of one quarter year.

Quarters are defined as:

- Quarter 1 January – March
- Quarter 2 April – June
- Quarter 3 July – September
- Quarter 4 October – December

Process for Requesting the use of Accrued Vacation/Holiday Leave
Vacation and holiday leave benefits may be requested up to twelve months in advance from the date the request in being made. All requests for vacation or holiday leave are to be in writing on the appropriate Agency benefit leave request form and submitted to the appropriate supervisor or Staffing Office (for Field employees). Benefit leave requests must be received no later than two weeks prior to the requested date. This is to insure that proper coverage can be arranged and/or that staffing levels will not be negatively affected. Any exception to the two-week minimum requirement must be due to extraordinary circumstances and will be reviewed by management on a case-by-case basis.

If an employee takes vacation time for his/her scheduled shift and later accepts another vacant position on the same day, he/she will not be compensated for both vacation and regular earnings during any overlapping period of time. For example: employee takes vacation time during regular scheduled shift from 8:00 a.m., to 8:00 p.m., and then elects to work a later shift

on the same day from 4:00 p.m. to 4:00 a.m., the employee can only claim vacation time from 8:00 a.m. to 4:00 p.m. and the remaining hours that are worked during that time will be paid at regular wages or overtime if hours exceed 40 in a work week.

Due to operational needs each department may differ with vacation approvals. All employees must consult with their department supervisor, manager or director for specific departmental policy prior to making plans for time off.

3.4 Vacation Cash-Out Program

Effective 11/1/02; Revised 6/07

Purpose

To allow employees to cash-out a limited amount of accrued vacation time on an annual basis.

Policy

Employees who have more than 30 days (240 hours) of accrued vacation will be allowed to "cash-out" a minimum of one (1) day (8 hours) up to a maximum of five (5) days (40 hours) per year for the amount of days over 30. This "cash-out" will be included in the second pay period of June. Vacation hours accrued as of the first paycheck in June will be used as the vacation "cash-out" eligibility criteria. Vacation hours used, accrued, or earned during the "cash-out" pay period will not be considered in determining vacation "cash-out" eligibility. All "cash-outs" must be in increments of 8-hours only. No partial days will be accepted.

Employees who want to take advantage of this benefit must have at least 240-hours remaining in their accrual balance after the "cash-out".

Vacation "cash-out" requests must be submitted through completion of the "Vacation Cash-Out Form" to the payroll department during the collection-reporting period for the second pay period in June. A copy of the completed form will then be forwarded to Human Resources to be included in the personnel files.

The payroll department has the authority to make necessary adjustments in an employee's "cash-out" request if the "cash-out" hours have been incorrectly requested (i.e., the number of "cash-out" hours is greater than the number of "cash-out" hours available).

Vacation "cash-outs" are wages and subject to all taxes and payroll deductions. "Cashed-out" vacation days cannot be reinstated.

3.5 Donation of Sick Leave

Revised 1/1/05; Revised 4/22/2013

Purpose

To allow employees to donate sick time to another employee that is in need due to long-term medical situations.

Policy

Employees requesting/receiving donated sick leave must have completed the first 90 days of employment, be eligible for Family Medical Leave and be under the care of a physician for a serious health condition, or caring for their spouse, child or parent who is under the care of a physician for a serious health condition. **The employee receiving the donated leave must have less than 32 hours of combined sick and vacation leave benefits available at the time of the donation.**

The employee donating the leave must have a minimum of 240 sick leave hours remaining after the donation. An employee may not donate more than 20 hours per pay period per recipient or donate more hours than is needed by a recipient.

Donated leave will be applied as needed up until the employee no longer qualifies for this benefit. The Human Resources Department will monitor the allocation of donated time.

Unused donated leave cannot be returned to the employee making the donation.

Employees wishing to donate leave to another employee should contact the Human Resources Department for information and processing.

3.6 Employee Referral Bonus Program

Effective 11/1/00, 7/1/15; Revised 8/1/08, 12/9/2008, 6/4/12, 6/23/12,1/27/15

The referral program encourages current employees to help the Agency attract and recruit the highest caliber of candidates and rewards them for their efforts.

Policy

For each new regular, full-time certified Paramedic, EMT and certified EMD candidate (certification from the International Academies of Emergency Dispatch) an employee identifies and successfully helps Medic recruit, hire, and retain, a bonus will be paid. The Paramedic/EMD referral will be paid in two installments, providing that both parties are still employed at Medic and in good standing. The first portion will be paid after the referred employee is released from their FTO/CTO. The remaining balance will be paid upon the referred employee's one-year employment anniversary. The EMT referral will be paid once the employee is released from their FTO to function independently.

In order to be identified as being referred, the new hire must name the employee on their Hiring Application. The employee making the referral must be employed with the Agency at least 90 days prior to the date of hire of the referred to be eligible to receive the referral bonus.

If two or more individuals have had a significant involvement in referring an individual whom Medic hires, the Agency reserves the right to split the bonus amount between the involved parties, in whatever manner it deems appropriate.

Members of management (supervisors, managers and directors) and Human Resources personnel directly responsible for recruiting are not eligible to receive referral bonuses, with exception of the EMT referral. Medic employees are not eligible to receive a bonus for candidates they refer that will fall under their supervision. These individuals are encouraged to refer candidates, but will not be eligible for bonuses.

Employees returning to Medic or staff members changing their status from part-time to full-time are not considered new full-time employees in this program. In the event that a newly hired employee is terminated, transferred or demoted before the time of payout, the referral bonus will be forfeited.

The employee referral bonus will only be authorized if budgeted funds are available. Account balance shall be monitored monthly to ensure availability of funds.

Bonuses will be considered normal income and are therefore taxable.

3.7 Holiday Time

Effective 11/1/02; Revision 5/18/10, 8/7/15, 9/15/17, 07/01/2021

Purpose

This policy provides guidelines for holiday wage compensation, which assists to assure proper staffing on holidays.

Policy

1. The Utilization Coordinator determines whether to keep the staffing at normal levels for that weekday or operate with an adjusted staffing pattern on the holiday based on analysis of past historical data.

2. Official Agency holidays are as followed

    - New Year's Day
    - Martin Luther King's Birthday
    - Good Friday
    - Memorial Day
    - Juneteenth Day
    - Independence Day
    - Labor Day
    - Veterans' Day
    - Thanksgiving Day
    - Day after Thanksgiving
    - Christmas Day
    - Two other day at Christmas (as designated by Mecklenburg County)

3. Holiday Hours' Accrual or Payment

    a. Employees subject to working holidays (EMTs, Paramedics, Operations Support Techs and Telecommunicators) will be eligible for eight (8) hours of holiday leave accrual or pay for each Agency holiday recognized.

3.8 Bereavement Pay

Effective 1/1/99, Revised 01/2022

Purpose

This policy provides guidelines for bereavement pay for active full-time employees that have a death in their immediate family.

Policy

Eligible employees will be granted time off to remember the family member that has passed. Employees will be paid their regular pay (excludes any premiums) for up to 24 consecutive regularly, scheduled work hours. Part time and temporary employees are not eligible for this leave. Bereavement leave is available after 90 days of employment.

Immediate family is defined as the employee's:

- Legal Spouse;
- Biological parent or an individual who stood in loco parentis* to an employee;
- Biological, adopted, foster child, stepchild, a legal ward or a child of a person standing in loco parentis;
- Brother, sister;
- Grandparent, great-grandparent, grandchild;
- Mother-in-law, father-in-law, sister-in-law, brother-in-law, daughter-in-law, son-in-law;
- Spouse's grandparents, spouse's great-grandparents;
- Step relationships to include siblings, parents, grandparent and children.

The department supervisor and/or manager may require reasonable proof of the employee's eligibility. With the approval of the department manager, any additional time off for a death of a close relative may utilized – sick, vacation or leave without pay.

*in loco parentis is defined as a relationship in which a person puts him or herself in the situation of a parent by assuming and discharging the obligations of a parent to a child.

3.9 Jury Duty and Witness Time
Effective 1/1/99, 4/1/21

Purpose
To provide guidelines for Agency employees who are requested to serve on a jury or are subpoenaed as a witness.

Policy
1. The Agency recognizes that every employee has an obligation to perform the functions of citizenship, such as voting, military service, and jury service. The Agency will grant employees time away from work to serve on jury duty and will pay the employee full salary for the time away from the job. The employee receiving notice of call for jury duty should immediately provide a copy of the notice showing the date and court of jurisdiction to their supervisor and the Human Resources Department. Failure to do so will result in disciplinary action.

2. The Agency will not seek to have employees excused from jury duty unless their job duties cannot be temporarily delegated to someone else and their absences would adversely affect the services rendered by the Agency.

3. Compensation received for jury duty shall be retained by the employee.

4. Any employee who is required (subpoena) to appear in court or at another legal proceeding as a witness in an Agency work-related case/incident in a State or Federal court proceeding in which the employee is not a party will receive his/her pay for any of those hours that require an absence from his/her regular work.

5. Employees who are required (subpoena) by law to appear in court or at another legal proceeding for a non-work related case/incident will be provided time off for that purpose. Employees will not be compensated for time off to serve as a witness.

3.10 Paramedic Training Education Assistance Program
Revised 11/1/04

Purpose
To provide qualified Agency EMTs with an on-site paramedic training program designed to increase the knowledge and training of the Agency's EMTs and the overall expertise of the Agency, improve the Agency's recruitment and retention efforts and provide EMTs with opportunities for professional and personal growth. It is the Agency's intention that the Program qualify under IRS Code § 127 as an educational assistance plan so that benefits provided to employees are eligible for exclusion from the employee's income.

Definitions
For purposes of this Policy, the following definitions will apply:

1. "Agency" means the Mecklenburg Emergency Medical Services Agency.

2. "Benefits" means the direct payment or reimbursement of Covered Costs incurred by a Participant for the Program.

3. "Covered Costs," means the tuition, fees and similar payments and the cost of books paid for or incurred by a Participant in the Program. Covered Costs shall not include the cost of any tools or supplies purchased by a Participant or the cost of meals, lodging or transportation incurred by Participant incidental to the Program.

4. "EMT" means an emergency medical technician as that term is used and defined under applicable North Carolina law and regulations.

5. "Participant" means any employee of the Agency who satisfies the eligibility requirements of the Program and is selected to participate in the Program.

6. "Program" means the Agency's on-site paramedic training program.

Eligibility
Each Program Participant Must:

1. Be a current full-time Agency employee in good standing;
2. Have been employed by the Agency as a full-time EMT for not less than ninety (90) days prior to application;
3. Pass an entrance examination approved by the Agency;
4. Meet the Agency's current assessment criteria;
5. Have and maintain an exceptional work history and positive performance ratings;
6. Possess an EMT-D certification and a clean DMV record;
7. Complete an application of interest available in the Agency's Human Resources Department;
8. Be selected for participation in the Program and enter into a Paramedic Training Program Participation Agreement; and
9. Comply with the Agency's attendance policy, attend all Program classes and meet or exceed minimum Program requirements. The Agency reserves the right to remove any EMT from participation in the Program at any time and for any reason.
10. Sign a consent form authorizing Program Sponsors and instructors to release employees' Program grades and education records to the Agency.

Participants who are no longer employed by the Agency or who otherwise fail to meet the foregoing eligibility requirements shall be automatically disqualified from further participation in the Program.

Benefits:

1. Participants will continue to be paid their current salary during the term of the Program.
2. All Covered Costs of the Program shall be paid by the Agency, subject to the following conditions and limitations:

    a. Participants who complete the Program, are certified as a paramedic, and who are offered full-time employment as an Agency paramedic are obligated to continue their employment with the Agency as a full-time paramedic for a period of not less than two (2) years;

    b. Participants who: (i) fail to complete the Program for any reason (except for the Participant's death or disability or termination of the Program by the Agency); or (ii) decline the Agency's offer of employment as a paramedic upon completion of the Program; or (iii) accept employment with the Agency as a paramedic upon completion of the Program, but fail to complete the minimum two (2) year service requirement, shall be required to reimburse the Agency for tuition and training costs; and

    c. All Participants will be required to sign a Participation Agreement and Promissory Note, as well as other documents acknowledging minimum service commitments and repayment requirements.

3. In accordance with IRS Code § 127, a Participant may not receive more than $5,250 per year in Benefits under the Program. Any Participant who receives more than this amount in Benefits may be subject to taxation of any amount in excess of the Benefits received.

Miscellaneous:

1. This Policy does not constitute a contract of employment with the Agency.
2. The Agency reserves the right to interpret, enforce, change or terminate the Program and the rules and regulations of the Program, and to decide all questions concerning the Program and the eligibility of any person to participate in the Program.
3. Participation in the Program is a privilege to be afforded to EMTs who meet or exceed qualifications established by the Agency. The number of Participants selected will be based upon the number of available positions, the number of eligible applicants, the Agency's needs, individual merit and other factors determined by the Agency.
4. All applicants who are not selected for participation in the Program will be told the specific reasons for the denial. Applicants who wish to appeal the denial must follow the Agency's grievance procedures. The decision of the Agency Executive Director shall be final and binding.
5. The Program shall be construed and enforced in accordance with the laws of the State of North Carolina to the extent not preempted by federal law.

3.11 Relocation Benefit

Effective 1/1/00, 7/1/15; Revised 8/1/08, 11/18/08, 6/26/12, 1/1/15, 1/27/15

The relocation benefit helps the Agency attract and recruit the highest caliber candidates for the designated positions and assists new employees with their employment transition.

Policy

A relocation benefit has been implemented to encourage and facilitate the recruitment and retention of qualified candidates for full-time certified Paramedic and Emergency Medical Dispatcher positions.

- A benefit of up to $2,500 has been implemented to reimburse eligible moving expenses for Paramedics and EMDs (certification from International Academies of Emergency Dispatch). The relocation benefit breaks down as follows:
    - Paramedics/EMDs moving 100-1000 miles: up to $1,500
    - Paramedics/EMDs moving 1001+ miles: up to $2,500

All requests for relocation must have copies of receipts and be consistent with the IRS guidelines.

By accepting relocation funds from the Agency, the recipient agrees to commit to one-year of full-time service. Any employee that voluntarily terminates employment sooner that one-year from the date funds are given, will be required to immediately repay the Agency at 50% of the total amount received.

Relocation benefits are for selected and hired applicants who relocate to the greater Charlotte area from 100 or more miles away. This benefit is payable after (3) months of service, as long as the individual is still employed by the Agency and in good standing.

- Candidates traveling by personal vehicle will be reimbursed at the federal mileage reimbursement rate.
- Candidates traveling by rental will be reimbursed up to the price of an economy sized vehicle. *Should you request, or require a larger vehicle, pre-approval from a member of human resources is required.*
- Reimbursement for hotel accommodation(s) will be capped at the IRS per diem rate. Candidates traveling by air will only be reimbursed for coach class airfare. *Should you request, or require additional room accommodation, pre-approval from a member of human resources is required.*

The relocation benefit will only be authorized if budgeted funds are available. Account balance shall be monitored monthly to ensure availability of funds.

3.12 Service Awards

Effective 10/1/99

Purpose

Medic believes continuing service of employees is an asset to the Agency and so recognizes length of service on an annual basis.

Eligibility

All active full and part-time employees are eligible for Service Awards provided they have completed at least five years of service at the time the Award Program is held (during the fall of each year) and is still employed with the Agency.

Procedure

For every 5 years of continuous service, the Agency will provide Service Awards. The value of each award will depend upon the number of years being celebrated.

3.13 Sick Leave
Revised 7/1/04, Revised 1/2/18

Purpose
The purpose of this policy is to provide full-time and part-time employees with some measure of relief from the financial burdens caused by loss of earnings during periods of personal illness during regularly scheduled shifts.

Policy
Sick leave is not intended to provide time off for recreation, personal reasons, or extended vacations.
t

Agency employees accrue sick leave biweekly at the following rate:

SHIFT	PER PAY PERIOD	ANNUAL
40 hr	3.69 hours	95.94 hours

There is no maximum accrued limit.

After the first ninety (90) days of employment, sick leave may be used.

a. Sick leave may be used for the illness of the employee or the employee's immediate family.
b. Employees may be required to run sick leave concurrently with family and medical leave.

Employees who have creditable service in the NCLGERS (State Retirement System) are eligible to have up to 96 hours of earned unused sick leave transferred to the Agency. Proper documentation of accrued sick leave from the previous employer is required.

Employees who terminate from the Agency will be paid 25% of all remaining accrued sick leave. Employees may be paid less than 25% under special circumstances by written request i.e., transfer of time to another agency. If the employee is leaving employment due to a medical disability and the employee's physician has stated in writing that the employee will be incapacitated for a period of time that will exceed the number of accrued days, the employee may be paid 100% of the accrued sick days.

3.14 Sign-On Bonus

Effective1/1/00, 7/1/15; Revised 7/1/03, 11/1/07, 8/1/08, 6/4/12, 6/26/12, 1/27/15, 02/01/2022

Purpose

The sign-on bonus program helps the Agency attract and recruit the highest caliber of candidates for certain designated positions and assists the new employee with the employment transition.

Policy

Sign-on bonuses are available to new hires that have not previously worked for the Agency, or at the discretion of the Agency may be available to rehires.

In the event that a newly hired employee is terminated, transferred or demoted before the time of payout, the sign-on bonus will be forfeited.

Bonus payments are taxable compensation and subject to appropriate tax reporting and withholding.

Certified Paramedics/EMTs

A sign-on bonus has been implemented to encourage and facilitate the recruitment and retention of qualified Paramedics and EMTs.

Paramedics and EMTs hired for a full-time or part-time bonus-designated position will be eligible for an initial payout upon their release from their FTO, with the remaining balance payable upon their one-year employment anniversary, as long as the individual is employed by the Agency and is in good standing.

Certified Emergency Dispatchers (EMD – Certification through International Academies of Emergency Dispatch)

A sign-on bonus has been implemented to encourage and facilitate the recruitment and retention of certified EMDs.

EMDs hired for a full-time, bonus-designated position will be eligible for the initial payout upon the release from their CTO, with the remaining balance payable upon their one-year employment anniversary, as long as the individual is employed by the Agency and is in good standing.

The sign on bonus will only be authorized if budgeted funds are available. Account balance shall be monitored monthly to ensure availability of funds.

Bonus payments are taxable compensation and subject to appropriate tax reporting and withholding.

3.15 Worker Compensation/Reassignments

Effective 1/1/99; Revised 1/23/2013

Purpose

To outline use of sick leave after a work-related injury and the assignment of temporary light duty shifts that may be available.

Policy

1. If an employee is unable to work due to a work related illness or injury, he/she may use accrued sick, vacation/holiday pay during the first seven (7)-calendar day waiting period. These benefits can also be used to supplement the Workers Compensation payment after it begins up to the amount of the employee's normal gross pay. If the injury results in a disability of more than twenty-one (21) days, the Workers Compensation shall be allowed from the date of the disability at a rate established under State Law. The Agency may require the employee to take FMLA, Workers Compensation or leave concurrent with Disability leave.

2. If the employee is released for light duty, he/she must contact Human Resources Risk & Safety office immediately with the appropriate medical release from the treating physician for possible temporary reassignment of light job duties.

3. When reporting for any light duty assignments, the Occupational Health Nurse or Risk & Safety Specialist will coordinate and schedule working hours according to the Agency's needs which may not necessarily be the same hours as the employee is accustomed to. The employee will maintain time keeping records for any temporary assignment.

4. Approved light duties may be assigned but will remain within the employee's injury restrictions.

5. At the discretion of the Agency, the Risk & Safety office will monitor the number of light duty workers based on need or demand.

3.16 Wellness Leave Benefit

Effective 07/01/2022

Purpose

Wellness leave is extended to eligible employees for the purpose of compensated time away from their regular work assignment.

Policy

Two (2) wellness days are granted at the beginning of each fiscal year to all full-time, regular employees for use after the initial ninety (90) calendar days of employment. Part-time and temporary employees are not eligible for wellness leave.

Wellness leave will be automatically applied to eligible employees' wellness bank on or near July 1 each year. This leave is to be used in full day increments, one day should cover a regularly scheduled shift for the employee. Any wellness leave not used by the end of the fiscal year will be forfeited and not rolled over to the next fiscal year. Wellness leave is not eligible for pay out at time of separation, as part of the vacation cash-out program, and cannot be used to add creditable service time into the LGERS system.

Process for Requesting the use of Wellness Leave

Wellness leave cannot be used for sick leave call-outs. It must be scheduled and approved in advance of the leave dates.

Wellness leave may be requested up to twelve months in advance from the date the request is being made. All requests are to be in writing or requested through the appropriate timekeeping software process, and submitted to the employee's Supervisor or Scheduling contact (for Operations employees). Wellness leave requests must be received no later than two weeks prior to the requested date. This is to ensure that proper coverage can be arranged and/or that staffing levels will not be negatively affected. Any exception to the two-week minimum requirement must be due to extraordinary circumstances and will be reviewed by management on a case-by-case basis. So long as the proper request is utilized, wellness leave may be used in conjunction with approved vacation leave.

Due to operational needs each department may differ with benefit leave approvals. All employees must consult with their department supervisor, manager or director for specific departmental policy prior to making plans for time off.

Chapter 4 – Leaves of Absence

4.1 Family Medical Leave Act

Revised 6/1/04, 7/1/05, 8/1/07, 10/9/09; 1/31/14

Purpose

To comply with the Family and Medical Leave Act (FMLA) of 1993.

Policy

In accordance with the Family Medical Leave Act that went into effect on August 5, 1993 and most recently amended by the National Defense Authorization Act for FY 2010 ("NDAA"), the Agency provides eligible employees up to twelve (12) weeks of leave for family and medical reasons and twenty-six weeks (26) for two types of military family leave.

Eligibility

Employees are *covered* by the FMLA when they are employed at a worksite that has 50 or more employees within a 75 mile radius. Eligible employees must have (a) worked for the Agency for at least 12 months, and (b) worked at least 1250 hours in the last 12 months.

Reasons for Leave: Eligible employees may take family/medical leave for any of the following reasons: (a) the birth of a son or daughter and in order to care for such son or daughter; (b) the placement of a son or daughter with the employee for adoption or foster care; (c) to care for a spouse, son, daughter, parent, or next of kin with a *serious health condition*; (d) because of their own *serious health condition* which renders the employee unable to perform the essential functions of the position, or (e) because of a qualifying exigency arising out of the fact that the employee's spouse, son/ daughter or parent is on covered active duty or called to covered active duty status in support of a contingency operation as a member of the National Guard or Reserves and the Regular Armed Forces.

Leave because of reasons (a) or (b) above must be completed within the 12-month period beginning on the date of birth or placement.

A *serious health condition* is defined as:

- A condition that requires inpatient care at a hospital, hospice or residential medical care facility,
- Any period of incapacity or any subsequent treatment in connection with such inpatient care, or
- A condition that requires continuing care by a licensed health care provider.

Generally, a *serious health condition* is one that results in a period of 3 consecutive days of incapacity with the first visit to the health care provider being within 7 days of the onset of the incapacity and a second visit within 30 days of the incapacity. For chronic conditions requiring periodic health care visits for treatment, such visits must take place at least twice a year.

Married Couple Both Employed at the Agency: If a husband and wife are both Agency employees and each wishes to take leave for the birth of a child, adoption or placement of a child in foster care, or to care for a parent (but not a parent "in-law") with a serious health condition, the husband and wife may only take a combined total of 12 workweeks of leave. The leave must be taken within twelve (12) months of the birth or placement of the child. If a husband and wife are both Agency employees and each wish to take leave to care for a covered injured or ill service member, the husband and wife may only take a combined total of 26 workweeks of leave.

In accordance with the National Defense Authorization Act:

- Eligible employees may take up to 12 weeks family medical leave for a *qualifying exigency* related to a military member on covered active duty or who has been notified of an impending call or order to covered active duty. Covered family members include spouse, parent, and child; or

- An eligible employee who is the spouse, son, daughter, parent, or next of kin of a military member shall be entitled to a total of **26 workweeks** for military related medical treatment to care for the service member. Under the caregiver leave the twelve month period will be calculated rolling forward from the first day of leave.

The *qualifying exigency* must be for one of the following:

- Short-notice deployment
- Military events and related activities
- Child care and school activities
- Making/updating financial and legal arrangements
- Counseling
- Rest and recuperation (up to 15 calendar days)
- Parental care
- Post-deployment activities, and
- Additional activities that arise out of covered active duty, provided that the employer and employee agree on the timing and duration of the leave.

Military Caregiver Leave: An eligible employee can take up to 26 *workweeks* in a *single* 12 month period. However, only 12 of the 26 *workweek* total may be for a FMLA qualifying reason other than to care for a covered service member. The *single* 12 month period begins on the first day that the employee takes military caregiver leave and ends 12 months later.

Light Duty: Employees who accept light duty assignments while recovering from a serious health condition will not be charged with FMLA leave while performing light duty, provided the Employee has not exhausted his/her twelve (12) week annual FMLA allotment at the time light duty commences.

Calculation of Leave Allowable: To determine eligibility of an Employee for FMLA leave, the Agency will, at the time of the Employee's request, use the "rolling backward" method. With the rolling backward method, each time an employee takes FMLA leave, the remaining leave entitlement at that time would be the balance of the twelve (12) weeks that has not been used during the immediately preceding twelve (12) months; i.e., we will take a "snap-shot" of the preceding twelve (12) months to determine how much of the twelve (12) week leave time has already been used and then allow for the remainder to be used with the current request for leave.

Intermittent / Reduced Schedule Leaves: Family and Medical Leave need not always be taken in one continuous leave period. Leave may be taken "intermittently" or on a "reduced schedule" basis when medically necessary and with prior Agency approval. Generally, intermittent leave is leave taken in separate blocks of time due to a single illness or injury, rather than for one continuous period of time. Reduced schedule leave is leave that reduces an Employee's number of scheduled working hours per day or per week. Employees must make reasonable efforts to schedule leave for planned medical treatment so as not to unduly disrupt the Agency's operations.

When planning medical treatment, a Employee should consult with his/her supervisor and his/her healthcare provider before scheduling treatment, in order to determine the schedule that

least disrupts the departmental schedule while allowing the Employee to receive medical treatment. Leave due to qualifying exigencies may also be taken on an intermittent basis.

In the case of the birth or placement of a child by adoption or foster care, an intermittent or reduced schedule leave may be approved by the Employee's supervisor if staffing and workload permit. Intermittent or reduced schedule leave to care for a qualified sick family member or for an Employee's own serious health condition will be approved if the leave is medically necessary. When intermittent or reduced leave is requested, the Agency may require the Employee to transfer temporarily to an alternative position which better accommodates recurring periods of leave or a reduced schedule, provided that the positions have equivalent pay and benefits.

Procedure for Requesting Leave: Employees desiring to take Family and Medical Leave must give at least thirty (30) days advance notice prior to commencement of leave if the need for leave is foreseeable. If thirty (30) days' notice is not possible, the Employee must give as much notice as possible under the circumstances and comply with the Agency's call-in procedures. Failure to comply with the Agency's normal and customary FMLA notice and procedural requirements may result in delay or denial in FMLA leave.

FMLA Request Form: An Employee must complete an FMLA Request Form. The request must describe and provide sufficient information, including the anticipated timing and duration of the leave, for the Agency to determine if the leave may qualify for FMLA protection. The Employee must also inform the Agency if the requested leave is for a reason for which FMLA leave was previously taken or certified. A sample FMLA Request Form is attached as **Exhibit A**.

Certification of Physician: A Certification Letter from the healthcare provider must be provided for any leave request based on a qualifying family member's or Employee's own serious health condition. The Employee should see Human Resources to request copies of the application forms including the Healthcare Provider Certification Letter.

The Agency's FMLA Application will identify the *due date* for the Healthcare Provider Certification Letter. The *due date* will be no less than 15 calendar days from when you receive the certification letter form. Failure to provide a complete and sufficient medical certification, in a timely fashion, may result in a denial of your FMLA request.

Certification from the healthcare provider must contain, at a minimum:

1. The date the serious health condition began;

2. The possible duration of the condition;

3. The appropriate medical facts regarding the condition;

4. If the leave is based on the care of a spouse, child or parent, a statement that the Employee is needed to provide care and an estimate of the amount of time that need will continue;

5. If the leave is based on the Employee's own serious health condition, a statement that the Employee is unable to perform the essential functions of his/her job; and

6. In the case of intermittent leave or leave on a reduced hour basis for planned medical treatment, the date the treatment(s) is expected to be given and the duration of the treatment(s).

A sample Certification Letter is attached as **Exhibit B**. If the Agency believes that the Certification requires clarification or authentication, or is otherwise inadequate, the Agency HR Manager may contact the physician to obtain additional information, provided the Agency has first given the Employee written notice of any deficiency in the certification and seven (7) days to cure the deficiency.
The Agency also reserves the right to require certification from a covered military member's health care provider if you are requesting military caregiver leave and certification in connection with military exigency leave.

Second Opinion / Recertification: The Agency may, at its own expense, require the Employee to provide a second or third opinion from a healthcare provider if the Agency reasonably believes the Employee's request for leave is not properly substantiated. Second opinions and recertification will not be required for covered service members.

In certain situations, the Agency may ask for Recertification. If the initial Certification specifies a period of incapacity that is greater than thirty (30) days, the Agency will not request a Recertification until the initial period has passed. In all cases, the Agency may request Recertification at least every six (6) months. Additionally, in the case of intermittent leave, the Agency may ask the Employee to provide a fitness-for-duty certification every thirty (30) days if the Employee has used intermittent leave during that period and reasonable safety concerns exist.

Notice of Eligibility: The Agency will provide the Employee with a Notice of Eligibility and Rights & Responsibilities Letter within five (5) business days of receiving the Employee's request for leave under the FMLA. The Notice will notify the Employee of his or her eligibility to take FMLA leave as well as his or her rights and responsibilities under the FMLA. The Notice may also detail additional information required from the Employee regarding his or her leave request. A sample Notice of Eligibility is attached as **Exhibit C**.

When the Agency has enough information to determine that the leave is being taken for an FMLA-qualifying reason, the Agency will provide the Employee with a Designation Notice. The Designation Notice will inform the Employee that the leave will be designated as FMLA-protected and the amount of leave to be counted against his or her FMLA leave entitlement. The Agency will provide the Employee with a Designation Notice within five (5) business days after the Agency determines whether the leave requested qualifies as FMLA leave. A sample Designation Notice is attached as **Exhibit D**.

Requirement to Exhaust Paid Leave: Employees are required to use and exhaust all accrued paid time off (PTO) concurrent with FMLA leave. Once all PTO is exhausted, the remaining leave will be unpaid and be considered Leave Without Pay (LWOP). The substitution of paid leave time for unpaid leave time does not extend the allowable applicable leave period. While on leave, Employees may not accrue PTO, including workers' compensation and/or disability leave.

Benefits Continuation While on Leave: An Employee on an approved FMLA may continue group health insurance coverage during the leave upon the same terms in place for all similarly situated employees who are not on FMLA leave.

In the event the Employee's right to payment is exhausted or payment is not adequate to cover the Employee's portion of the premium before the completion of the leave period, the insurance premiums, or portion thereof, normally paid by an Employee must be paid directly to the Agency during the time in which the Employee does not receive compensation. Premiums are due on a monthly basis, in advance of the coverage period.

The Agency will pay the individual life insurance premiums for Employees on LWOP status if they have at least five (5) years of service in the North Carolina Local Government Employee Retirement System or if they are receiving Workers' Compensation benefits.

An Employee's failure to pay his/her portion of the insurance premiums owed for dependent / spouse coverage will result in termination of the coverage after proper notice, at the end of thirty (30) days following commencement of the leave, or at the end of thirty (30) days following the date premiums became due.

An Employee who fails to return to work following FMLA leave is required to reimburse the Agency for premiums paid by the Agency to continue the employee's insurance coverage during the unpaid portion of the leave. This does not apply if the Employee is medically unable to return to work.

Additional Voluntary Benefits Continuation While on Leave: An Employee on an approved FMLA may continue his or her voluntary participation in other benefits programs, including but not limited to 401K, Roth IRA, Supplemental Life Insurance, Dependent Life Insurance, AFLAC, Flexible Spending Account, Dependent Care Account, Vision and Dental, offered by the Agency during the leave upon the same terms in place for all similarly situated employees who are not on FMLA leave.

In the event the Employee is on LWOP or the Employee's payment is not adequate to cover the Employee's portion of the premiums for participation in these voluntary benefits programs before the completion of the leave period, the premiums normally paid by an Employee must be paid directly to the Agency during the time in which the Employee does not receive compensation. Premiums are due on a monthly basis, in advance of the coverage period.

An Employee's failure to pay his or her portion of the premiums owed for his or her participation in these voluntary benefits programs will result in termination of the coverage after proper notice, at the end of thirty (30) days following commencement of the leave, or at the end of thirty (30) days following the date premiums became due.

Accrual of Benefits While on Leave: Vacation, sick leave and accrued holiday time will not continue to accrue during any portion of a FMLA leave that is unpaid. However, Employees retain benefits accrued prior to but not used during the leave.

Reinstatement Upon Return From Leave: Eligible Employees will be reinstated to their former position, or to an equivalent position, with equivalent pay, benefits, and working conditions upon return from FMLA in accordance with these guidelines. If an Employee has been on leave due to his/her own serious health condition, a fitness for duty statement will be required to determine whether the Employee can perform the essential functions of the job.

However, reinstatement is not always required for certain highly compensated "Key Employees". If the Agency determines that reinstatement of a Key Employee would cause substantial and grievous economic injury to the operations of the Agency, reinstatement may be denied.

An Employee requesting FMLA leave will generally be notified, at the time of the request if he or she is a "Key Employee." If such notice cannot be given immediately, because of the Agency's need to determine whether the Employee is a Key Employee, notice will be given as soon as practical after receipt of the leave request (or the commencement of the leave, if earlier).

If the Agency determines, after the leave has begun, that the Agency will not be able to reinstate the Key Employee at the end of the leave, the Key Employee will be notified by the Human Resources Department in writing, and the Key Employee will be given a reasonable time in

which to return to work. In such a case, the Key Employee's insurance coverage will continue in effect throughout the entire FMLA leave period.

Disability/Workers' Compensation Benefits: Employees on FMLA leave due to their own serious health condition may be eligible for payments from other sources such as Workers' Compensation or disability insurance. Employees should ask the Human Resources Department for more information if they think they are eligible for these benefits. The pay allowances while on disability leave are based on an Employee's length of service, as well as the laws of the state of employment.

Aggregate Date, Service Date and Annual Review Date: Employees who return from LWOP status will have their aggregate date, Agency service date and annual review date adjusted to reflect the time the Employee was actually off of the Agency's payroll.

Other Non-FMLA Leaves of Absence: Notwithstanding the FMLA policy outlined above, an Employee may qualify for other non-FMLA leaves of absence including Administrative Leave, Disaster Response Leave, Extended Family Leave, Extended Medical Leave, Military Leave and Parent-Child School Leave. However, none of these non-FMLA leaves of absence shall entitle an Employee to the FMLA-protected benefits detailed above including, but not limited to, Reinstatement upon Return from Leave and Benefits Continuation. Employees who qualify for FMLA leave may not automatically qualify for other non-FMLA medical leaves. Employee shall be required to apply and be approved for such leave independent of their FMLA-protected leave and will be subject to the terms and conditions of the applicable non-FMLA leave policy.

4.2 Administrative Leave (Leave without Pay for up to 30 days)

Effective 1/1/99, 12/9/09, 2/1/2010; Revised 1/23/2013

Policy

Administrative leave is leave without pay and may be granted for compelling personal reasons after the 90-day introductory period. The length of leave will be determined by the circumstances surrounding the situation but generally may not exceed 30 calendar days. Each case will be considered on its own merit.

Written request must be made to the supervisor stating the reason for the leave and the date of expected return. Final approval for the leave will be made by the department director.

Employees are responsible for all insurance premiums for individual and dependent coverage. Employees are also responsible for all premiums associated with the Employee's continued voluntary participation in other benefits programs, including, but not limited to 401K, Roth 401K, Supplemental Life Insurance, Dependent Life Insurance, ALFAC, Flexible Spending Account, Dependent Care Account, Vision and Dental, offered by the Agency.

In the event the Employee is on leave without pay status, or the Employee's payment is not adequate to cover the Employee's portion of the premiums for participation in these voluntary benefits programs before the completion of the leave period, the premiums normally paid by an Employee must be paid directly to the Agency during the time in which the Employee does not receive compensation. Premiums are due on a monthly basis, in advance of the coverage period.

No benefit time will be accrued while on leave without pay. This includes vacation, sick and holiday hours.

An Employee's failure to pay his or her portion of the premiums owed for his or her participation in these voluntary benefits programs will result in termination of the coverage after proper notice, at the end of thirty (30) days following commencement of the leave, or at the end of thirty (30) days following the date premiums became due.

Upon returning from leave without pay, employees will be offered a similar position to the one when going on leave, not necessarily the same shift and assignment. The employee may bid at the next shift bid for a new assignment.

Should an employee decide not to return at the end of Administrative Leave, they will be paid for all vacation leave and 25% of accrued sick leave (as defined in the sick leave and vacation benefit leave policies). Failure to return from Administrative leave will be considered a resignation.

4.3 Disaster Response Leave

Effective 1/1/99, Revised 3/1/06, 4/1/21

Policy

The Agency will recognize disaster relief operations as approved by the Executive Director.

1. Directed to Participate by the Agency - Employees directed by the Agency to participate in disaster relief efforts will be considered on-the-job and will be paid the same salary as working their regularly scheduled hours. There is no break in retirement service credit and all benefits will continue as normal. If the disaster operation is outside our service area, payment for travel time will be provided. Employees will be required to submit timekeeping records to the Agency as requested and any pay received from disaster relief sources must be turned over to the Agency.
2. Approved by the Agency - Recognized relief organizations such as SORT, MED1, SMAT, etc., may contact Agency departments to request specialized assistance with relief operations. These requests will require Deputy Director approval. Employees with approval to be part of these special operations are not considered to be on-the-job. Employees are encouraged to confirm, in advance, with the relief organization or program coordinator about pay, travel expenses, liability insurance and workers compensation, even if the relief organization operates on Medic property. Employees are not required to use accrued benefit leave during their absence. If the employee elects not to use benefit time, they will be placed on a leave without pay status. However, the employee is responsible for their portion of benefit premiums while out of work.
3. Volunteer Services – Employees may volunteer on an individual basis for disaster relief operations but are encouraged to inquire in advance with the program's coordinator about liability/disability insurance and any other coverage or benefit that may be provided to volunteers. These requests will require Deputy Director approval. These employees must use accrued vacation leave subject to the usual supervisory approval. If an employee does not have benefit time available, they will be placed on a leave without pay status. However, the employee is responsible for their portion of benefit premiums while out of work.

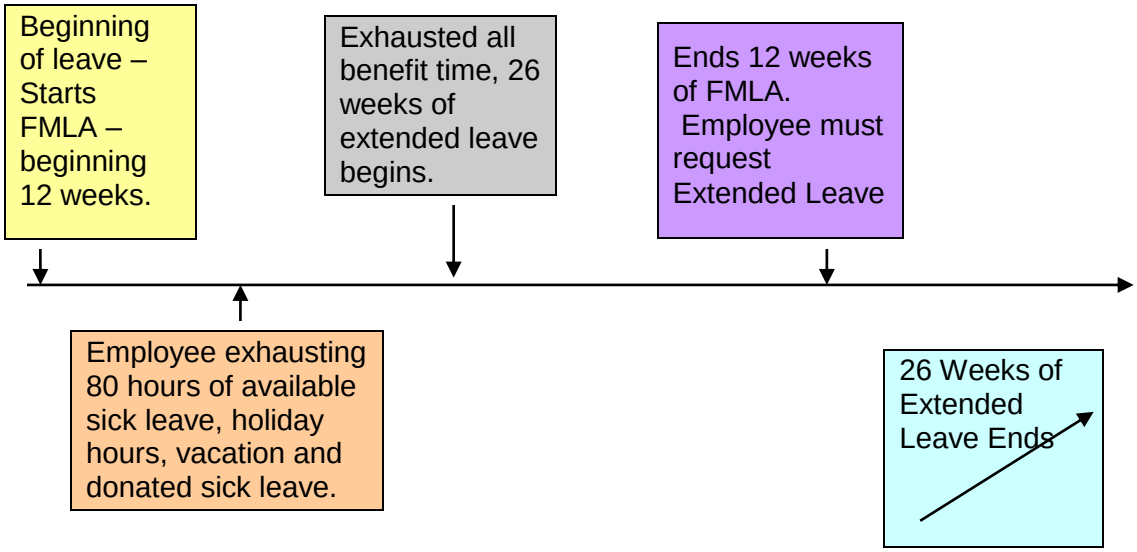
Note: Employees on leave for 90 or more days, must meet all applicable requirements of the Return to Full Duty Work program (4.9).

4.4 Extended Leave Without Pay (LWP) for more than 30 days
Effective 2/1/2010; Revised 1/23/2013; 4/18/2013

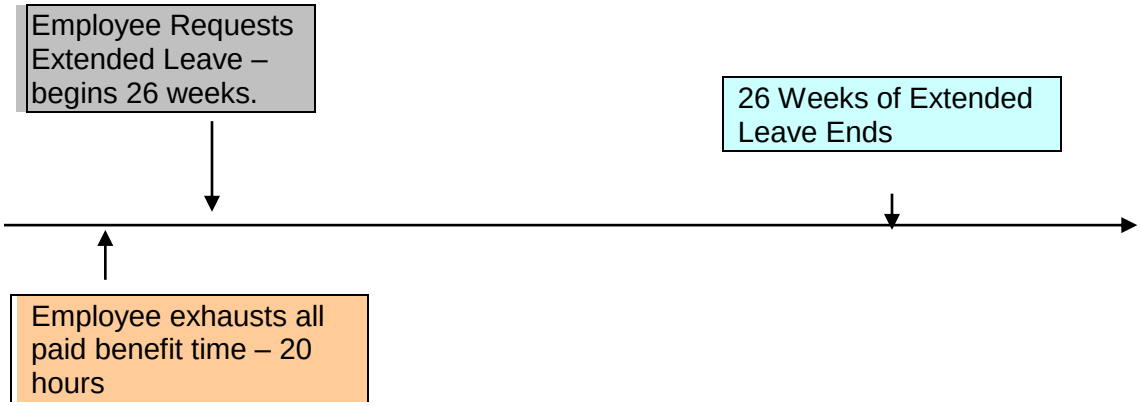
Policy
The Agency will grant eligible employees Extended Leave, leave without pay (LWP), for good and sufficient reason. Extended Leave will be considered for leave beyond FMLA and/or after the employee has exhausted all paid benefit time and donated sick time. If an employee is using benefit time to supplement short-term disability, the benefit time must be exhausted in order to be considered for LWP. Extended leave does NOT run concurrent to Worker's Compensation. (See Workers' Compensation Policy)

All regular, full-time employees are eligible to request Extended Leave. The Extended leave may be granted for up to a maximum of 26 weeks. (The 26 weeks may run concurrently with FMLA, but begins when paid time off is exhausted.)

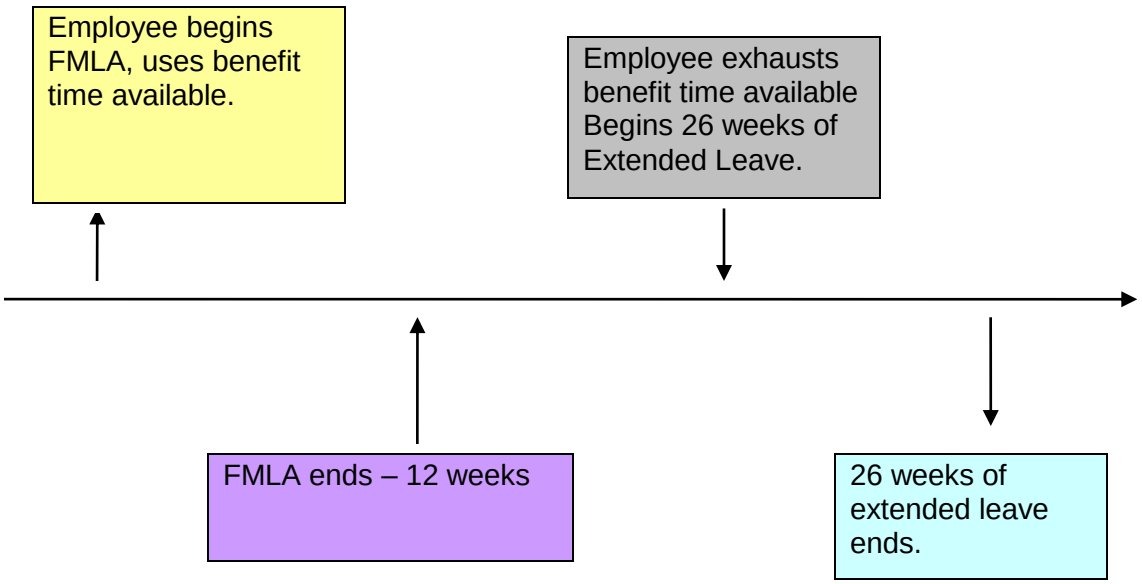
Example 1: Employee Eligible for FMLA, has some benefit time available.



Example 2: Employee Not Eligible for FMLA, has some benefit time available.



Example 3: Employee is eligible for FMLA and has 600 hours of benefit time available



The Employee shall be required to use and exhaust all appropriate benefit time; accrued Sick Leave (as defined in the Sick Leave Policy), Donated Sick Leave (as defined in the donation of sick leave policy), Holiday Time (as defined in the Holiday Time Policy) and Vacation Benefits Leave (as defined in the Vacation Benefits Leave Policy), in that order. Once all benefit time is exhausted, the remaining leave will be unpaid and be considered Extended Leave, or leave without pay (LWP). No benefit time will be accrued while on leave without pay. This includes vacation, sick and holiday hours.

Extended leave is intended to be taken in a block of time and will not be granted for intermittent leave. When an employee has exhausted the 26 weeks of allowable time, to be eligible to request an additional Extended Leave, an employee must have worked for the Agency for at least twelve (12) months since the previous Extended Leave ended and have worked at least 1,250 hours during the twelve (12) months prior to the onset of the leave period.
Requests for Extended Leave must be approved by the Department Director. Written requests and/or required documentation must be submitted to the department director for approval. Whenever possible, the request should be received by the department director at least 30 days prior to the beginning of the Extended Leave. The written request and/or documentation must be submitted to the Human Resources Department to be put in the employee's permanent personnel file.

An employee on *Extended Leave* is responsible for all individual and dependent medical and life insurance premiums. Premiums include both Medic and Employee *portions of the* premiums. *Employees are also responsible for all premiums associated with the Employee's continued voluntary participation in other benefits programs, including, but not limited to 401K, Roth 401K, Supplemental Life Insurance, Dependent Life Insurance, ALFAC, Flexible Spending Account, Dependent Care Account, Vision and Dental, offered by the Company.*

Employees on Extended Leave are responsible for payment to cover the Employee's and Medic's portion of the premiums for participation in these voluntary benefits programs before the completion of the leave period, the premiums normally paid by an Employee must be paid directly to the Agency during the time in which the Employee does not receive compensation. Premiums are due on a monthly basis, in advance of the coverage period.

An Employee's failure to pay the premiums owed for his or her participation in these benefits programs will result in termination of the coverage after proper notice, at the end of thirty (30) days following commencement of the leave, or at the end of thirty (30) days following the date premiums became due.

REPLACEMENT AND RETURN FROM EXTENDED LEAVE

Employees returning from Extended Leave will have their aggregate date, Agency service date and annual performance evaluation date adjusted equal to the amount of time they were actually off the payroll.

When the employee is on Extended Leave the employee's position may be filled if the employee is not otherwise eligible for FMLA leave. Upon returning from leave without pay, employees may be offered a similar position to the one when going on leave if available, but not necessarily the same shift and assignment. The employee may bid at the next shift bid for a new assignment.

Following a leave, the Agency reserves the right to ask for a completed physical ability assessment and/or be evaluated by a physician (to be approved by the Agency) prior to a full and unrestricted return to duty. Any assessment will be paid for by the Agency.

4.5 Leave of Absence Guideline
Revised 2/1/2010

TYPE OF LEAVE	**ELIGIBLE FOR LEAVE**	**MAXIMUM TIME**
Administrative	After first 90 days of employment (In some circumstances may be granted sooner)	Up to 30 Days
Bereavement hours	After first 90 days of employment	Up to 24 consecutive hours
FMLA *may run concurrently with workers comp & disability leaves	After 1 year of service with 1250 hours worked prior to leave	Up to 12 weeks
Extended Leave– May run concurrently with FMLA, begins after all appropriate benefit leave time has been exhausted.	Full time employees may request leave for good and sufficient reason	Up to 26 weeks of unpaid time off.
Parent-Child Leave	From date of hire	Up to 4 hours
Military/Disaster	As may be necessary or as directed by the Agency	
Note: For leave related events, the Agency reserves the right to ask for a completed physical ability assessment and/or be evaluated by a physician (to be approved by the Agency) prior to a full and unrestricted return to duty. Any assessment will be paid for by the Agency.		

4.6 Military Leave

Effective 1/1/99, Revised 5/1/05, Revised 4/25/16

National Guard, Reserve and Volunteer Training Leave

In accordance with the federal and state law, the Agency will recognize military training for National Guardsmen, reservists, and volunteers. The intent of these guidelines is to assure that employees will not earn less than they would have earned working in their normal position.

The Agency will supplement employees' military pay up to the amount that they receive for working their regularly scheduled hours. All military pay received during training, except for lodging and food; will be counted as base pay. Leave may be in consecutive days or spread out over the year, but may not exceed 10 days annually in order to be eligible for supplement.

In lieu of the pay supplement, the employee has the option to use accrued vacation or holiday leave. If accrued benefit leave is not used, the employee will be considered to be on Leave Without Pay status (LWOP). This means retirement credit is not earned and there is no accrual of benefits. Under normal circumstances, an employee leaving for annual training will continue to have the individual portion of medical and dental benefits paid by the Agency. An employee going to annual training will normally be on the job some work days in every pay period within a month; therefore, the Agency would pay for individual insurance coverage.

Employees are required to provide proof of military duty and to provide copies of the military orders and pay vouchers so the amount of the Agency pay supplement can be determined. This information will become part of the employee's permanent personnel file. Compensation will not be granted under this policy without proper documentation. The difference in pay between the military compensation and Agency compensation will be awarded after the employee returns to normal job duties.

Active Military Duty Leave

Leave without pay shall be granted for periods of active duty in the armed forces of the United States. Extended active duty is that period of time for which an employee is ordered to active military service under the following circumstances:

1. Voluntary enlistment
2. Call-up or order to federal or state active duty
3. Induction into active military service via Selective Service

The Agency will supplement employees' military pay for a specified time approved by the Agency's Management Committee up to the amount they receive for working their regularly scheduled hours excluding overtime and other compensation additions that may have been earned if the employee were on the job. Taxes will be deducted from the pay supplement. Other optional deductions will not be deducted. Supplemental pay will be direct deposited or mailed to the employee's home address.

Employees are required to provide proof of active military duty and copies of orders and pay vouchers so the Agency can determine the amount of pay supplement. This information will become part of the employee's official personnel record. Compensation will not be granted without proper documentation. The difference between military pay and Agency pay will be paid monthly, quarterly or annually after required documents are presented to the Human Resources Department.

Eligibility requirements for military pay supplement:

- Active military duty
- Leave without pay status from the Agency (not using vacation hours)
- Military pay is less than Agency pay
- Proof of active military duty, copies of orders and pay vouchers

Benefits for employees on active military duty will be affected as follows:

a. **Medical and Dental Insurance:** The Agency will continue to pay individual coverage for employees on military leave. During the time of the employee's leave, the Agency's medical and dental insurance will pay secondary to the Federal plan for non-service related injuries or illnesses. The federal government covers all service-related injuries and illnesses. If employees want to continue to cover their family members, they must mail a check to the Agency's Payroll Department by the first of each month for the amount of the dependent coverage. Dependent and/or spouse premiums will not be deducted from the supplemental pay. Once the employee returns from leave, payroll deduction for family coverage will be reinstated.

b. **Basic Term Life Insurance:** Even though there is no act of war exclusion, employees have to be actively at work to be covered by this benefit. However, our insurance provider is extending coverage to employees on military leave for 12 weeks. After this period of time, coverage can be converted to an individual plan for the duration of leave. Premiums after the 12 week period are paid by the employee directly to the provider. Employees should contact the Benefits Specialist in the Human Resources Department for *conversion* forms. Group coverage is reinstated upon return to work.

c. **Supplemental Term Life Insurance:** Even though there is no act of war exclusion, employees have to be actively at work to be covered by this benefit. However, our insurance provider is extending coverage to employees on military leave for 12 weeks. Since employees on Military Leave are not on the payroll, premiums should be paid by the employee directly to the provider. After the 12 week period, coverage can be converted to an individual plan for duration of leave. Employees should contact a Human Resource representative for *conversion* forms. Group coverage is reinstated upon return to work**.**

d. **Accidental Death and Dismemberment: *Does* *contain exclusion for acts of war.*** Coverage ends upon employee's last day of work. Coverage is reinstated upon return to work.

e. **Short Term Disability: *Does* *contain exclusion for acts of war.*** Coverage ends upon employee's last day of work. Coverage is reinstated upon return to work

f. **Retirement:** Retirement deductions will not be made from employees' supplemental pay. The Agency's contributions to the retirement system for these employees will also cease, but will not affect length of service in the retirement system if the employees complete Retirement System Form DD214 and request service credit for this time. Neither the employee nor the Agency is required to retroactively contribute to the retirement system.

g. **Vacation and Sick Leave and Holidays:** Accruals of these benefits will continue while the employee is in a military leave status.

h. **401k and 457 Deferred Compensation:** Voluntary and employer match/ contributions to both the 401k and 457 plans will cease. After the employees return from leave, they will be allowed to contribute retroactively to their accounts. If employees choose to do this, then the Agency will be required to contribute its match/contribution retroactively.

i. **Aggregate Date, Medic Service Date, and Annual Review Date:** These dates will not be adjusted for time off the payroll.

j. **Merit Increase:** If an employee's annual review date occurs while they are on active military leave, the employee will receive the average merit increase budgeted for the

year in which their review occurs. The increase is effective when the employee returns to active status.

A person returning from active military duty must apply for reinstatement within 90 days following military discharge. Failure to apply for reinstatement will be considered a voluntary resignation.

4.7 Parent-Child School Leave

Effective 1/1/99, 4/1/21

Purpose

To allow employees time off from work without pay for parent involvement in school activities.

Policy

The Agency will grant up to four hours of unpaid leave per year to any employee who is a parent, guardian or person standing in loco parentis of a school-aged child so that the employee can become involved in school activities. The following guidelines have been established for this policy:

1. The leave must be scheduled for a time that is mutually agreeable to the Agency and employee.

2. The Agency may require the employee to make a written request at least 48 hours before the leave begins

3. The Agency may require the employee to furnish written verification from the child's school that the employee attended or was involved in school activities during the time of the leave.

Note: Employees may opt to use vacation time for this period, if appropriately requested and approved.

4.8 Paid Family Leave
Effective 01/01/2018

Purpose
The Mecklenburg EMS Agency offers Paid Family Leave to employees who need to take time off work to bond with a new child entering their life by birth, adoption, or foster care placement, or to care for a seriously ill child, parent, or spouse.

Eligibility
To be eligible for Paid Family Leave, the employee must be a qualified employee under the Family Medical Leave Act (FMLA) and on approved FMLA Leave for one of the following reasons:

- To care for the employee's spouse, son, daughter, or parent who has a serious health condition;
- To bond with a newborn child within one year of birth; or
- To bond with a child following adoption or foster care placement within one year of adoption or placement.

Part-time, Limited Part-time and Temporary employees are not eligible for Paid Family Leave.

Policy
Benefit
Paid Family Leave will provide 100% of an employee's base compensation for up to 6 weeks. Employees may not use vacation, sick leave, or holiday pay while receiving Paid Family Leave. Employees cannot receive Short Term Disability while receiving Paid Family Leave. An employee may receive Paid Family Leave prior to obtaining Short Term or after Short Term ends.

Duration
Employees can receive up to six weeks of paid leave in a single continuous block. Paid Family Leave runs concurrent with FMLA Leave. If at the time the employee takes Paid Family Leave, the employee has less than six weeks of FMLA Leave remaining, the employee will only be eligible for Paid Family Leave up to the amount of FMLA Leave the employee has remaining.

An employee may only receive Paid Family Leave for one qualifying event within a rolling twelve-month period. The amount of paid family leave for any one person shall not exceed six weeks in a rolling twelve-month period. All leave must be completed within twelve months of the qualifying event.

If both parents are employed by the Agency and have one qualifying event, each parent is eligible for the six weeks of Paid Family Leave. Each parent can use their allocated six weeks of Paid Family Leave, either concurrently or consecutively.
Nonaccrual of benefit
Upon separation of employment, the employee shall not be eligible for payment for any unused Paid Family Leave.

Use
Employees are to use Paid Family Leave only for the reason(s) approved by the Agency. Use of Paid Family Leave for any other purpose violates Agency policy and may result in disciplinary action, up to and including termination.

Prohibition on Secondary Employment

An employee on Paid Family Leave cannot engage in outside or supplemental employment while on leave. Violation of this policy may result in disciplinary action, up to and including termination.

4.9 Return to Full Duty
Effective 9/2021

Policy
The Agency has a Return to Full Duty program for employees who have missed 90 or more days of work as a field provider due to an approved leave, modified duty, or failure to pick up shifts as a dual rolled employee.

The Return to Full Duty program provides employees with support from each applicable department in an effort to get the employee ready to return to their role as a field provider. The employee will have 14 days to complete each task unless otherwise advised. Any employee that does not complete each task may be subject to disciplinary action up to and including termination.

Employees that fall within this program will be placed in a transition status until they complete each required step of the Return to Full Duty process. This process will begin with Human Resources and the employee will return to their pre-leave field job functions once Human Resources verifies the completion of all required tasks. These tasks will vary based on the employee's job description and time on leave. Each employee will receive documentation, to include instructions, on how to navigate through the Return to Full Duty Work process.

Requirements for provider levels (EMT-B & EMT-P) are as follows:

1. Employees returning after 90-180 days must –
    a. Complete all deficient continuing education sessions, administrative and operation items.
    b. Successfully complete the Agency's local credentialing examination (Scope of Practice).
        i. Basic/Advanced complete Scope of Practice.
    c. May request to ride in a 3rd person status in order to re-acclimate to the field. This will be at the discretion of the operations management team.
2. Employees returning after 180-365 days must –
    a. Complete all deficient continuing education sessions, administrative and operation items.
    b. Successfully complete the Agency's local credentialing examination (Scope of Practice).
        i. Basic/Advanced complete Scope of Practice
        ii. Basic/Advanced psychomotor skills station
    c. Successfully complete the oral board examination as administered by the medical director or EMS fellow (Paramedics only).
    d. May request to ride in a 3rd person status in order to re-acclimate to the field. This will be at the discretion of the operations management team.
3. Employees returning after 365 or more days must –
    a. Successfully complete one of the following, based on their credentialing:
        i. State approved EMT Refresher course
        ii. State approved Paramedic Refresher course
    b. Successfully complete the Agency's local credentialing examination (Scope of

Practice).

i. Basic/Advanced complete Scope of Practice

ii. Basic/Advanced psychomotor skills station

c. Successfully complete the oral board examination as administered by the medical director or EMS fellow (Paramedics only).

d. Successfully complete all Field Training Officer (FTO) requirements within a maximum of a 4-week period.

Any field-credentialed employee who does not work as a field provider for 90 or more days must successfully complete the MEDPAT and all other requirements provided in this policy. Additional requirements can be found on the Return to Full Duty Work Form that will be provided to the employee upon return from leave status.

All other departments will provide employees returning from leave their department specific requirements.

These requirements are subject to change without notice.

Note: Employees on leave for 90 or more days due to their own medical condition must provide Human Resources with the appropriate return to work documentation prior to beginning this process. The Agency reserves the right to require a completed physical ability assessment and/or a fit for duty evaluation by an Agency approved physician prior to a return to full and unrestricted duty. The Agency will cover the cost of any fit for duty evaluation done by an Agency approved physician.

Chapter 5 – Payroll and Compensation

5.1 Employee Classification

Revised 2/1/05, 7/1/05, 5/1/17

Purpose

To define exempt and non-exempt employee classification as required by Federal statutes.

Definitions

Exempt:

Federal laws exclude certain employees from minimum wage and overtime pay requirements. In order to comply with the FLSA salary basis test, exempt employees regularly receive a predetermined salary amount each pay period. Exempt employees will work the number of hours necessary to fulfill their job responsibilities and do not receive additional wages for hours worked in excess of the scheduled hours. Full-time, exempt employees are expected to work an average of 40 hours a week. The Agency does not recognize compensatory time off for exempt employees.

Non-Exempt:

Employees not excluded from the provision of the laws are termed “non-exempt” and are subject to minimum wage and overtime regulations as set forth in the Federal Labor Standards Act (FLSA).

Full Time:

Employees who are regularly scheduled to work more than 32 hours per week are considered full time.

Part Time Permanent:

Employees who have transitioned over to the Agency from the County, work less than 32 hours per week and are eligible for benefits. These employees have been “grand fathered” in when the transition occurred.

For Field Employees going part-time:

In order to maintain a part-time status at Medic, you will need to adhere to the following:

- Work an average of 3 credits per month as defined in the part time policy.
- Stay current with all required continuing education.
- Stay current with all annual corporate compliance and HIPAA training.
- Stay current with all annual health screening requirements.
- Notify the staffing office if there are any issues regarding availability.

Should you request and be granted to return to work full time, your seniority for the purposes of any shift bids or promotions will be based on the date you returned full time. In addition, accruals for sick and vacation will be calculated at the starting time.

Part Time Temporary:

Employees who work a minimum average of 8 hours per pay period but not more than 40 hours per week. Part Time Temporary Employees are not eligible for benefits. This includes the loss of seniority in shift-bids.

Temporary Employees:

Employees who work for a temporary period of time to fill vacancies or to assist with special projects or assignments. Temporaries are generally assigned for no more than 3 months). Temporary employees are not eligible for benefits.

Introductory Employees:

Employees who are in their first 90-days of employment.

On-Call Compensation:
The premium for on-call pay is equivalent to one hour of pay at the employee's actual hourly salary rate and will cover a 24-hour period or any portion thereof. Exempt employees are not eligible for additional compensation if they return to work.

5.2 Employee Reassignments

Effective 2/1/2007

Purpose

To determine pay when moving to a new position with a lower pay grade assignment.

Policy

Reassignments are job changes for employees who move to a different position with a lower pay grade. Salary decreases due to reassignments may be at the discretion of the department director; however, salaries will not exceed the maximum of the new pay band. In considering a salary change, the department director should consult with a member from Human Resources, review the relationship of the employee's salary to the market rate of the new position, the employee's performance, and whether the reassignment is voluntary or involuntary.

5.3 Compensation Guidelines

Revised 7/1/05

Purpose

To ensure our market-based pay program reflects competitive pay practices of the different industries and regions in which we compete.

The Agency is committed to providing competitive pay that reflects the full spectrum of experience and performance.

To access the complete Compensation Program Guideline for Human Resources, go to the Agency's Extranet or contact the Human Resources Department directly.

5.4 Electronic Timekeeping System/Reporting

Effective 12/15/00, Revised 11/16/09; 11/9/2011; 7/1/2013

Purpose

To ensure employees are paid fairly and correctly and to provide a process for properly authorizing and verifying actual hours worked, the following guidelines will be followed:

Use Required

All hourly employees will utilize the electronic time keeping system via the electronic time clocks located at Post 100 when reporting for and ending duty. To ensure that hours outside of an employee's scheduled work hours were worked and authorized, a pay authorization form signed by a supervisor will be required to authorize pay. An authorization form is also required for missed time clock punches.

The pay authorization form is available next to the time clock in the bay and from the operations assistant, scheduling department and human resources. The form must be completed and submitted to a supervisor who will verify and approve. The completed and approved form will then be placed in the drop box located in the operations area.

Forms must be completed and submitted to a supervisor the **day of the occurrence.** In the absence of a supervisor, a drop off location will be provided to the employee that provides a central collection point for the supervisor to validate and approve submitted forms. **Failure to submit a pay authorization form within the day of occurrence may result in a delay of processing these hours until the next scheduled pay period. An employee's work time will be recorded as their scheduled time for the day if the proper authorization and verification form is not turned in as described.** For incidents involving missed time punches, no time will be added to the employee's time card until authorization for the actual time worked is received.

Any employee who clocks in prior the employee's scheduled shift , submits a false pay authorization or otherwise falsifies the pay authorization for the purpose of collecting pay (outside of a scheduled shift, training, demo, special event, etc.) for hours not actually worked will be subject to disciplinary action up to and including termination of employment.

Reporting To Work

Employees are to report to work ready to start their shift (in uniform, with personal equipment, etc.,) before clocking in for the day. Time clocks are located in the following locations:

Post 100 Time clock at Support Services window
Post 100 Time clock located inside Communications Center

The electronic timekeeping system utilizes a 15-minute rounding rule. All time worked is rounded to the quarter hour (.00, .25, .50, .75).

XX:53 – XX:07 rounds to .00
XX:08 – XX:22 rounds to .25
XX:23 – XX:37 rounds to .50
XX:38 – XX:52 rounds to .75

The time clocks allow employees to clock in seven minutes before the start of their scheduled shift and will allow employees to clock out any time after their shift ends.
If an employee gets a "Not Accepted" message from the time clock and needs to clock in/out or is unable to clock in or out, the employee must contact Scheduling or a supervisor immediately.

Requesting Authorization and Tracking Training Attendance

To ensure all hourly employees are compensated for training times, the training organizer should complete a training authorization form with the appropriate information, including a attendance roster, and submit to the approving Manager ***before*** the actual training date. This will ensure that both the budgetary approvals are made as well as correct employee compensation is established for attendance.

The organizer should ensure that employees are not clocked in under any circumstance (i.e. not clocked in while working a shift) while attending training and should print and sign their name on the attendance roster to confirm their attendance. If the employee must clock out for training during a shift, they should clock back in immediately following the training.

The training organizer must submit the training authorization form along with the attendance roster to the scheduling department within the day the training occurs.

Employees attending Agency required training must complete and sign the Agency attendance roster provided by the instructor. The training department should be contacted to ensure the time is documented for any authorized class attended. The employee will be paid from the attendance roster maintained by the instructor. Employee should not use the time clock for scheduled training. Employee is not required to complete a pay authorization form for the training. It is the responsibility of the instructor (and each employee) to ensure participants are documented.

Requesting Authorization and Tracking Meeting Attendance

To ensure all hourly employees are compensated for meeting times, the meeting organizer should complete a meeting authorization form with the appropriate information and submit to the approving Deputy Director ***before*** the actual meeting date. This will ensure that both the budgetary approvals are made as well as correct employee compensation is established for attendance.

After receiving approval, the organizer should bring the form to the scheduled meeting. The organizer should ensure that employees are not clocked in under any circumstance (i.e. not clocked in while working a shift) while attending the meeting and should print and sign their name on the attendance roster to confirm their attendance. If the employee must clock out for a meeting during a shift, they should clock back in immediately following the meeting.
The meeting organizer must submit the meeting authorization form along with a completed roster to the scheduling department within the day the meeting occurs.

Unauthorized Use

Employees are not permitted to clock in/out other employees at anytime. Any employee clocking in/out for another employee will be subject to disciplinary action up to and including termination of employment.

Any employee who attempts to use their ID card to report hours not actually worked will be subject to disciplinary action up to and including termination of employment.

Leave Without Pay

Leave without pay requires approval of a Deputy Director or higher. Employees who exhaust all paid leave without prior approval who must be placed in a leave without pay status will be subject to disciplinary action up to and including termination.

Pay Period

Each pay period consists of two work weeks beginning at 0000 hours on Tuesday and ending at 2359 hours on the following Monday for all job descriptions. Employees are paid in the current

week for any shift worked that begins before 2359 hours on Monday until the shift ends on Tuesday.

Timekeeping System Failure

In the event the timekeeping system should fail, employees will be given manual timesheets to complete before the end of the pay period. All time documented on the attendance logs will be used to ensure employees are paid correctly.

5.5 On-Call and Remote Access Pay

Effective 7/1/07

Purpose

To ensure that authorized non-exempt employees who are on Restricted On-Call status are compensated in accordance with the Fair Labor Standards Act (FLSA), and to ensure that non-exempt employees who are on Non-Restricted On-Call Status, although not entitled to pay under FLSA, receive some benefit.

Policy

Non-exempt employees who are on Restricted On-Call Status, or who have been authorized to work off site by remote access, such as computer or telephone, will be paid for all hours worked, and such hours will be counted as hours worked for purposes of calculating overtime.

Non-exempt employees who are on Non-Restricted On-Call Status will not be paid while on-call, and time spent on-call will not be counted as hours worked for purposes of calculating overtime. However, the Agency will pay employees who serve in Non-Restricted On-Call Status one (1) hour's pay at the employee's current hourly rate for each twenty-four (24) hour period, or portion thereof. Any employee who is required to report to work while on Non-Restricted On-Call will be guaranteed a minimum of two (2) hours' pay, even if the employee works less than two (2) hours.

The Executive Director or his authorized designee(s) must approve, in advance, all Restricted On-Call and Non-Restricted On-Call as well as remote access arrangements.

For purposes of this policy, the following apply:

1. "Restricted On-Call" is defined as call requiring that the employee's activities be so restricted and burdensome that the time spent on-call is predominantly for the benefit of the Agency. Employees on restricted on-call status are not free to pursue normal personal activities while waiting to be engaged by the Agency. It is anticipated that Restricted On-Call Status will only be requested or required under extraordinary circumstances.

2. "Non-Restricted On-Call" is defined as call that is not predominantly for the benefit of the Agency where the employee is basically free to pursue his or her own normal personal activities. Employees on Non-Restricted On-Call Status must be able to respond or report for duty within the time prescribed.

3. Exempt employees, who are not eligible for overtime pay, are also not eligible for on-call or remote access pay.

Questions regarding this policy should be directed to Human Resources.

5.6 Overtime
Effective 1/1/99

Purpose
To provide employees with guidelines for the assignment of overtime hours.

Policy
Overtime may be utilized when staffing falls below acceptable minimum staffing levels to fill vacancies that occur or to cover unexpected workloads. Employees are asked to contact their supervisor for more information regarding overtime shifts.

The Agency may mandate overtime or holdovers during periods of peak demand or disaster.

5.7 Paycheck Distribution

Effective 1/1/99; Revised 7/1/07

Purpose

To provide a standard for the time, place, and procedure of paycheck distribution.

Policy

1. Employees are expected to utilize direct deposit.

2. Direct deposit slips shall be e-mailed to employees Medic e-mail account by 4:00 p.m., on the Thursday before payday. Paydays are bi-weekly.

3. Due to the Privileged Information Act, payroll information cannot be released over the telephone.

4. Any discrepancy regarding payroll hours should be directed to the Scheduling Department for all field personnel and to a supervisor for all other employees.

5. Any discrepancy regarding pay rates, benefits or deductions should be directed to the Human Resources Department.

6. No one may pick-up a pay related document for another employee unless the absent employee has a signed consent form on file with the Payroll Department authorizing the individual to pick-up the paycheck on his or her behalf.

7. Holidays may alter the check distribution date. In the event this occurs, employees will be advised prior to the holiday.

5.8 Performance Evaluations

Revised 3/1/05, 11/1/2006, 9/1/16

Purpose

To specify policy/procedure involved with performance evaluations.

Policy

Human Resources is responsible for timely notification of department managers/supervisors when evaluations are due and for monitoring the timeliness of completion of evaluations. In addition, the Human Resources Department is responsible for the processing of evaluations and to insure completed forms are filed in personnel folders.

Human Resources will also send a report to the department manager/supervisor notifying them of any delinquent evaluations.

Employees receive formal performance evaluations annually on a common review date of September 1st each year, in addition to regular, on-going feedback from supervisors.

The method to evaluate employees is based on job descriptions and other standards of performance.

Evaluations allow for employees to provide written input on the review and require acknowledgement and/or signature from the employee and the supervisor before it is processed. Copies of completed evaluations are available in Human Resources.

Employees who perform below standards will not be eligible for a salary increase and the department manager/supervisor will determine the next appropriate step which will include: deferral of a salary increase for a period not to exceed one year with additional coaching sessions during the deferral period and disciplinary action up to and including termination. Any deferrals of an increase shall not be retroactive.

5.9 Promotional Increases

Revised 9/1/04

Purpose

To financially reward employees who are assigned to a new position in a higher salary grade.

Policy

Promotional salary increases are given when an employee is assigned on a regular basis to a new position in a higher salary grade. A promotional increase is intended to provide competitive pay and financial rewards to recognize increased job responsibilities.

An employee who is placed in a job with a higher market rate will be raised to the minimum salary or receive the percentage difference in market rates not to exceed 10%, whichever is greater. Exceptions to this procedure must be requested by the department director and the Director of Human Resources.

5.10 Daylight Saving Time

Effective 1/1/99

Purpose

To provide compensation guidelines for those employee shifts that are lengthened or shortened by time change.

Policy

Spring: One fewer hour will be worked/paid

Fall: One more hour will be worked/paid

5.11 Longevity Pay

Revised 7/1/04; Revised 11/18/08

Policy

The Agency places a priority on offering competitive compensation and rewarding employee performance. Therefore, employees hired after June 30, 2004 will not be eligible to receive a longevity bonus. Employees hired prior to July 2004 will be eligible to receive a longevity bonus once they have attained at least 10 years of accumulated credit for service as indicated by the service date and at least 10 years of service with the North Carolina Local Governmental Employees' Retirement System based on the employee's aggregate date maintained by the Human Resources Department. For longevity purposes, no credit will be given for years during which retirement contributions have been withdrawn from the system.

Annual longevity payments will be computed according to the following scheduled:

Years of Service	***Annual Longevity Allowance***
10 but less than 15 years	1%
15 but less than 20 years	2%
20 but less than 25 years	3%
25 years and over	4%

Longevity will be paid once a year to all eligible employees. To be eligible to receive this payout you must be actively employed at time of the payout to receive full payment. Payment will be made on the last paycheck in November of each year and is treated as taxable income. The amount of longevity to be paid to each eligible employee is calculated on October 31st of each year. For example, if an employee reaches 10 years of retirement credit on or before October 31st, the employee is eligible for a 1% bonus. This amount is automatically calculated on October 31st and paid to the employee in the last paycheck of November. If an employee reaches 10 years of retirement credit after October 31st, the employee will not be eligible for longevity pay until the following year.

If an employee eligible for longevity pay terminates their employment at any time of the year, a pro-rated longevity amount based on the elapsed time from November 1st to the date of termination will be paid to the employee in their final paycheck. No payment will be made to employees who are terminated for cause or who resign in lieu of termination. Employees whose performance did not merit an increase with their most recent performance appraisal are not eligible for a longevity bonus for that year. Longevity bonuses owed to a deceased employee will be paid to their estate.

Longevity is not considered a part of the annual base pay for classification and payment purposes, nor is it recorded in personnel records as a part of annual base salary.

5.12 Staff/Supervisor/Administrative Credentialed Patient Care Provider Field Time Guidelines

Effective 07/01/12, Updated 12/01/2016, Updated 08/01/2018

Purpose

Supervisors, managers and administrative personnel who hold a valid NC paramedic or EMT certification, and have privileges to function within Mecklenburg County are required to obtain regular time in the field and CMED each year. The purpose of this is to maintain regular exposure to patient care and to develop/maintain employee relationships. This requirement is approved by both the Agency's Medical Director and Lead Team.

Policy

Paramedic/EMT-certified supervisors, managers and administrative personnel are required to achieve 36 hours of field time, following the parameters outlined below, each quarter.

In order to achieve the required hours, staff may elect any, or combination of, the following options:

1. Function in the role of crew chief
2. Function in the role of non crew chief (second person)
3. Ride with a crew in a third person status
4. Providing coverage for special events when serving as part of a dedicated Medic crew
5. The time can be achieved by riding with crews that are 9-1-1 ALS, NET ALS or NET BLS
6. If assigned an Agency response vehicle, time can be achieved by directly responding to calls throughout the county to facilitate exposure to a larger number of calls and interaction with a greater number of employees at one time.
7. A minimum of 50% of the required quarterly hours must be acquired from options #1, #2 or #3.

Annually, each staff paramedic, EMT, supervisor or administrator must observe in CMED for a minimum of 4 hours. These hours are considered part of the total time requirement and not in addition to. This time requirement may be satisfied in one sitting or broken up over multiple months/quarters.

There is no minimum number of hours required for each field experience. Staff may elect smaller blocks of time as long as the time modification does not negatively impact system coverage.

Compensation options remain unchanged.

5.13 Exempt Stipend Policy
Effective 7/1/2012

Purpose
The goal of this policy is to use resources of exempt employees to help fill vacancies in the schedule and fulfill critical roles in the Agency.

Policy

The Stipend is paid to Exempt employees who work as a Paramedic during off scheduled time to help fill vacancies in the schedule and fulfill critical roles in the Agency. The employee must also function in either a crew chief or 2nd person paramedic status.

The Stipend is paid for working as a Paramedic for any full shift worked outside of your regular position. The Stipend is paid at the top OT rate for a Paramedic Crew Chief for 12 hours. Each time the pay band is re-evaluated the pay will change accordingly.

The rate applies to all 10, 12 and 14 hour shifts.

You can work a field shift in trade for a day of your current assignment if your workload permits and your supervisor approves but with no additional pay.

You are classified as an exempt employee based on your regular job responsibilities. Any additional shifts you sign up for cannot make up more than 50% of your total work time; otherwise, your exempt status as determined by FLSA will be jeopardized.

To record your time, clock-in and clock-out using the correct code. If not starting work at the Agency fill out an exception card and turn-in to scheduling.

5.14 Part Time (Temporary) Operations Employee Policy

Effective 5/1/11; Revised 09/02/13; 1/10/14; 3/11/15; 05/01/17; 08/01/2020

Purpose

To provide employees with guidelines regarding options for transitioning to part time employment and returning back to full time employment. This policy only pertains to employees that are eligible to perform in Operations.

Policy

The Agency desires to offer employment status changes with operations staff that are eligible and wish to transition to either part-time or back to full-time status. In an effort to maintain effective staffing resources, the Agency has outlined eligibility requirements, transitional procedures and work requirements to remain in good standing with an approved transition.

Eligibility for Part Time

A position must be available. The number of part-time employees in Operations is determined by the Deputy Director of Operations. This number may vary dependent upon system needs.

An employee must be in good standing to request a part-time position. This includes:

- Current with all required continuing education, annual corporate compliance testing/training, annual HIPAA testing/training, fit testing, applicable health screenings and all necessary certifications and licenses.
- No active Progressive Discipline (PD) on file.
- Most recent performance review of Meets or higher.
- Meet the service requirement of one consecutive year of employment.
- For Field Operations, employee must have a GeoTab score of 4 or higher.

Requirements

Employee must function in their primary role/job title for the minimum requirements. Any combination of the credits can be worked so long as the minimum monthly requirement is met.

- **Minimum Monthly Requirement = 3 Credits**
    - Credit Values:
        - 1.0 credit = Any weekday shift (Friday shift start times prior to 1500)
        - 2.0 credit = Friday with at clock-in time of 1500 or later, Saturday or Sunday shift
        - 0.5 credit = High school football game outside of a regularly scheduled field shift (no additional credit for being assigned to a football game standby as a system 911 truck); Partial shifts (a minimum of 4 hours worked); Dedicated standbys of less than 10 hours.

Other hours such as continuing education, OST, OA, etc. do not count toward this requirement.

The maximum hours that can be scheduled by the employee are 28 hours per pay week, 130 hours per month and no more than 1000 per calendar year. These total hours include all hours worked (con-ed, committees, assessment centers, standby assignments, etc.). Any exceptions to hours worked must be approved through the Operations Manager prior shift pick-up. An employee who exceeds the maximum may be subject to progressive disciplinary action.

Employees are required to notify their direct Supervisor if there are any issues regarding availability. Cancellation of any assigned shifts will continue to follow the existing call out and attendance policies. Employees are responsible for logging into the Agency's time-keeping

software system to assure they are in compliance with the hours' requirement. Any deviation from the minimum required hours must be approved (in advance) by the Operations Manager.

- **Administrative Requirements**
  - Stay current with all required continuing education.
  - Stay current with all annual corporate compliance and HIPAA testing/training.
  - Stay current with all annual health screening requirements.

Transition Procedures

1. Field employees will make the request through their assigned supervisor who will verify with the Operations Managers that a part time position is available. CMED employees will submit requests directly to the Operations Manager – Communications.
2. Once availability has been determined and the employee's supervisor is in agreement with the transition, the supervisor will forward a letter of recommendation to the manager requesting that the employee be granted part time status. Employee should provide a minimum of a 30-day notice to their assigned supervisor to ensure there is sufficient time for the transition.
3. The Deputy Director will make the final approval. Once approved, the manager will forward the request to HR to determine the date in which the part-time status will begin. The manager will then forward the approval to the Scheduling Department to process the PAF (personnel action form).
4. Paramedic Crew Chiefs/BLS Team Leaders will be reclassified to Relief Crew Chiefs/Relief Team Leaders with associated pay decrease (excluding 30-year retiring crew chiefs).
5. Performance pay will adjust based on transition date.

Progressive Discipline Action

Part time employees are subject to the progressive disciplinary actions as outline in the Agency's Employee Handbook section "Attendance Policy". Due to the limited hours that are required to maintain part time status, the following items have been added as conditions for employment.

A. Any Part time (temporary) employees who accumulate six (6) behavior infractions in a twelve (12) month period will result in termination.

B. Failing to work an assigned shift in a 3 month period will be considered a voluntary resignation unless pre-approved by the Operations Manager.

C. Failure to meet minimum required credits over 3 consecutive months may result in termination unless pre-approved by the Operations Manager.

Eligibility for Transition to Full Time from Temporary Part Time

A full time position must be available. The Forecasting Supervisor will coordinate the assignment of shifts.

An employee must be in good standing to request a full-time position. This includes:

- Current with all required continuing education, annual corporate compliance testing/training, annual HIPAA testing/training, fit testing, applicable health screenings and all necessary certifications and licenses.
- No active Progressive Discipline (PD) on file.
- Most recent performance review of Meets or higher.
- For Field Operations, employee must have a GeoTab score of 4 or higher.

Transition Procedures

1. The employee must make the request through their immediate supervisor who will verify that a position is available.
2. Once availability has been determined and the employee's supervisor is in agreement with the transition, the supervisor will forward a letter of recommendation to the manager requesting that the employee be granted full time status. The letter of recommendation must include a start date that is at the beginning of a pay period. Sufficient time for the transition approval process must be considered when determining the start date.
3. The manager will forward the approval to the Forecasting Supervisor. The Forecasting Supervisor will process the personnel action form (PAF). The Deputy Director of Operations will be notified of the final approval.
4. If you are a returning Relief Crew Chief, you will remain in that function upon return to full-time status. You will be ranked accordingly into the Relief Crew Chief pool. A Crew Chief assignment will be determined by the Crew Chief Bid Process.

Employees who request the return to full time status will only be permitted to do so once unless specifically authorized by the Deputy Director.

An employee's time in position date for the purposes of any shift bids or promotions will be based on the date in which they returned to full time status. In addition, accruals for sick and vacation time will be calculated from the return to full time status date, unless there was no withdrawal from the NC State Retirement System.

- For example:
  - JD was originally hired full time on January 1, 2007
  - JD was approved for part time status on January 1, 2011
  - JD was approved for return to full time status on March 1, 2011
  - JD time in position date (used in shift bid) is now March 1, 2011
  - Vacation and sick time will be calculated from March 1, 2011

5.15 Field Operations Scheduling Policy

Effective 5/1/14; Revised 6/4/14, 1/2/18, 2/1/23

Purpose

To provide employees information on the Field Operations Scheduling

Scheduling Department/OA/Supervisor Schedule Responsibilities

The daily operations schedule is maintained utilizing Medic's online ePro Scheduler. The schedule responsibilities are shared between the scheduling department, the operations assistant and the operations supervisor based upon the three time periods described below.

Beyond Three Days (72 hours+)

The scheduling department is the **sole contact** for items associated with the schedule beyond three days of the current day. This includes employee schedule change requests, benefit leave requests, shift pickups and shift swaps. The shift pickups and shift swap queue will be viewed regularly by the scheduling department to assure timely employee notifications.

Within Three Days (72 hours)

The operations assistant and supervisor may make adjustments to the schedule as needed within three days of a shifts scheduled start time. This includes employee schedule change requests, shift pickups and shift swaps. The shift pickups and shift swap queue will be viewed regularly to assure timely employee notifications.

Current Day (within 24 hours)

The operations assistant and supervisor coordinate unit assignments throughout the day therefore have control of the current day's schedule. This includes employee call outs, schedule change requests, shift pickups and shift swaps. The shift pickups and shift swap queue will be viewed regularly by the operations assistant and/or supervisor to assure timely employee notifications.

Questions related to these responsibilities should be directed to the scheduling supervisor.

Field Operations ePro Schedule Publishing

The field operations schedule will be published online for a minimum of three weeks. The dates for publishing and assigning employees to shifts are posted in the document library of ePro Scheduler. Employees bid on open shifts for one week prior to awarding assignments. After one week of bidding, shifts will be assigned per policy.

ePro Shift Pickup - Submissions

Shift pickups can be submitted at any time. Shift pickups within 24-hours of the shifts scheduled start time will be processed as encountered by the operations assistant or supervisor in no specific order. To assure a timely assignment, **a phone call to the operations assistant is encouraged** for current day submissions.

ePro Shift Pickup - Assignments

Schedules will be published online one pay period at a time and extend up to 5+ weeks in advance from the current day. Once the new pay period is published online, floaters, part-time and administrative staff will bid on the open shifts for a period of one week. During the bid period (first week of the published schedule) only full time floaters up to 40 hours per pay week will be assigned. All others will remain in queue. At the end of the one week bid period, all remaining bids in the assignment order of 2 through 4 will be processed by the scheduling department. Number 5 will remain in queue until the 7 day mark from the current day. Inside of 7 days, bids for number 5 will be processed.

Assignment Order:

1. full time floater to 40 hours per pay week
2. Part-time employees
3. Admin Personnel - up to the required number of hours per quarter
4. Full-time employees (overtime)
5. Admin Personnel - that exceed the required number of hours per quarter

After the initial week of processing bids, assignments will be first come, first serve with the exception of number 5 in the assignment order as indicated above.

The dates of when each pay period is published online are posted in the Document section of ePro Scheduler. Questions reqarding shift assignment should be directed to the Scheduling department supervisor.

Float Shifts
A floater or float shift refers to a 40-hour per week employee that does not have a preset work schedule for each week. Their shifts are assigned by the scheduling department within the first week of a published schedule. Employees with a float assignment must be compliant with the guidelines set forth in their job description in order to maintain their float assignment. Float shifts are included in the annual shift bid process.

ePro Shift Pickup - Qualification Requirements
Shifts pickups that do not match the employee's qualification type i.e. crew chief for a non-crew chief position will not be considered for assignment until the shift is within seven days of its start time. Prior to this period, all attempts to fill the shift with a matching qualification type will be made. Part time relief crew chiefs may be assigned to non-crew chief positions prior to assigning a non-crew chief in overtime.

Paramedic's cannot be assigned to BLS units nor turn a BLS unit into an ALS unit without the authorization of the Operations Manager.

ePro Shift Pickup - Cancellations
Employees who choose to cancel an approved overtime shift **must call** the scheduling department or the operations assistant who will "Clear" the employee from their shift and re-open the shift for overtime. This function is permissible from the OA position at any time for a published schedule. Shift cancellations may be subject to the attendance policy. See the attendance policy for details.

ePro Shift Availability
Employees who would like to indicate their availability to pick up shifts should do so by selecting the ePro Scheduler menu item titled *Shift Availability*. The scheduling department and/or the operations assistant may use this information to notify employees of opening that occur within the schedule. The primary form of picking up shifts should be through the Pickup Shifts menu item.

Shortening Shifts Times
Shifts may be shortened to accommodate administrative ride time, crew pairing and overtime inside of three days (72 hours) of the shifts scheduled start time. Prior to this period, all attempts to fill the entire shift will be made. Shift pickups that involve reducing shift times will remain in a pending status until they are within the three day period.

Administrative salaried employees who sign up to work 12+ hours are required to work the entire shift as scheduled with no time adjustments.

Crew Pairing Procedure
Employees will be paired by the scheduling department, operations assist and operations supervisor within the time frames described above. Pairing will occur to maximize the number of

unit hours produced (units on the street). If circumstances change after pairing has occurred, adjustments may dictate another change to achieve this goal. The schedule will be monitored continually for changes/adjustments that are necessary to maximize unit hour production.

Crew Pairing – Shift Start Time Adjustments
Employees who are paired with differing shift start times from their partner may elect to start their shift at the same time. The employee interested in pairing up equally should contact scheduling or send an email via scheduling@medic911.com. Once the change has been made, the employee will receive an email confirmation from the scheduling department. For the current day requests, the employee should call the operations assistant/supervisor.

Relief Crew Chief Movement-Pairing
Relief crew chiefs may be moved from their non-crew chief position to crew chief a unit anytime within the published schedule period.

Benefit Leave Requests
Employees must receive benefit leave approval to be scheduled off on a scheduled work day. After the annual shift bid has been conducted an announcement will be made indicating a date in November for when benefit leave will be accepted for the new shifts that begin the following January. Requests will be accepted through August 31st at that time. Beginning January 1, request will be accepted for the remainder of the year leading up the next full bid's effective date.

Benefit leave requests must be submitted through ePro Scheduler for the full duration of the shift. No partial shift will be accepted for employees that are scheduled to deploy on a Medic unit. The scheduling department is responsible for processing all leave requests based upon internal set criteria.

Time off will be approved based upon the employees accrued vacation bank. Holiday time that is transferred into the vacation bank is not a pay period based accrual item and therefore can only be utilized after the holiday has occurred and the hours are actually in the employees vacation bank, i.e. an employee may use their Independence holiday time after the time is reflected in their vacation bank. Employees who choose to receive pay for their holiday time do not accrue holiday time.

Benefit leave requests must be received no later than two weeks prior to the requested date. This is to insure that proper coverage can be arranged and/or that staffing levels are not be negatively impacted. Any exception to the two week minimum requirement must be due to extraordinary circumstances and must be approved by the employee's manager on a case by case basis.

Deleting a Pending Timeoff Request
A timeoff request that has not been approved can be deleted in ePro Scheduler. An email confirmation will not occur.

Benefit Leave Cancellation
Employees may cancel approved benefit leave prior to a published (released) schedule and return to their shift. Employees who cancel approved benefit leave for a published (released) schedule will return to their shift **if the shift is open**. If the shift has been filled, the employee will be required to pick up another shift during the same pay week to obtain their hours for the week. Employees are encouraged to check the status of their shift prior to cancelling if their objective is to return to their shift. A phone call to the scheduling department is also encouraged for timely action to the request. An employee cancelling benefit leave will not be able to "bump" another employee from a shift.

Cancellation Notification Procedure-

Inside of Three Days (72 hours) from the Current Day
Employees cancelling approved benefit leave must do so by calling the scheduling department, operations assistant or supervisor.

Beyond Three Days (72 hours) from the Current Day
Employees may request cancellation of benefit leave online in ePro Scheduler, by going to REQUEST TIMEOFF, at bottom of the screen click the blue highlighted Benefit Leave for the date(s) they wish to cancel, choose DELETE and then OK. A message will then be sent to Scheduler advising that you wish to cancel the selected date. You must wait for a confirmation message advising that your timeoff request has been cancelled and whether you have been returned to your scheduled shift or if you will have to pick up another shift in the same pay week. Until the confirmation email is received, the approved Benefit Leave will remain on the schedule. A phone call to the scheduling department is encouraged for timely action on the request.

ePro Shift Swaps
Shift swaps must be submitted for the same pay week with an employee with the same qualification (crew chief, non-crew chief) or they will not be approved. When an employee submits a shift swap, the other employee must login to ePro-Scheduler and approve the shift swap request (agree to the swap). The swap cannot receive final approval until this occurs. The pay week begins on Tuesday and ends on Monday. Both employees must uphold their swap otherwise the exchange may be cancelled. It is recommended that shift swaps be submitted at least 3 days in advance to assure adequate time for approval. The swap becomes each employee's scheduled shift for the day and all attendance policy rules apply for the employee scheduled to work. Scheduling approval will only occur after the schedule is published (3.5-5.5 weeks) and as long as both employees remain active.

ePro Split Shifts – Benefit Leave
Shifts must be split in ePro Scheduler for instances where an employee utilizes benefit leave for part of their shift. The OA/supervisor must do so as it occurs to assure that the appropriate leave is applied. Part of their shift will show hours worked with the remaining hours indicating the type of leave being applied.

Administrative Scheduled Shift Removal Request Notice Requirement
All types of requests for being removed from the field schedule will generally require a minimum two-week notice. Removal may be contingent upon obtaining adequate coverage for vacated shift and operations manager approval.

Employee Scheduled Shift Removal – Supervisor/Manager Requests
The request must be received in writing via scheduling@medic911.com from the department manager or designee no later than **two-weeks** prior to the requested date. This is to ensure that proper coverage can be arranged and/or that staffing levels will not be negatively impacted. Any exception to the two week minimum requirement must be due to extraordinary circumstances and must be approved by the employee's director on a case by case basis.
Rosters submissions or payroll authorization cards for the event will be required for employee pay.

Employee Scheduled Shift Removal – Hour Compensation Difference
Employees who are removed from the schedule for an event or training that result in fewer hours than their regularly scheduled shift should see the on duty supervisor at the completion of the event or training for opportunities that may enable the employee to complete their regularly scheduled hours for the day. The supervisor will take into consideration the practicality of employees location and type of training when making a determination, i.e. exhaustive SWAT training.

If the employee has more than two regularly scheduled hours, the supervisor will pursue all efforts at placing a Medic unit in service for the employee(s) remaining hours. If this option is not feasible, the employee may choose to utilize benefit leave.

Employees that are participating in the same training session and are capable of pairing to produce a Medic unit should contact the Scheduling department in advance of their training for pre-determined field unit scheduling.

The only exception would be for night shift employees who must leave early for the night prior to the event or training. There should be an eight hour break between the employee's end of shift the night prior and their scheduled start time the next day. Administrative time will be paid for scheduled hours inside of the eight hour window, i.e. an employee scheduled for 18:30-06:30 will be attending an event the following day at 08:00. In this scenario, the employee will work their scheduled shift until midnight and receive administrative time for their remaining night shift hours. Activities of this type should be last resort to avoid removing an employee from their scheduled shift.

Internal Certification Upgrade – Third Person Upgrade Ride Time
Internal department requests for upgrades must be received via scheduling@medic911.com from the department manager or designee no later than one week prior to the requested date. This is to insure that proper coverage can be arranged and/or that staffing levels will not be negatively impacted. Any exception to the one week minimum requirement must be due to extraordinary circumstances and must be approved by the employee's manager on a case by case basis.

External Ride Time Request – Third Person Ride Time
External requests for ride time must be received via scheduling@medic911.com from the requester no later than two weeks prior to the requested date. This is to insure that the scheduling department has sufficient time to coordinate the third person ride time. FTO's cannot be utilized for external requests. The Scheduling department must have authorization from the Medical Services department manager prior to adding non-Medic personnel as third person.

Upgrade/Trainee Release Date Notification
The Learning and Development department will notify the Scheduling department of any anticipated upgrade or release date of a trainee so that their shift regular assignment can be taken into consideration. Upgrades will typically be effective the pay period following the upgrade notification from L & D. Employees may be directed to ride third or pickup open shifts to finish out the current pay period.
Employees will not technically be considered upgraded or released until the Scheduling department receives a personnel action form (PAF) from L&D. The appropriate ePro qualification will be added to the employee for the pay period that the upgrade is effective.

Removal from a Shift (Bumped)
Employees who sign up for an open shift will generally not be "bumped" from the shift unless the shift is being filled by an employee returning from OJI, FMLA or released from training. Employees may be required to pick up open shifts if their regular shift has been assigned to another employee.

Bereavement Leave
The bereavement leave earning code must be applied to any schedule item that meets the criteria (see specific policy). Proper documentation of the relationship shall be included.

Employee with No Partner
A scheduled employee that does not have an assigned partner for the current day may be provided another related assignment by the on duty supervisor. The employee may be given the option to utilize benefit leave for the duration of their shift.

Scheduled Medic Units
Medic units scheduled for field deployment cannot be taken out of service for administrative training, etc. without the approval of an operations manager/director. This excludes instances for the current day when system status levels are high and the field operations supervisor has made arrangements with the communications supervisor. In such case, the unit remains subject to call assignment as needed.

On-The-Fly Shifts (OTF)
On the fly shifts will be added to the schedule by the scheduling department as determined by the scheduling supervisor. Requests for OTF shifts should be directed to the scheduling supervisor, operations manager or director.

ePro Scheduler Username/Password
ePro Scheduler has an interface that looks up the employees Medic password each time they log into the system. Passwords are maintained by Medic's IT department. Medic's IT department should be contacted to verify employee passwords. The Scheduling department should be contacted to verify that usernames are correct in the system. The "forgot password" option at the ePro login should not be used for password verification.

ePro Scheduler Notification Preference Option*
When an employee is assigned an overtime shift or when there are changes to their shift, the default method of notification is the employee's Medic email address. This option allows the employee to choose their own personal preference by electing to be notified via personal email and/or cell phone text message.

ePro Scheduler Notification Preference for Open Field Overtime Shifts*
Employees may choose if and when they would like to be notified for open shifts, i.e. overtime shifts that exist within 24-hours of the shift scheduled start time. These notifications can be sent to the preferred email address and/or personal device at only the times specified.

Submission Process for Notification Preference*
Complete the form by clicking the Notification Preference link in ePro Scheduler under the miscellaneous menu item. The scheduling department will periodically update these settings in ePro Scheduler. Employees should return to the Notification Preference link in ePro Scheduler for change requests to their preferences. If an employee enters multiple requests, the most recent will be included in the update.

***Standard text messaging rates may apply. Please contact your mobile service provider to determine rates and fees that maybe associated with your text service. Medic is not responsible for any charges on your personal cell phone bill.**

ePro Scheduler System Upgrade Announcement
Periodically system upgrades may make the schedule inaccessible for what is typically at around midnight for about 10 minutes. Scheduling will post a note on the system message board and notify the on duty field and CMED operations supervisors of upgrade the day of the occurrence.

Shift Assignment Change Requests
To be equitable to all employees and create stability within the schedule, employee requests for temporary or permanent moves will not be accepted. Shift bid participation and permanent shift exchanges are the methods in which an employee will be permitted to change shifts.
Open crew chief shifts that occur will be eligible to upgrading crew chiefs. Open non-crew chief shifts that occur will be eligible to new or displaced employees only.
The only exceptions to moves would be to or from the NET team as approved by the NET supervisor or a move the places the employee on a shift of critical need, such as nights or weekends as determined by the scheduling supervisor.

Work Maximums
To ensure adequate downtime for the employee, the following work maximums have been established.

- Daily Hours – Employees who work two consecutive shifts that total more than 26 hours must have a 10-hour break between shifts.
- Weekly Hours (per pay week) – 80
- Consecutive Days – 7

High Performance Unit Performance Credit (NET TEAM)
HP team employees that reach their required point total will end their shift early and be paid for their entire shift. The NET supervisor or designee will record the additional hours in ePro with the earning code of "call volume".
Non-NET team employees who are paired with a HP unit will receive a maximum credit equal to that of the HP member's total. For example, a 12-hour non-NET team member is paired with a 10.5 hour NET team employee. They complete their shift in 9-hours. Both employees receive 1.5 hours of "call volume" credit. The 12-hour employee would use 1.5 hours of benefit leave in addition to the "call volume" credit to end their shift for day.

ePro Shift Discrepancy Documentation
Administrative users of the schedule should include comments for each shift as needed to assist in the supervisors following day discrepancy review.

ePro Missed Punches
A yellow payroll authorization card is required for missed punches. These cards will be submitted to the operations supervisor for validation that the employee was present and that the time is correct. See payroll policy for further details.

ePro Timecard Discrepancies – Supervisors/Managers
The previous day's discrepancies should be processed daily. The current day cannot be processed until all employees have completed their shift. All supervisors and managers should have a backup to handle these items in their absence.

ePro Timecard Approval – Employee
Employees are required to approve their timecards by 12 p.m., Monday or after the completion of their Monday shift at the end of each pay period. If the timecard is incorrect, the employee shall select disapprove (no) and provide a clear description of the problem so it can be easily be identified and corrected. If there is an error in an employee's timecard that shorts their pay and the employee does not submit the correction prior to the close of the pay period, payment will not be made until the next regular paycheck.

ePro Timecard Approval – Supervisors/Managers
Supervisors and Managers are required to approve their employee's timecards by 12 p.m., Tuesday at the end of each pay period. Timecards will be closed out at 12 p.m. Missing or unverified information may result in delayed payment to the employee.
Questions should be routed to Scheduling at scheduling@medic911.com or via phone at ext. 6235 or 6252.

PALS/ACLS Classes
Employees without an opportunity to obtain necessary recertification classes may request their shift off to obtain the class. These requests require a **two-week** notice to assure adequate backfill for the shift and must be received from the Learning and Development manager. The employee may switch out and work another day during the pay week or receive approved time off if staffing permits. Employees that are approved for the day off will be paid for their class time and benefit leave applied to their remaining shift hours.

Jury Duty
Employees must contact the Scheduling department at least one week in advance and request to be removed from the schedule for any schedule shifts for first day appearances for jury duty. For any subsequent days, the employee must call in and speak with someone in the Scheduling department or the on duty OA/Ops office the day before jury duty to ensure removal from the schedule.

Modified Duty
All employees who are assigned modified duty for an OJI and/or a non-OJI are subject to this attendance policy at all times. For further explanation or questions please see Risk and Safety.

Subpoenas and Court Orders
Any employee who is out for a subpoena or court order must determine any schedule changes with the supervisor on duty.

Outside Agency Event Participation
Employees who choose to participate in an event and are scheduled to work must do so by utilizing approved benefit leave or shift swap to be removed from the schedule. Any exceptions require Director approval.

Clocking In and Out
Employees are responsible for clocking in and out at the beginning and end of each shift.

Clock Failure Contingency
In the event of a total clock failure, employees will sign in and out on a timesheet roster. Completed rosters will be submitted to the Scheduling drop box.

Reporting Payroll Corrections
Employees with a payroll correction request should contact scheduling scheduling@medic911.com via email. Include the specific dates and number of hours for each date that need to be corrected. Once verified, this information will be forwarded to the Finance department for processing.

Personal Information Changes
Human Resources department should be informed of any changes in personal information by sending an email to humanresources@medic911.com. Visit Medic's extranet or contact Human Resources for more information.

Shift Bid

New Employee Assignment Bid
An assignment bid will occur prior to the new employee's completion of ride time in coordination with the Learning and Development department. Employees will be ranked and given the shift choice based upon their academy class score. This will be an online bid coordinated by the scheduling supervisor.

Annual Holiday Bid
Scheduling will conduct a holiday bid each year by August 31st. The holiday bid includes Thanksgiving, Christmas Eve and Christmas day.

Full System Shift Bid
The schedule and operations staff will complete an updated demand analysis for call volume on an annual basis. There will be some adjustments in scheduling patterns in order to address call volume changes to the call distribution patterns. Quantities of each shift type may change based upon system needs.

Medic may conduct an annual shift bid. If a full system bid is necessary due to system needs, the process and parameters to perform the bid will be communicated Agency-wide in advance of the bid.

Shift Assignment
Once an employee is assigned during an annual bid, the assignment will be considered permanent and final until the next full bid.

Out-of-Work Employees
Employees who are out of work due to temporary OJI, FMLA or military leave will be able to participate in the bid. These employees are expected to follow the shift bid guidelines provided. If an employee is on long term, approved leave with no anticipated return date, they will not participate in the bid process.

Chapter 6 – Corporate Compliance

6.1 Conflict of Interest

Effective 9/1/99

Purpose

To explain the procedure in the event a potential or actual conflict of interest should arise.

Policy

No Agency employee shall have any interests, direct or indirect, in any contract or proposed contract for materials or services to be furnished or used in conjunction with the Agency.

An employee with an actual or potential conflict of interest shall report it to his or her immediate supervisor. If the matter can be resolved such that there is not the potential for or appearance of a conflict of interest, no further action is required.

If the conflict cannot be resolved or if there is the potential for the appearance of a conflict of interest, the matter should be brought to the attention of the Executive Director or his designee through appropriate supervisory channels. The Executive Director or his designee shall ultimately determine how the conflict of interest matter shall be resolved.

6.2 Corporate Compliance

Effective 12/1/99, 6/1/2013

Purpose

The Corporate Compliance Program provides guidelines to follow whenever an employee is faced with questions of ethics or good business practices. It is designed to prevent fraud, abuse and waste. The program affirms the Agency's commitment to fair and ethical business practices and promotes adherence to applicable laws.

Policy

The Agency's Management Committee has officially adopted the Carolinas HealthCare System's Compliance Program as the model for its compliance. The Agency appreciates the willingness of CHS to share its program.

Employees are expected to be familiar and comply with the corporate compliance policies that the Agency has adopted. These policies are available on the Agency's Intranet under Corporate Compliance.

All Agency employees shall receive compliance training and applicable literature during initial orientation and on an annual basis. All questions, comments and concerns about this program should be brought to the Agency's Corporate Compliance Director.

As part of the annual performance appraisal, a signed attestation of compliance with this policy will be required of all employees.

Corporate Compliance Issues should be reported immediately to your Direct Supervisor. If needed, you may contact the Compliance Hotline anonymously. All inquiries are investigated and callers may follow up on the status; if remediation is needed efforts will be implemented.

Retaliation against an employee for providing information to the Hotline is prohibited.

6.3 Employee Records

Effective 1/1/05

Purpose

To maintain accurate employment records for all employees.

Policy

The Human Resources Department maintains a personnel file for each employee in which pertinent information related to employment is recorded.

Personnel files are considered confidential. Employees should notify the Human Resources Department any time there is a change in information such as name, address, telephone number, marital status, number of dependents, change in benefits, etc., so that the file may be kept current.

Employees who wish to inspect their personnel file may do so by notifying the Human Resources Department to set up an appropriate time for this review to take place. All personnel files are Agency property and the employee has a right to inspect the files and take notes, but no employee is allowed to remove anything from the personnel file.

Personnel records will be retained and maintained in accordance with applicable state and federal law and Agency policies.

6.4 Gifts and Gratuities

Effective 7/1/03

Purpose

To provide guidance in the event gifts and/or gratuities are being offered.

Procedure

No employee shall place himself or herself, through the acceptance of gifts or favors, in a position to be improperly influenced or give the appearance of having been improperly influenced, in the performance of his or her official duties.

No employee shall directly or indirectly solicit, accept or receive any gift or favor, whether in the form of money, services, loan, travel, entertainment, hospitality, trips, or other property of any kind, under circumstances in which it reasonably could be inferred that the gift was intended to influence the employee in the performance of his or her official duties or that the gift was intended as a reward for official action on the part of the employee.

This procedure is not intended to prohibit receiving items or souvenirs of nominal value (i.e. anything defined as having a value of less than $100) or meals served during business related meetings and other bona-fide business meals.

Examples of gifts that must be avoided for their potential to present a conflict of interest are:

1. Cash gifts of any kind or amount cannot be accepted.
2. Quid pro quo relationships or transactions are not acceptable.
3. Educational programs where more costs and program time are spent for social content (meals, entertainment, activities, etc) than for educational content.

There are certain instances where business relationships produce gifts and/or gratuities that are acceptable; however, because they may give rise to conflicts or potential conflicts, the nature and instance of these relationships must be disclosed annually to the Agency's Compliance Officer.

Any questions regarding acceptable forms of gifts and gratuities should be directed to the Agency's Compliance Officer.

6.5 Employee and Patient Confidentiality

Effective 9/1/00

Purpose

To stress the importance of maintaining a strict level of employee and patient confidentiality.

Policy

The agency prohibits release of information by unauthorized personnel concerning patients and Agency employees.

Releasing confidential information is grounds for termination of employment.

Any requests regarding Agency personnel should be directed to the Human Resources Department.

Requests for patient information such as subpoenas should be directed to the Agency's Risk and Safety Specialist's office or designee.

Any requests from the media should be referred to the Public Relations Manager. Refer to the Public Records/Public Information Policy in this chapter for more specific details.

When an employee is involved in a crisis*, whether on duty or not, that other employees would likely be interested in, the Public Relations Manager or other appropriate administrator, will:

Ensure that the employee's next of kin are properly notified and that we as an Agency offer our help and support as needed.

Determine from the employee and their family what information they want released to colleagues at Medic.

Use various appropriate means, such as pagers, e-mail, etc., to communicate as completely and fully as possible based on the employee's wishes.

*Examples of crises include motor vehicle crashes, health problems, deaths in the family, etc., and will be determined on a case-by-case basis.

6.6 Employment of Relatives

Effective 9/1/04

Policy

The employment of close relatives within the same department or unit is prohibited where there is the possibility of a conflict of interest. Close relatives shall not be employed within the same department or unit if such employment will result in one supervising a close relative, or where one member occupies a position which has influence over the other's employment, promotion, salary adjustments, and other related management or personnel considerations. Close relatives are defined as employee's spouse; biological parent or an individual who stood in loco parentis to an employee when the employee was a son or daughter; biological, adopted, or foster child, a stepchild, a legal ward, or a child of a person standing in loco parentis; brother, sister, mother-in-law, father-in-law, sister-in-law, daughter-in-law, son-in-law; grandparent, grandchild, spouse's grandparents; and step relationships.

Chapter 7 – HIPAA and Privacy

7.1 Identity Theft and Information Breach

Effective 5/1/09, 01/10/2013, revised 3/3/2015

SUMMARY STATEMENT

Mecklenburg EMS Agency ("MEDIC") is committed to maintaining the security and integrity of confidential information related to patients, employees and operations. Confidential information can include medical information, billing information, employee information, financial information, consumer accounts, as well as other confidential information. While MEDIC has implemented numerous physical, technical and administrative protections to protect this confidential information, it is possible that the security of the information may be breached and used for wrongdoing, including identity theft.

This Identity Theft Prevention Program is intended to promote the detection, prevention and mitigation of information breaches and identity theft, as well as provide guidance on how to respond in the event of a breach of confidential and personal information. It is in addition to, not in lieu of, any existing policies and procedures relating to the protection and handling of confidential information, including those related to Corporate Privacy (including all HIPAA Policies), Information Services (including the Acceptable Use Policy), and Human Resources (including Employee Information Policies).

DEFINITIONS

Identifying Information: Is any personally identifying information about a person that could be wrongfully used to commit Identity Theft. This includes a person's:

1. Last Name, including in combination with first name or first initial
2. Social security or employer taxpayer identification numbers
3. Driver's license, State identification card, or passport numbers
4. Checking account numbers
5. Savings account numbers
6. Credit card numbers
7. Debit card numbers
8. Other financial information, including billing account information
9. Personal Identification (PIN) Code
10. Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names
11. Digital signatures
12. Any other numbers or information that can be used to access a person's financial resources
13. Biometric data
14. Medical information
15. Passwords
16. Parent's legal surname prior to marriage
17. Unencrypted personal data

Identity Theft: A fraud committed or attempted using the identifying information of another person without authority. This can include an Information Breach.

Identity Theft Prevention Program: The program established by MEDIC to detect, prevent and mitigate Information Breaches and Identity Theft. *This includes the MEDIC Initial Identity Theft Prevention Program.*

Individual: A person who is the subject of the Information Breach or Identity Theft.

Information Breach: An incident where it is possible that an Individual's Identifying Information has been accessed or used in an unauthorized or illegal manner. This can include Identity Theft.

Red Flag: A pattern, practice or specific activity that indicates the possible existence of an Information Breach and/or Identity Theft.

Response Team: The Red Flag Response Team; a team charged with investigation and response to Red Flags.

POLICY

Detecting Red Flags

Vigilance for Red Flags:

A. Red Flags are usually in the form of one of the following:
    a. Suspicious documents;
    b. Suspicious Identifying Information;
    c. Suspicious or unusual use of accounts; and
    d. Alerts from others (e.g. customer, Identity Theft victim, or law enforcement)
B. Personnel handling Identifying Information should be alert to how the information is being accessed, used and maintained, both by internal and external parties, and be aware of any possible Red Flags.
C. An Information Breach is not unique to patient information; it can be in the form of unauthorized access to or use of an employee's information as well.
D. Departments with access to Identifying Information should conduct ongoing assessments of the security of the Identifying Information and of possible Red Flags. Changes to operations and handling of such information should be made accordingly.
E. Personnel should follow all security and confidentiality policies and procedures regarding Identifying Information, including those relating to protected health information and the protections under HIPAA.

Proper Use of Social Security Numbers:

A. The confidentiality of Social Security Numbers ("SSNs") should be maintained, except for proper business purposes.
    a. SSNs are a common data element sought by Identity Theft perpetrators and, consequently, personnel should be very careful in how they use, store, display, print and disclose SSNs.
    b. SSNs should not be used as publicly available identifiers.

B. It is acceptable to use SSNs for legitimate business purposes such as submitting billing claims; verifying identity; internal administration; responding to court orders, law enforcement or governmental agency demands; or other legitimate reasons.

Examples of Red Flags of Identity Theft

A. Alerts, notification and other warnings from consumer reporting or fraud detection agencies.
B. Suspicious or unexplained address and phone number changes.
C. Inconsistent information on employment records, medical records or registration information with the person or among the records.
D. Patient complains s/he is receiving bills for services s/he never received.
E. Employee claims they did not receive a paycheck.
F. Documents that appear to be forged or altered.
G. Missing laptops, security codes, key FOBs, equipment with patient or employee information on it, and other devices or information that could be used to access Individual Information.
H. Unauthorized access by personnel to servers or systems.

Reporting a Red Flag

If you suspect information has been shared and/or there has been an information breech please take the following steps:

1. Contact Your Immediate Supervisor. If there is still suspicion that the information being provided by the individual is false after the inquiry or information has been shared, the incident should be reported immediately to the Red Flag Response Team by **calling 704-943-6220**. The Response Team will handle the Red Flag according to applicable procedures.
2. Report Information. In making the report, the following information should be given:
    a. The name, number and department of the person making the report
    b. The nature of the Red Flag, the information involved and the date it occurred
    c. The name of the individual who is the source of the Red Flag, as well as the name of the suspected victim
    d. Any other relevant information

Red Flag Response Team

The Red Flag Response Team will follow its procedures and process in handling the Red Flag. Personnel should be cooperative and forthcoming with information when asked by the Response Team or members of other affected departments.

In no event should personnel contact the potential victim of the Red Flag unless expressly directed to do so by the Response Team – the Response Team will handle all communications and contact with the patient, victim, law enforcement, media or other entities or other persons.

Ongoing Self-Assessment

A. Departments handling Identifying information should continually conduct a self-assessment for its exposure to Information Breaches, how to evaluate them, learn from experiences with them and how to improve prevention and reaction to them.

B. Medic's Public Relations Director should be contacted immediately if there are any inquiries from the media at 704-943-6160.

7.2 Accounting for Disclosures of Patient Information
Effective 2/1/09, 01/10/2013

POLICY

This policy establishes the procedure for a patient, a patient's legal representative or other authorized party ("Requestor") to request an accounting of patient information disclosures.

PROCEDURE

A. Upon receipt of request for an accounting of patient information disclosures ("Accounting of Disclosures") from the Requestor, the Agency shall provide Requestor with the form entitled Authorization for Release of Information Form which is attached. Requestor must complete and sign the Request Form. The Agency shall log requests for Accounting of Disclosures in a central database.

   a. *Release of patient records is a function of the Risk and Safety office. All requests shall go to the Risk and Safety office for verification and release.*

B. The person receiving the request shall verify that the Request Form is signed by Requestor as set forth in the administrative policy, v*erifying the Identity of a Person Requesting Patient Information*

C. Disclosures may be released in the following circumstances without a patient's or a patient's legal representative's authorization provided the *Minimum Necessary Requirement, verifying the Identity of a "Person Requesting Patient Information"* policy is followed:

1. As Required by Law
2. Public Health Activities
3. To Public Health Agency
4. Child Abuse Cases
5. Person Subjected to FDA Regulations (Pharmaceutical & Medical Device Manufacturers – principally for MedWatch form)
6. To Report Adverse Events to Manufacturers as Required by the FDA
7. As Required by the FDA
8. To Enable Product Recalls
9. To Report Diseases as Required by Law
10. Abuse/Neglect Reports (must notify patient if reasonable)
11. Health Oversight Activities Including Quality; Fraud and Abuse; Criminal; Discipline provided to an Appropriate Government Entity
12. Judicial/Administrative Procedures Pursuant to Law (As an EMS Provider per NC Statute 143-518 will release with court order only).
13. Certain patient information to Law Enforcement Looking for Suspect, Fugitive or Witness
14. To Disclose Crime Victim Data to Law Enforcement
15. Crime on Premises
16. To Alert Law Enforcement of Crimes in Emergencies
17. To Medical Examiners
18. Funeral Directors
19. For Tissue Donation
20. To Avert a Serious Threat to Health or Safety
21. On Military Personnel as Required by the Military
22. To Protect the President or Other High Level Government Officers

including Foreign Leaders of State*

23. For National Security and Intelligence*
24. To Prisons about Prisoners*

*Accounting for disclosure is not required

D. The Agency will review reports from the Accounting for Disclosure Requestor's, including denials to Requestor. Responses to requests will be logged in the Agency's database.

E. The Agency shall receive appeals to any denials and log such appeals in the central database. The Facility Privacy Director will review appeals and respond to the requestor. The Agency shall log responses to appeals in the central database.

F. Support of the Agency database shall be the responsibility of Facility Security Director.

MECKLENBURG EMS AGENCY

Request for Accounting of Non-Authorized Disclosures of Patient Information

I hereby request the accounting of non-authorized disclosures of my patient information.

Patient Name (*First Middle/Maiden Last Suffix)*	
Current Mailing Address *(Street Address, City, State, Zip Code)*	
Home Telephone	**Work Telephone**
Social Security #	**Date of Birth**
Dates of Service Requested **TO:**	**FROM:**

You may request a listing of disclosures for any segment of the most recent 6 years dating from April 14, 2003.

There will be a charge of at least $25 per request after the first request within a 12 month period.

Facility Where Services Rendered	

(Patient/Authorized Representative*)

Printed Name	**Signature**	**Date**	**Time**

* If Authorized Representative, please indicate relationship to patient: Spouse, Parent, Other _____

FOR MECKLENBURG EMS AGENCY USE ONLY

- Identification verified
- Processing fee received
- Copy of request given to patient MEDIC Employee

Requestor

Printed Name	Signature	Date	Time

MEDIC Employee

Printed Name	Signature	Date	Time

7.3 De-Identification-Removal of Patient Identifiers

Effective 4/1/09, 01/10/2013

POLICY

Patient information includes any piece of information identifying an individual, whether used alone or in combination with other information. Any information that does not contain patient identifiers or a means to re-associate identifiers is not subject to the HIPAA Privacy Rule because it is de-identified; thus, it can be used and/or disclosed without patient authorization. A MEDIC information provider is any individual, department or entity providing patient information to another individual, department or entity.

PROCEDURE

1) MEDIC Approved Method of De-identification

    a. The only approved method for de-identifying information at MEDIC is the safe-harbor method unless the Facility Privacy Director approves an exception.

    The Safe harbor method removes all of a list of enumerated identifiers such that the information cannot be used alone or in combination to identify a subject of the information.

    b. If the information is de-identified and no means of re-identification is supplied to the recipient of the information, it is not subject to the HIPAA Privacy Rule.
    c. If the information is re-identified, the information once again becomes protected health information and is subject to HIPAA's privacy regulations.
    d. Each MEDIC provider of information, regardless of form, will be responsible for determining whether the information requested contains patient identifiers and, therefore, subject to HIPAA's privacy regulations.
    e. A log of requests and decisions about providing PHI should be maintained by all formal and informal data providers, such as those areas that produce reports for decision support or receive report/data/information and pass it on to others.

2) Process for De-identifying Patient Information

    a. Information is considered de-identified when MEDIC has no reasonable basis to believe that the information can be used to identify an individual patient. To de-identify information, the following data elements must be removed:

        1) Name (including biometric identifiers, including finger and voice prints and full face photographic images and any comparable images)

        2) Location of individual (can use state, but no location more specific).

        3) Dates (all dates related to the subject of the information, i.e., birth dates, admission dates, discharge dates, encounter dates, surgery dates, etc.)

        4) Numerical identifiers (addresses, telephone numbers, email, fax numbers, zip codes, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, device identifiers and serial numbers, web universal resource locators (URLs), internet protocol (IP) address

numbers) driver's license numbers, vehicle identifiers, etc).

b. The MEDIC user needs to take into consideration that free text fields may contain identifiable elements. If identifiable elements within an unstructured free text field cannot be filtered, the free text must be removed in order to complete de-identification.

C. Special Circumstances – De-identification

1. A "limited data set" may be used for research, public health and health care operation activities provided the data does not include direct identifiable information (i.e., name, street address, etc.)
2. A Data Use Agreement which is defined as a documented agreement between MEDIC and the recipient of a limited data set is required for use of the limited data set.

   Agreements must:

   a. Establish the permitted uses and disclosures of the limited data set. The Agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements set forth in this policy.
   b. Establish who is permitted to use or receive the limited data set; and
   c. Provide that the limited data set recipient will:
      1) Not use or further disclose the information other than as permitted by the Agreement or as otherwise required by law;
      2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the Agreement;
      3) Report to MEDIC any use or disclosure in violation of the Agreement (of which the recipient becomes aware.
      4) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient; and
      5) Not identify the information or contact the individuals.

   The following data elements may be used in a limited data set:
      a. Age (Individuals 90+ years old must be aggregated to prevent potential identification)
      b. Race
      c. Ethnicity
      d. Marital status
      e. Codes (a random or fictional code that can be used to link cases or re-identify the health information at a later time. Codes may not be a derivative of the individual's social security number or other identifiable numerical codes, i.e., birth date, fax number, etc.)
      f. Dates (birth date, admission date, discharge date, date of death)
      g. Town or city, state, zip code

4. Questions concerning de-identification of patient information should be forwarded to the MEDIC Facility Privacy Director.

D. Process for Re-Identification

1. The MEDIC information provider may assign a code to allow de-identified information to

be re-identified. The code or mechanism used to re-identify information may not be derived from information related to the individual or otherwise information that could be translated to identify the individual.

2. The MEDIC information provider is prohibited from disclosing the mechanism/codes for re-identification (i.e., tables, codes or algorithms). If the MEDIC user discloses a key or mechanism for re-identification of the health information, the information is no longer considered de-identified and the exemption to the HIPAA Privacy Rule no longer applies (i.e., patient consent and/or authorization is required prior to use.)

7.4 Duties of the Facility Privacy Director and Facility Security Director

Effective 2/1/09, 01/10/2013

POLICY

MEDIC shall designate a Facility Privacy Director (FPD). The privacy official is responsible for the development, implementation and maintenance of privacy and security policies and procedures for the organization. The Facility Privacy Director will oversee the implementation of the patient privacy policies and procedures at Medic and assist in operating in accordance with the HIPAA policies.

MEDIC's FPD shall be responsible for monitoring MEDIC's overall HIPAA program and ensure that an effective privacy and security program is in place at each MEDIC facility to protect the privacy of each patient.

1. The duties of the FPD shall include, without limitation, the following:

    a. To oversee the development, distribution and implementation of MEDIC's HIPAA policies and procedures designed to facilitate compliance with HIPAA.
    b. To periodically review policies and procedures and design and implement needed updates.
    c. To monitor for significant changes in the law and modify policies as appropriate.
    d. To advise and communicate policy changes as indicated.
    e. To promote open lines of communication so that employees feel free to report concerns, questions, and instances of improper conduct without the fear of retaliation.
    f. To investigate alleged HIPAA violations (i.e., reported directly to the CHS Corporate Privacy Department via the CHS Customer Careline and others as applicable.)
    g. To establish and administer with Human Resources a consistent disciplinary process in response to improper uses or disclosures of Patient Information across all workforce members.
    h. To consult with Medic's Agency Legal Counsel and/or CHS's Legal Department on facets of HIPAA that are unclear or difficult to understand or as policy directs.
    i. To coordinate any investigation or survey activities initiated by the Office of Civil Rights.
    j. To keep Executive Director and Leadership Team informed about Medic's Privacy compliance efforts.
    k. To oversee the educational and training aspect of the HIPAA privacy and security efforts and the development of ongoing education and training materials.
    l. To monitor staff attendance/participation to ensure HIPAA educational requirements are met (e.g., evaluate test outcomes to determine whether staff achieved the expected competence in the subject matter).
    m. To verify that privacy risk assessments, auditing and monitoring programs routinely occur at Medic.

    The Agency HIPAA Facility Privacy Director is:

    Jeff Keith
    Deputy Director
    704.943.6160
    jeffk@medic911.com

Exhibit I
Mecklenburg EMS Agency Facility Privacy Director Responsibilities

The Facility Privacy Director (FPD) oversees the implementation of MEDIC's patient privacy policies and procedures at MEDIC and assists the Facility in operating in accordance with the HIPAA Policies. The FPD must function as an independent and objective individual who reviews and evaluates privacy issues/concerns within the Facility.

Responsibilities:

1. To oversee compliance with the HIPAA Privacy Rule at the Facility (e.g., make sure departmental policies comply with MEDIC's administrative policies);
2. To coordinate privacy violation investigations at the Facility;
3. To oversee privacy training programs at the Facility;
4. To report to the Facility Privacy Director regarding privacy issues/violations at the Facility;
5. To participate in privacy risk assessments, auditing and monitoring programs at the Facility as needed; and
6. Others as needed.

Exhibit II
Mecklenburg EMS Agency Facility Security Director Responsibilities

The Facility Security Director (FSD) oversees the implementation of MEDIC's patient security policies and procedures at MEDIC and assists the Facility in operating in accordance with the HIPAA Policies. The FSD must function as an independent and objective individual who reviews and evaluates security issues/concerns within the Facility.

Responsibilities:

1. To oversee compliance with the HIPAA Security Rule at the Facility (e.g. make sure departmental policies comply with MEDIC's administrative policies);
2. To coordinate security violation investigations at the Facility;
3. To oversee security training programs at the Facility;
4. To report to the Chief Privacy Officer and Medic's FPD regarding security issues/violations at the Facility;
5. To participate in security risk assessments, auditing and monitoring programs at the Facility as needed; and
6. Others as needed.

7.5 HIPAA Privacy Sanctions
Effective 2/1/09, 01/10/2013

POLICY
MEDIC has a duty to reasonably safeguard protected health information (PHI) from intentional and unintentional misuses or disclosures. Failure to comply with the HIPAA Privacy regulations and related MEDIC policies and procedures (collectively, the "Privacy Standards") will result in disciplinary action. The disciplinary action shall be based on the severity and context of the violation and shall be in accordance with existing MEDIC policies and/or appropriate legal action. Remediation steps may vary slightly by type of employee but ultimately deliver similar sanctions up through termination for similar violations. (Please see Exhibit I).

ENFORCEMENT AND DISCIPLINE
MEDIC shall generally utilize a progressive discipline process for infractions committed by employees. Certain cases may warrant escalation of discipline, including skipping steps and terminating employment. Disciplinary actions shall not be limited to MEDIC employees. Contractual relationships, business agreements or any other relationship with MEDIC may also be terminated as a result of a violation of the HIPAA Standards. Disciplinary actions shall vary depending on the severity of the violation possibly coupled with other documented performance deficits.

In determining and administering the appropriate disciplinary response to an improper use or disclosure of PHI, please consult the Facility Privacy Director. The Facility Privacy Director will provide evaluation and guidance in the remediation process thus providing consistency for similar cases. MEDIC will take into consideration whether the incident is a first offense or whether a pattern or practice of improper conduct exists. In addition, MEDIC will determine whether the improper use or disclosure of PHI was:

- Accidental (carelessness, acting in good faith)
- Made knowingly or willingly in violation of the Privacy Standards
- Made with malicious disregard of the Privacy Standards (acted under false pretenses and/or planned to sell, transfer and/or use for commercial advantage, personal gain or to inflict harm.)

The attached Exhibit I delineates the sanctioning body by employee and student. Exhibit II lists examples of improper uses and disclosures of PHI and the expected disciplinary response for the offense.

NON-RETALIATION
No individual who identifies a practice that they believe to be inappropriate or unlawful will be retaliated against. All employees have the responsibility to report the violation to the MEDIC Privacy Officer. However, employees must realize that disciplinary action shall be taken if MEDIC reasonably concludes after investigation that such employee's report of wrongdoing was intentionally fabricated, distorted, or exaggerated by the employee in any way.

COMPLAINT MECHANISM
MEDIC employees shall use the MEDIC Chain of Command attached as Exhibit III to report improper uses or disclosures of PHI. For example, MEDIC employees should first report the incident to their supervisor. If the issue concerns their supervisor, or if the employee is uncomfortable discussing the violation with their supervisor, they may contact their manager. If the employee is uncomfortable discussing the violation with their manager, the employee may contact the MEDIC Facility Privacy Director at 704-943-6160 or the MEDIC Executive Director

at 704-943-6050. Patients should contact the MEDIC Privacy Officer to report potential Privacy violations.

RESPONSE AND PREVENTION

Complaints received by the MEDIC Facility Privacy Director will be documented using the elements contained in the "Mecklenburg EMS Agency Corporate Privacy Investigation Report" attached as Exhibit IV. The MEDIC Facility Privacy Director will review such reports, as well as any other reports received and conduct a preliminary inquiry to determine what steps will be taken.

Where indicated, the MEDIC Facility Privacy Director, with the assistance of the CHS Corporate Privacy Department and/or legal representation shall assess how the information disclosed might cause harm and take appropriate steps to mitigate such harm. For example, if PHI were inadvertently provided to a third party without authorization in a domestic abuse situation, MEDIC would promptly contact the patient as well as appropriate authorities and apprise them of the potential danger.

The MEDIC Facility Privacy Director shall maintain a record of complaints filed along with a brief description of the resolution of such complaints, if any. MEDIC's document retention plan shall include provisions to ensure that all records related to reports of wrongdoing are preserved in accordance with law.

Individuals who would like to know how to file a complaint with the Secretary of the United States Department of Health and Human Services should be encouraged to call the MEDIC Facility Privacy Director.

Exhibit I Remediation Steps by Group

Group	Policy	Example Remediation Steps	Sanctioning Body
Employees	**Human Resources**	**-Level I – Accidental**	**Human Resources**
Students:	**Operations Supervisor**	**Documentation and discussion**	**Operations**

Exhibit II
ENFORCEMENT AND DISCIPLINE
DISCIPLINARY RESPONSES

PURPOSE
There are three levels of Privacy violations and resulting sanctions:

1. Accidental Disclosure of Patient Information
2. Knowing or Willful Disregard of the Privacy Standards (as defined in the policy attached hereto)
3. Malicious Disregard of the Privacy Standards

The purpose of the three levels of privacy sanctions is to give employees an opportunity for correction of inappropriate behavior. However, certain types of misconduct are so serious that they may warrant skipping one or more of the levels even through immediately termination.

The three step disciplinary process for HIPAA typically excludes coaching, as all employees have received HIPAA training at least through but not limited to the HIPAA Privacy & Security Ace Module and Posttest:

1. Level I Violation -Accidental Disclosure of Patient Information

   An employee commits a Level I violation when such employees unintentionally accesses, reviews, or reveals patient information without a HIPAA defined legitimate "need to know." Lack of education may be considered in remediation of Level I violations, but does not excuse the violation. **Examples include but are *not* limited to the following:**

   a. Failing to sign off an unattended computer terminal
   b. Failing to secure information in a reasonable manner
   c. Discussing patient information in a public area without discretion
   d. Accessing his or her own records without using the proper procedure for requesting and gaining access
   e. Asking another employee to access his or her own record
   f. Faxing PHI incorrectly the second time within a relatively short period of time
   g. Leaving PHI in public areas (i.e. public bathrooms, hallways and cafeteria's)
   h. Laptop, EPCR, PDA. Blackberry or any other mobile device containing PHI left in an unsecure manner.

   Corrective Action for a Level I Violation will be coupled with other performance deficits. For corrective action please consult with Human Resources. Discovery of a pattern of violations will result in the accumulation of the individual discipline for each violation.

2. Level II Violation – Knowing or Willful Disregard of the Privacy Standards or a repeated Level I violation:

   An employee commits a Level II violation when such employee accesses, reviews, discloses or discusses patient information for purposes other than those allowed under HIPAA: patient care or the performance of such employee's specific job responsibilities for treatment, payment or healthcare operation (TPO).

   Examples include but are not limited to the following:

a. Accessing an employee's patient record outside the employee's defined job responsibilities (i.e. to determine for example the birth date or address of a friend or relative) Accessing the record of a patient out of concern or curiosity.
b. Reviewing a publicized/famous person's record
c. Using another employee's access code.
d. Using aggregate data without facility approval
e. Releasing patient data inappropriately
f. Repeating a Level I violation even as a part of the same incident
g. Mixing patient information such that an inappropriate disclosure occurs or could occur.
h. Giving results to unauthorized persons.
i. Manager who has repeat violations in their area of responsibility and are unable to determine who is responsible for the HIPAA violation.
j. Laptop, EPCR, PDA, Blackberry or any other mobile device containing unencrypted and/or non/weak password protected PHI that is stolen where the user has not followed MEDIC policy for securing portable equipment (employing lock down kit, strong password with no PHI stored on hard drive, etc.)
k. Disposing of PHI inappropriately.
l. Accessing patient information to make an employment decision.
m. Manager telling co-workers about the patient information of an employee (i.e. reason for absence without employee's explicit permission).
n. Taking PHI home without manager approval.
o. Failure to return PHI to the employee's assigned work unit.
p. Allowing observation of a patient without proper authorization.
q. Placing patient information into the public domain in any way unencrypted (i.e. Internet).

Corrective Action for a Level II Violation will be coupled with other performance deficits. For corrective action please refer to the following Human Resources Discipline Policy or consult with Human Resources. Discovery of a pattern of violations will result in the accumulation of the individual discipline for each violation.

3. <u>Level III Violation -Malicious Disregard of the Privacy Standards</u>
A employee commits a Level III violation when such employees accesses, reviews, discloses in any way such that others receive the PHI regardless of the stated intent of the person who disclosed the PHI or discusses patient information for personal reasons, personal gain or with malicious intent. **Examples include but are not limited to the following:**

a. Releasing data for personal or business gain
b. Compiling a mailing list for personal use
c. Compiling a mailing list for sale to a third party for personal gain
d. Reviewing a patient record to use information in a personal relationship
e. Destroying or altering data intentionally
f. Releasing data with the intent to harm an individual or MEDIC
g. Repeating a Level II violation even as part of the same incident
h. Taking or accessing PHI from a non-work location to show others (family members, spouse, life partners or friends)

Corrective Action for a Level III Violation will be coupled with other performance deficits but will likely result in termination of the employee. For corrective action please refer to the Human Resources Discipline Policy or consult with Human Resources. Discovery of a pattern of violations will result in the accumulation of the individual discipline for each

violation.

4. Photography (Except as described in the Policy: *Protection, Release and Review of Protected Health Information (PHI)*

    a. Photography or photos of any patient or patient identifiers are strictly prohibited. That includes any part of a patient (like an isolated injury) even if the patient is not visibly identifiable in the photo. If someone e-mails, texts or shares in any way such photos or patient identifiers to you, you must not forward these and they should be promptly deleted or destroyed. You also have a responsibility (under corporate compliance guidelines) to identify such HIPAA related violations to proper authority.

    b. If it is clinically pertinent to photograph a scene, such as documenting damage to a vehicle or other mechanism of injury, it should be done so after the patient is extricated and clear of the photograph. Such photos should be shown only to the receiving physician and then promptly deleted. These photos must not be forwarded or shared with anyone else.

    c. Not only is the camera capability of the cell phone restricted, any use of a cell phone, including text messaging while driving an Agency vehicle, or while engaged in patient contact is prohibited. Exceptions: Use of the phone to contact an out of county hospital or to make a call on behalf of a patient and as a back-up communications device during a radio system failure or overload.

    d. Using a hands free device while driving is acceptable if you are not dialing or otherwise distracted by phone operation. However, the driver of an Agency vehicle responding to an emergency should never be using a cell phone in any way.

Please contact your supervisor if you have any questions about these policies, HIPAA or Corporate Compliance.

Medic takes any HIPAA violation very seriously and will result in disciplinary action up to and including termination.

Exhibit III MEDIC Chain of Command

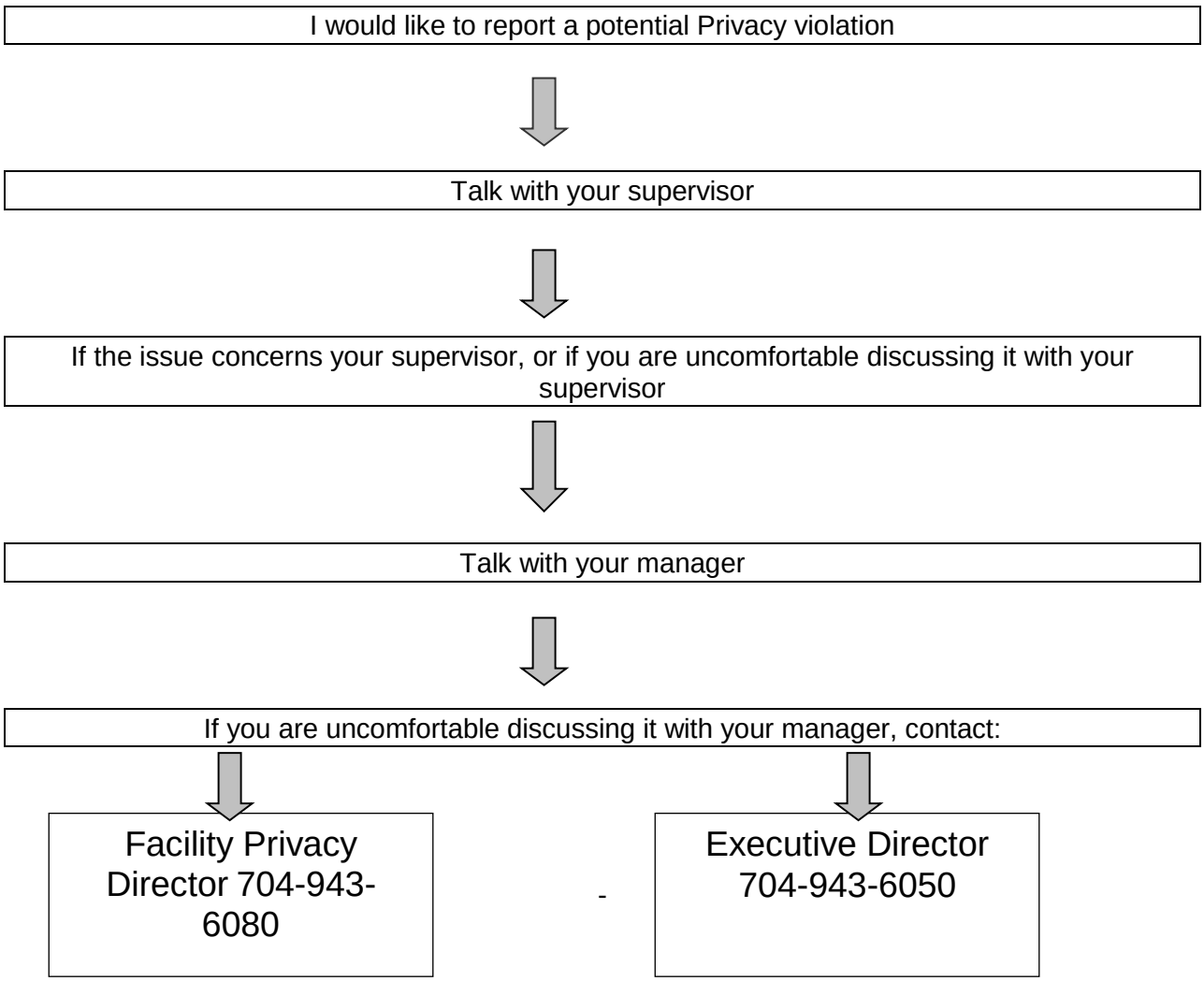


Exhibit IV
Mecklenburg EMS Agency Corporate Privacy Investigation Report

Privacy Log#:_____

Date of incident: _____

Investigator Name and Facility: _____

Consulted with to the Corporate Compliance Privacy Dept. on: _____
Notes from discussion with corporate privacy department:

Response due date to the Corporate Compliance Privacy Department:

Investigation: Please document the steps of the investigation by providing responses to the following questions/requests. If the questions/requests do not apply, indicate your response by "N/A".

- Provide the details of the allegation, including date of allegation, people involved and PHI involved
- Describe the steps taken to investigate this allegation.
- Describe the findings and conclusion of the investigation? (All comments or responses received by investigator from involved management should be added to this report section without alteration.)
- Describe the disciplinary action and where such action is documented.
- Describe corrective action necessary to prevent further violations where applicable: - Relevant education provided to all department staff to prevent further instances? - Revision of any policies and procedures? -Other – please explain.

Note: **MEDIC** should contact the complainant (if possible) and provide a brief and high level response to the concern after final consultation with the CHS Corporate Privacy Department. Specific employee's disciplinary action is not to be shared.

Date completed: _____If you have any questions, please contact MEDIC Corporate Privacy at 704- 943-6080.

7.6 Minimum Necessary Requirement
Effective 2/1/09, 01/10/2013

POLICY
MEDIC must limit any access to patient information to that which is reasonably necessary to accomplish the allowable payment or health care operations purpose for which the request is made. Full disclosure of all patient information is allowed for treatment purposes.

PROCEDURE

1. Exceptions to the Minimum Necessary Requirement The Minimum Necessary

Requirement does *not* apply to:

a. Disclosures to or requests by a health care provider for treatment purposes;
b. Uses or disclosures made to the individual who is the subject of the patient information;
c. Uses or disclosures made pursuant to an authorization requested by the individual;
d. Disclosures made to the Department of Health and Human Services (DHHS) when disclosure of information is required under the rule for enforcement purposes (i.e., in response to a complaint filed with the Secretary of DHHS);
e. Uses and disclosures that are required by law (i.e., victims of abuse, neglect or domestic violence; judicial administrative proceeding; and law enforcement purposes).

2. Use of Patient Information

a. The Agency will be responsible for establishing policies and procedures that identify the type(s) of persons, the conditions, and categories of information that MEDIC employees may access based on job responsibility. Policies and procedures should:
    - Identify the persons or classes of persons in MEDIC's workforce who need routine access to patient information;
    - Identify the type and amount of Patient Information necessary to carry out their duties; and
    - Identify situations, other than treatment, where it is necessary for Agency staff to have access to the entire medical record.

b. The Agency management will authorize access to computerized health information. Use of this information will be limited based on reasonable determinations regarding an individual's position and/or department. An individual's access will be controlled via user ID and password; the sharing of logon IDs and passwords is prohibited.

3. Routine or Recurring Requests and Disclosures for Patient Information

a. Requests for patient information made on a routine or recurring basis shall be limited to the minimum amount of patient information necessary to meet the needs of the request/disclosure.
b. The Agency will be responsible for determining its 'minimum necessary' definitions and establishing standard protocols for routine or recurring requests/disclosures (i.e., list the patient information that is routinely disclosed to a medical transcription service.).
c. Individual review of the request will not be required for requests/disclosures made on a routine or recurring basis where standard protocols have been developed.

However, annual or some regular review should be made for routine on recurring requests to ensure the requests are still valid and necessary.

4. Non-routine Request for Disclosure of Patient Information
    a. Non-routine requests for patient information will be reviewed on an individual basis to limit the patient information sought/disclosed to the minimum amount necessary to accomplish the purpose of the request/disclosure.
    b. The Agency will be responsible for establishing a procedure for reviewing such requests on an individual basis *unless* the request/disclosure is to a health care provider for treatment purposes.
    c. Disclosures or requests by a health care provider for treatment purposes are *not* subject to the minimum necessary standard.
    d. Disclosures to/requests authorized by the patient will *not* be subject to the minimum necessary standard but are subject to the terms of the authorization.
    e. MEDIC will *not* use/disclose an entire medical record if it is determined after conversation with requestor or established protocol that the entire medical record is not justified as the amount that is reasonably necessary to accomplish the purpose of the use/disclosure. If it is determined after conversation with information requestor or after review of established protocol that the entire medical record is not necessary to accomplish the intended use/disclosure, MEDIC may not release the entire medical record.

5. Reasonable Reliance
    a. The Agency will rely on the judgment of the party requesting the disclosure as to the minimum amount of patient information reasonably necessary for the stated purpose when:
        - Making permitted disclosures to public officials, if the public official represents that the patient information requested is the minimum necessary for the stated purpose(s);
        - The patient information is requested by another covered entity (i.e., health care provider, health plan, or health care clearing house);
        - The patient information requested is the minimum necessary for the stated purpose and requested by a professional who is requesting patient information for the purpose of providing professional services to the Agency. (i.e., member of MEDIC's workforce or business associate or
    b. MEDIC employees should always exercise judgment/discretion when making determinations about disclosures and limit the disclosure to that amount of patient information necessary to satisfy the purpose of the request.

I. Restrictions
    a. Use/disclosure of patient information will be subject to any agreed upon patient restriction(s) entered into by MEDIC with the patient.
    b. The Agency will be responsible for establishing a procedure to check for restrictions prior to using / disclosing patient information.
    c. Patient information may not be used / disclosed without proper consent or authorization.

7. When Requesting Patient Information:
    a. When requesting patient information from other covered entities, the Agency will limit any request for patient information to that which is reasonably necessary to accomplish the purpose for which the request is made.

7.7 Patients Request for Privacy Protections (Restrictions & Confidential Communications)
Effective 8/1/09, 01/10/2013

POLICY
Medic permits patients to request privacy protections related to Patient Information; requests will be considered on a case-by-case basis.

A. Patients may request that Medic **restrict** certain uses and disclosures of Patient Information as described in this policy.
B. Patients may request to receive **confidential communication** of Patient Information as described in this policy.

PROCEDURE

Patient Requests for Restrictions

A. Medic permits patients to request restriction(s) on how patient information is used or disclosed for the following activities: treatment, payment, health care operations, involvement of others in patient care, and/or notification activities to alert next of kin of the patient's transport.
    1. The request for restriction(s) should be put in writing using the Confidential Communication/Restriction Request Form (Attachment A).
    2. Completed forms should be forwarded to Facility Privacy Director or Risk and Safety Officer or designee for appropriate processing except as noted below.
    3. Completed forms should be filed or distributed as follows:
        a. Original – Risk and Safety Officer
        b. Copy – given to the individual requesting the restriction
B. Medic is not required to agree to restriction requests; however, Medic will abide by any agreed upon restrictions except in emergency situations.
    1. If the individual who requested the restriction requires emergency treatment and the restricted patient information is needed to provide such treatment, Medic may use or disclose the restricted information to a health care provider for treatment purposed.
    2. If restricted patient information is disclosed to a health care provider for emergency treatment, Medic will ask that provider *not* to further use or disclose the information.
    3. Any restriction Medic agrees to will not be effective to prevent uses or disclosures of patient information permitted or required:
        a. By the Secretary of DHHS for investigation purposes;
        b. Without authorization or opportunity to object as described in §164.512 or NC General Statute 143-158 (see Attachment B for full list).
    4. Medic will be responsible for establishing a mechanism (i.e., User Defined Field or other) to alert users of the restriction(s), so they can comply.
        a. Documentation regarding the restriction must be maintained for six years from the date it was created or the date it was last in effect, whichever is later.
        b. A restriction will only be binding for Medic and will only be effective for that specific patient encounter.
    5. Medic may terminate its agreement to a restriction if:
        a. The individual agrees to or requests the termination in writing;
        b. The individual orally agrees to the termination and the oral agreement is documented; *or*

c. Medic informs the individual that it is terminating its agreement to a restriction. When Medic terminates its agreement, such termination is effective only with respect to the PHI created or received after Medic so informed the individual.

Patient Requests for Confidential Communications

A. Medic permits patients to request communication of patient information via alternative means or at alternate locations and will accommodate reasonable requests of this nature.

1. Requests for confidential communications should be made in writing using the Confidential Communications/Restriction Request Form (Attachment A) and must specify the alternative address or method of contact being requested. The Finance Department or designee will complete the bottom portion of the form and ensure copies are provided to the Requestor, placed with the Requestor's Patient Record and filed with the Facility Privacy Director.

2. Medic may utilize an alternate mailing address provided by the Patient/Responsible Party for billing correspondence. Medic is unable to maintain or administer more than one mailing address for a patient. Therefore, the mailing address provided during the patient's most recent transport or patient encounter will be used for all Medic mailings until such time that a new address is provided.

3. Patient requests for communication of patient information via alternate means will be considered on a case-by-case basis. Reasonable requests will be accommodated when possible (i.e., if mechanisms exist to accomplish the request consistently in accordance with the normal course of daily business activities).

Attachment A: Confidential Communication/Restriction Request Form

Medic is not required to agree to a restriction or confidential communication request. Receipt of such requests does not guarantee approval. If Medic agrees to a restriction or confidential communication, the change will be effective for the specific patient visit/encounter during which it is processed and future bills. Some confidential communications may require an authorization (email, for example).

1. Signature:_____ 2. Date: _____
(Patient / Legal Representative)

3. Relationship to Patient: _____

An agreement to a restriction may be terminated by Medic or the individual making the request. Requests for termination of a restriction should be submitted in writing to: Mecklenburg EMS Agency; Attention: Facility Privacy Officer; 4525 Statesville Road, Charlotte, North Carolina 28269.

For Mecklenburg EMS Agency Use Only

Instructions: Complete this form to document a patient's request for confidential communications/privacy restrictions. Requests must be noted in writing. The Confidential Communication/Restriction Request Form must be signed and dated by the patient or his/her legal representative at the time the request is made.

4. Patient Name: _____

Document Confidential Communications:

Use an alternate means of communicating with the patient. Please list the means by which you request Medic to contact you in the future.

_____

Use an alternate mailing address for patient to receive Medic correspondence. (Please note this is the address Medic will use for all mailings to you. Medic is unable to administer more than one mailing address for a patient. The mailing address provided during the patient's most recent transport or encounter will be used for all Medic mailings until such time that a new address is provided).

Alternate mailing address: _____
_____

City / State /
ZipCode:_____/_____/_____

Document Requested Restrictions. Restriction(s) that are not listed below must be referred to the Facility Privacy Officer for consideration.

O**ther Request as Described:** _____

_____

_____

Requested Confidential Communication/Restriction(s) has been:

☐Accepted ☐Denied

If denied, note reason: _____

Signature: _____

Date: _____ Unit / MR#: _____

Print Name & Title: _____

Attachment B

Disclosures That Cannot Be Restricted

Any restriction Medic agrees to will not be effective to prevent uses or disclosures patient information permitted or required under § 164.512 of the HIPAA Privacy Rule or NC General Statue 143-1518. . These activities are discussed throughout Medic's administrative policy manual. Please reference the applicable policy for detailed information related to them. These activities include the following:

Uses and Disclosures Required by Law
Uses and Disclosures for Public Health Activities
Disclosures about Victims of Abuse, Neglect, or Domestic Violence
Uses and Disclosures for health Oversight Activities
Disclosures for Judicial and Administrative Procedures including pursuant to a court order
Disclosures for Law Enforcement Purposes
Uses and Disclosures about Decedents
Uses and Disclosures for Cadaveric Organ, Eye or Tissue Donation Purposes
Uses and Disclosures for Research Purposes including health research projects under rule adopted by NC Medical Care Commission.
Uses and Disclosures to Avert a Serious Threat to Health or Safety
Uses and Disclosures for Specialized Government Functions
Disclosures for Workers' Compensation
Disclosure to a Medical Review Committee or Peer Review Committee
Disclosure to a state-wide data processor

.

7.8 Protection, Release, and Review of Protected Health Information (PHI)

Effective 5/1/09, 01/10/2013

POLICY

Provide guidelines for the use and disclosure of Patient Health Information (PHI) to ensure that the Agency and its First Responders comply with state and federal laws protecting patient privacy including, but not limited to, NC General Statute 143-518 and HIPAA

For the purposes of this Policy, the following definitions will apply:

Agency – Mecklenburg Emergency Medical Services Agency, including the Agency's First Responders.

Authorized Persons – the Agency's Risk and Safety Specialist, Director of Human Resources and Executive Director

Patient Financial Records – personal financial records compiled or maintained by the Agency in connection with admission, treatment and discharge of individual patients, including, but not limited to, patient charges, patient accounts and patient credit histories.

Patient Identifiable Data

1. Name
2. Address, including zip code
3. Social security number
4. Age (if over 89 years of age)
5. Telephone number
6. Fax number
7. E-mail address
8. Medical records number
9. License plate number
10. Vehicle identifiable number
11. Full-face photographs or other photographic image by which patient may be personally identified
12. Other information by which the identity of the patient could be determined with reasonable accuracy and speed either directly or by reference to other publicly available information.

Patient Medical Records include:

1. Records compiled or maintained by the Agency in connection with the dispatch, response, treatment or transport of individual patients, including, but not limited to, patient care reports, CMED records, 911 tapes, recorded radio traffic and other patient information collected and maintained by the Agency and its First Responders**.**
2. Records compiled or maintained by the Agency in connection with statewide trauma system.
3. Other records compiled or maintained by the Agency that contain personal information relating to a patient's physical or mental condition, medical history, medical treatment and/or patient identifiable data.

Records – all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data processing records, artifacts or other documentary material, regardless of physical form or characteristics, made or received by the Agency in the transaction of business.

POLICY GUIDE

Patient information is confidential. Patient Medical Records and Protected Health Information are strictly confidential and will not be released to the public or any Agency personnel, except for treatment, payment or healthcare operations.

PROCEDURE

Valid Authorization:

1. A valid authorization to release or review PHI must be signed by the patient or the patient's legal representative, whose relationship is stated. The authorization must be presented in writing to the Risk and Safety Officer, FPD or designee. The authorization will apply only to the date(s) of service specified. A valid authorization must contain the following elements:

a. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

b. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

c. The name or other specific identification of the person(s), or class of persons to whom the Agency may make the requested use or disclosure;

d. A description of each purpose of the requested use or disclosure;

e. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;

f. A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;

g. A statement that the Agency may not condition treatment, payment, enrollment, or eligibility for benefits on whether the individual signs the authorization, except in certain stated circumstances;

h. A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by this rule;

i. Signature of the individual and date; and

j. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual.

(See Attachment – Authorization for Release of Health Information)

2. The authorization must be signed and dated by the individual or his/her legal representative.

a. If the patient is unable to sign because he/she does not have sufficient mental ability to understand the situation and make a rational decision regarding the authorization form, then reasonable efforts shall be made to contact a legal representative to sign.

b. If a legal representative does not exist, then authorization may be signed by the next of kin (see policy verifying the Identify of a Person Requesting PHI).

c. The Agency must obtain an individual's voluntary and informed authorization before using or disclosing PHI for any purpose that is not otherwise permitted or required under the Privacy Rule.

B Authorization to Release Medical Information

1. With Patient Authorization: Only a competent adult (18 years of age or older) or minor emancipated by marriage or court, may sign an authorization to release his / her medical information.

The *following exceptions* apply:

a. Minors: If a minor has given consent for treatment to a licensed physician for the following conditions, the minor alone can authorize the release of medical information: 1) venereal disease and other reportable diseases, 2) pregnancy, 3) abuse of controlled substances or alcohol, and 4) emotional disturbances.

b. Incompetent Patient: If a patient has been declared incompetent by a court of law, the patient's legal guardian must sign the authorization form. The guardian's court appointment must be verified.

c. Signature: If a patient is unable to sign the authorization form, he/she should mark an "X" in the signature blank. An authorized Medic employee must witness the mark and sign the form. The patient representative cannot be a treatment professional.

d. Deceased: If the patient is deceased, an estate representative should present letters of administration from a court of law to the Risk and Safety Officer or the Agency's FDP. When there is no court-appointed executor or administrator, as evidenced by a written document signed by the clerk of court or a written affidavit signed by the patient's next of kin, the patient's next of kin may sign the authorization form for release of information.

e. Adoptions: If a patient is adopted, the patient's birth parents can no longer access the minors health records unless by court order or by written authorization of the adoptive parents. No person or entity shall release from any records any information that could reasonably be expected to lead to the identity of an adoptee, an adoptive parent of an adoptee, an adoptee's birth parent or an individual who, but for the adoption, would be the adoptee's sibling or grandparent, except upon a court order.

f. Foster Parents: The foster parent must provide a document certifying that he/she is the foster parent and must have an authorization from DSS in order to inspect or obtain copies of the minor's health information.

g. Step Parents: If the patient has a step-parent, the step parent is not legally authorized to access the minor's medical record except upon the written permission of the patient's parent or legal guardian.

h. Legal Guardians: If the patient has a legal guardian other than a(n) adopted, foster, or step parent, the legal guardian must provide written proof of guardianship (i.e. a court order).

i. Divorced/Separated Parents: If the patient's parents are divorced, either parent can access the minor's medical records, in the absence of a court order to the contrary.

j. Abortion: If the minor has had an abortion, only the minor's parent or a judge can authorize disclosure of the medical record. The minor cannot authorize disclosure of such record.

2. Approved Release of PHI Without Patient Authorization

All requests for information should be evaluated and reasonable efforts should be taken

to limit the use and disclosure of protected health information to the minimum necessary to accomplish the intended purpose of the request. Verification of a treatment relationship is required before providing PHI. Agency personnel should contact the Privacy Department or Risk and Safety Officer with questions about the release of patient information. Records will be released to comply with N.C. General Stat. 143-518 such as:

- Made to a Medical Review Committee pursuant to N. C. Gen. Stat. 143-518 (a)(5);
- As part of a health research project in accordance with the requirement of N.C. Gen. Stat 143-518(a)(6)
- If made a statewide data processor pursuant to N. C. Gen. Stat. 143-518(a)(7); or
- Otherwise permitted by N.C. Gen. Stat. 143-518.

a. Treatment: A patient's health information may be used or disclosed to doctors, medics, or other personnel or people outside of the Agency who are providing services that are a part of a patient's medical care.

b. Payment: A patient's health information may be used or disclosed to an insurance company or third party payer so that treatment and services provided may be billed and collected.

c. Health Care Operations: A patient's health information may be used or disclosed for health care operations in order to give quality care to our patients and evaluate the performance of our staff. Information may be disclosed to doctors, medics and other Agency personnel for review and learning purposes.

d. Medical Emergencies: Disclosures to medical personnel shall be made when and to the extent necessary to meet a bona fide medical emergency when there is a legitimate need for the information.

e. Non-Criminal Judicial or Administrative Proceedings: Court Order / Lawsuits / Disputes: In non-criminal situations, Agency may only release protected health information ("PHI") upon receipt of a valid patient authorization or a court order from a North Carolina Court or a Federal Court (please see table below). The Risk and Safety Office should be consulted for criminal situations.

**For depositions, contact the Risk and Safety Officer or FPD.

f. Research: Under certain circumstances, a patient's health information may be used or disclosed for research purposes. All research projects are subject to a special approval process, which evaluates the use of medical information for the research project in order to balance the research needs with the patient's need for privacy. In most circumstances, patients are asked for specific permission if the researcher will have to access the patient's name, address or other information that reveals the identity of the patient. (Refer to the administrative policy, *Authorization for Release of Health Information for Purposes of Research*).

g. Threat to Health or Safety: If the Agency, in good faith, believes the use or disclosure: Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and is disclosed to a person reasonably able to prevent or lessen the threat, including the target of the threat; or Is necessary for law enforcement authorities to identify or apprehend an individual: Because of a

statement by an individual admitting participation in a violent crime that Medic reasonably believes may have caused serious physical custody harm to the victim. Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

h. Disaster Relief: the Agency may use or disclose protected health information to Federal, state, or local government agencies engaged in disaster relief activities, as well as to private disaster relief or disaster assistance organizations (i.e., the Red Cross) authorized by law to assist in disaster relief efforts, to allow these organizations to carry out their responsibilities in a specific disaster situation.

i. Public Health Activities: The Agency may disclose protected health information to a health authority that is authorized by law to collect or receive information for the purpose of preventing, or controlling disease, injury, or disability (i.e., surveillance, communicable disease investigations, registries, birth or deaths, immunizations, product defects or problems, adverse events)

j. Health Oversight Activities: Disclosure is allowed when activities are authorized by law, for appropriate oversight of the Agency (i.e., audits, administrative, or criminal investigations, licensure or disciplinary actions)

k. Food and Drug Administration: Disclosure of protected health information to a person under the jurisdiction of the FDA is not restricted for the purpose of reporting adverse events, product defects/problems, or biological product deviations, or for tracking products, enabling recalls, repairs, or replacement, or for conducting post-marketing surveillance.

l. Law Enforcement: The Agency is permitted to disclose protected health information in response to a request from a law enforcement official: (see also policy: Law Enforcement Access to Medical Information)

- For the purpose of identifying or locating a suspect, fugitive, material witness for missing person;
- If it pertains to an individual who has died in order to alert law enforcement of the death if Medic suspects that the death may have resulted from criminal conduct;
- For information that the Agency believes in good faith constitutes evidence of criminal conduct that occurred on its premises; and
- To alert law enforcement, in response to a medical emergency, of the commission and nature of a crime, the locations of the crime or its victims, and the location, description, and identity of the perpetrator.
- The information that may be disclosed is *limited* to:

    1. Name and address;
    2. Date and place of birth;
    3. Social security number;
    4. ABO blood type and Rh factor;
    5. Type of injury;
    6. Date and time of treatment;
    7. Date and time of death (if applicable); and
    8. Description of distinguishing physical characteristics PHI related to

DNA or DNA analysis, dental records, or typing, samples or analysis of tissue or body fluids (other than blood) may ***not*** be disclosed for the purposes of location or identification.

- Disclosures pertaining to victims of a crime are permitted *only* if the individual agrees to the release, or if agreement cannot be obtained due to the incapacity or other emergency situation of the individual,
    - If law enforcement indicates that the requested information is needed to determine whether a violation of law by a person other than the victim has occurred, and the information is not intended to be used against the victim;
    - If law enforcement represents that immediate law enforcement activity depends on whether the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; or the disclosure is in the best interests of the individual.

m. Inmate: Disclosure of protected health information to a correctional institution or law enforcement official having lawful custody of an inmate or other individual is allowed if the institution or official represents that such PHI is necessary for the provision of health care to the individual; the health and safety of the individual; law enforcement on the premises of the institution; and administrative and maintenance of the safety, security, and good order of the institution.

n. Domestic Violence: The release of protected health information to an authority authorized by law to receive reports of child abuse or neglect, or disabled adult abuse or neglect, does not require written authorization of the involved individual. There are no mandatory requirements for healthcare providers to report domestic violence in North Carolina unless the injury involves disabled adult abuse or neglect, child abuse or one of the following:

- Bullet wounds, gunshot wounds, powder burns, and any other injury arising from or caused by the discharge of a gun or firearm;
- Every case of illness caused by poisoning (refers to intentional poisoning, not suicide attempts by overdose);
- Every case of a wound or injury caused by a knife or sharp or pointed instrument if it appears that a criminal act was involved; and
- Every case of a wound, injury or illness involving grave bodily harm or grave illness if it appears that a criminal act was involved.

o. Organ Donation: The Agency's designated organ procurement organizations (i.e., LifeShare of the Carolinas) may have access to the patient's medical record for the purpose of determining organ or tissue donation potential.

p. Military & Veterans: The agency may use or disclose protected health information of individuals who are members of the United States Armed Forces for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the Federal Register the following information: Appropriate military command authorities; and The purposes for which the protected health information may be used or disclosed. National Security & Intelligence Activities: The Agency may disclose protected health information to authorized Federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act.

q. De-identified Information: Information which does not identify an individual patient is not subject to the HIPAA Privacy Rule. Protected health information is considered de-identified when the Agency has no reasonable basis to believe that the information can be used either individually or in combination to identify an individual. (Refer to the administrative policy, *De-Identification of Protected Information.*)

r. News Media: All requests for information by the news media shall be referred to the Agency's Public Relations Director. (See Policy: Release of Patient Information to the News Media)

C. Correction of Medical Records

Refer to the administrative policy, *Request for Amendment or Correction to Health Record Information*.

D. Inspect or Obtain a Copy of a Medical Record

1. An individual has the right to request to inspect and/or obtain a copy of the health information used to make decisions about his/her care (i.e., medical and billing records) for as long as the information is maintained in the designated record set by or for Medic.

1. The request to review PHI should be put in writing and submitted to the Facility Privacy Officer, Risk and Safety Officer or designee.

    a. Individuals presenting in person will be required to verify their identity and complete the Authorization for Release of Health Information form (Attachment A).

    b. Written requests for copies) of health record information must include information provided in this policy under A. Valid Authorization,

2. Provision of Access

    a. The Facility Privacy Director or the Risk and Safety Officer or designee will review the request to determine if the individual is eligible to inspect and/or obtain a copy of the health record information requested.

3. Non-Reviewable Grounds for Denial of Access to PHI. The Agency may deny an individual access *without* providing the individual *an opportunity to have the denial reviewed*, in the following circumstances:

        a. PHI (protected health information) requested was compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;

        b. Request from an inmate to *obtain a copy* of PHI if obtaining a copy would:

- Jeopardize the health, safety, security, custody, or rehabilitation of the individual or other inmates; or
- Jeopardize the safety of any officer, employee or other person at the correctional institution or responsible for transporting the inmate. (Note: If an inmate requests *inspection* of PHI, the *request must be granted* unless one of the other grounds for denial applies.)

        c. Information created or obtained by the Agency in the course of research

that includes treatment, for as long as the research is in progress, provided that:

- The individual has agreed to the denial of access when consenting to participate in the research that includes treatment; and
- The Agency has informed the individual that the right of access will be reinstated upon completion of the research.

4. Reviewable Grounds for Denial

The Agency may deny an individual access in the following circumstances, provided that the individual is given the *right to have such denials reviewed*.

a. A licensed health care professional has determined, in the exercise of professional judgment, that the access is reasonably likely to endanger the life or physical safety of the individual or another person;

b. The information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

c. The request for access is made by the individual's legally authorized representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such representative is reasonably likely to cause substantial harm to the individual or another person.

1. Notification of Acceptance

The Agency personnel accepting the request will schedule a convenient time for the individual to inspect, obtain a copy or receive a mailing of the health record information requested.

2. Notification of Denial

If the request is denied, the Risk and Safety Officer or FPD or designee for the Agency denying the request will provide the individual with the reason for the denial and document all communication with the requesting party.

3. Record Keeping

The Agency will be responsible for maintaining the log of Release of Patient Health Information and the completed forms.

E. Charges for Copying Medical Record Information

1. Requestors will be charged according to the most recent schedule of copying fees for Medical Records as established by the Agency based on North Carolina law. If the purpose of the request is for payment justification, the charge will be waived.

2. The Agency may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

a. Copying, including the cost of supplies for and labor of copying the protected health information.
b. Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
c. Preparing an explanation or summary of protected health information when agreed upon by the individual in advance. The Agency may provide the individual with a summary of the health information requested, in lieu of providing access to the health record, if:
    - The individual agrees in advance to such a summary or explanation; and
    - The individual agrees in advance to the fees imposed for such summary or explanation.

NOTE: there will be no charge for inspection of health record information.

3. Insurance Related Requests: Insurance related requests shall be honored when considered appropriate by an Agency employee. A charge shall be made for this service based upon the number of copies and type of information requested. Such requests may originate from, but are not limited to:
    a. Attorney(s)
    b. Commercial Insurance Companies
    c. The Social Security Administration unless for Disability
    d. Life Insurance Carriers

4. Medicare/Medicaid Related Requests: Medicare and Medicaid will not be charged for copies of medical records.

F. Retention of Written Requests: Copies of Authorization for Release of Health Information forms shall be logged and maintained in original or electronic format for six years from the date of creation or the date that it was last in effect, whichever is later.

G. Revocation of Authorization: If patients give authorization to use or disclose health information, they have the right to revoke the authorization, in writing, at any time. The written revocation only applies to uses or disclosures of health information after the date of the revocation. The Agency is responsible for documenting and tracking revocations.

<u>Method of Releasing Medical Records and Information:</u>

1. Mail: Copies of patient medical records may be mailed to authorized requestors with patient or legal representative authorization.

2. Telefax: Disclosure of health record information via fax will be limited to urgent or non-routine transmittals for continued patient care. In general, sensitive or highly personal health information will not be faxed. This would include health information about a patient's drug or alcohol treatment, mental illness, sexually transmitted diseases or HIV/AIDS status. PHI may be released via fax when the information is urgently required by a third-party payer and failure to fax the records could result in loss of reimbursement. (Refer to the administrative policy, *Communications Environment Acceptable Use*).

3. Overnight Delivery: In rare cases, when a record will not reach a requestor in time for a follow-up appointment, overnight delivery will be utilized.

4. In Person Request: Copies of patient medical records may be released to authorized requestors, at the Agency, with patient or legal representative consent. (Refer to the administrative policy*, Request to Inspect or Obtain a Copy of Health Information*).

H. PHI in Photographic or other non-typical media:

1. All photographic or other non-typical media which contain the patient likeness or has affixed, in any manner, patient identifiers is subject to all requirements set forth in this policy including the authorization requirement (Authorizations are purpose specific. Changes to purpose require reauthorization with the new purpose statement).

2. Based on the purpose of the photography or capture of patient identifiers or patient likeness in other non-typical media, certain departments are to be contacted for coordinate/authorization:

a. Photographs of Patients for Medical/Legal Purposes

- Medic employees may take a photograph of a scene if it is clinically pertinent, such as documenting damage to a vehicle or other mechanism of injury. It should be done after the patient is extricated and clear of the photograph. Such photos should be shown only to the receiving physician and then promptly deleted. These photos must not be forwarded or shared with anyone else.

- Other persons wishing to take photographs of patients for medical / legal purposes may do so provided the patient or patient's legal representative gives permission, the physician of the patient is informed and there is no medical reason why pictures should not be taken. Since this is not for treatment, payment or healthcare operations, the patient's authorization should be documented in the medical record on the authorization as described in Section A & B.

- In cases in which the patient is in the custody of law enforcement authorities, permission from the investigative officer is required when the purpose is neither Treatment, Payment, nor Healthcare Operations.

▪ Regardless of purpose, the following should be documented in the patient's medical record when such images are made.

a. The request to take photographs,
b. The fact that the physician has been informed
c. Information regarding when the pictures were taken, of what areas and by whom.
d. Please remember any non-patient authorized use/disclosure that is not treatment, payment or healthcare operations must be reported on under Reporting Misuses and Disclosures of PHI.

7.9 Receipt and Acknowledgement of the Notice of Privacy Practices
Effective 3/1/09, 01/10/2013

POLICY

1. **Presentation of Notice to Patient**
   a. All patients receiving care will be given an opportunity to review the Agency's Notice of Privacy Practices

   b. The Agency's Privacy Director or their designee will be responsible for delineating a process for the distribution of the Notice.

   c. The Agency will post the Notice on the Agency's Intranet and website.

2. **Tracking Receipt of Notice**

   The Agency will maintain patients' current written acknowledgement for the receipt of information pertaining to Notice of Privacy.

   A good faith effort is made to obtain written acknowledgement utilizing the Request for Treatment and Authorization Form.

   The written acknowledgement must be signed and dated by the individual or his/her authorized representative

   If the patient is unable to sign because he/she does not have sufficient mental ability to understand the situation and make a rational decision regarding the Notice, then reasonable efforts shall be made for a legally appointed guardian, patient's spouse, adult child, parent, adult sibling, nearest relative, or other legal representative, in that order, to sign.

   If the patient is unwilling to sign, Agency staff will document attempt(s) to obtain written acknowledgement and the reason(s) why written acknowledgement could not be obtained.

   All attempts at obtaining the patient's signature and any reason the written acknowledgement could not be obtained should be documented.

   Written acknowledgements must be documented and retained in the medical record.

3. **Changes to the Notice of Privacy Practices**

   The Agency's Privacy Officer will monitor for any material changes to:
   a. Uses or disclosures
   b. Individual rights
   c. Agency's legal duties
   d. Other privacy practices stated in the notice

   In the event of material change(s), the Agency Privacy Officer or designee will be responsible for updating the Notice of Privacy Practices and making revisions to the corresponding policies and procedures.

   a. No changes will be implemented prior to the effective date of the notice in which the change is reflected, except where required by law.

b. The revised notice and date of revision will be posted on the Agency's Intranet and website.

Copies of the notice(s) issued by the Agency will be retained for six years from the date of its creation or the date when it was last effective, whichever is later.

7.10 Release of Patient Information to the News Media
Effective 4/1/09, 01/10/2013

POLICY

This policy is to specifically set forth patient information that can be shared with the media.

PROCEDURE

1. Authorized Spokesperson:

Because it is the Medic Public Relations Department's responsibility to answer questions for the local media, all inquiries made during normal business hours should be directed to a media relations representative at (704) 621.0932. After hours, should someone need more than routine information, as in instances of breaking news, a designated representative is always available and may be reached nights, weekends and holidays by calling (704) 943.6238 and speaking with the CMED Supervisor on duty, who also have authority to provide basic information regarding patient status to the media.

Patient Condition Reports:

Life Threatening Injuries – This patient has been transported Priority 1 **(**Questionable prognosis. Vital signs are unstable and not within normal limits. Patient may be unconscious. Indicators are unfavorable).

Potentially Life Threatening Injuries – This patient has been transported Priority 2 (Vital signs may be unstable and not within normal limits. Patient is acutely ill. Indicators are questionable.)

Non-Life Threatening Injuries – This patient has been transported Priority 3 (Vital signs are stable and within normal limits. Patient is alert and comfortable. Indicators are excellent.)

General Information Withheld: A patient's name will never be released, nor will the specific physical address of an incident. Patients' right to privacy demands that no statement be made as to diagnosis or, whether a person was intoxicated, poisoned, or whether the injuries were because of sexual assault, attempted suicide or suicide. By N.C. law, we will also keep confidential all information including acknowledgement that an individual is a patient at a psychiatric or substance abuse treatment facility.

7.11 Requests for Amendment or Correction to Health Record Information
Effective 4/1/09, 01/10/2013

PURPOSE

To define a process for handling patient requests for a correction to his/her Personal Health Information and Personal Information Data.

PROCEDURE

1. **Request for an Amendment**

   a. An individual who believes that information in his or her health record is incomplete or incorrect has the right to request an amendment or correction to the information for as long as the information is kept by the Agency.

   b. Any request for amendment or correction will be in writing on the form attached to this policy and must provide a reason supporting the requested amendment. Individuals presenting in person shall be referred to the Risk and Safety Specialist or designee for assistance.

   c. All amendment requests shall be sent to the Risk and Safety Officer, Agency's Privacy Officer or designee for processing. The Agency shall act on the individual's request for amendment no later than sixty (60) days after receipt of the request.

2. **Responding to a Request for Amendment**

   Acceptance of a Request for Amendment

   a. The Agency will notify relevant persons with which the amendment needs to be shared at which time the Agency shall make reasonable efforts to inform and provide a copy of the amended request form.

   b. Health care providers and other entities, including but not limited to Agency business associates, who have the information that is the subject of the amendment and that may have relied, or might be expected to rely, on such information to the detriment of the patient.

   Denial of a Request for Amendment

   The Agency may deny the request for amendment if the record entry that is the subject of the request:

   a. Was not created by the Agency, unless the individual provides a reasonable basis to believe that the originator of the record entry is *no* longer available to act on the request;

   b. Is not part of the individual's health record (designated record set) kept by or for the Agency.

   c. Would not be accessible to the individual in accordance with applicable State and Federal laws.

d. Is accurate and complete.

If the request is denied, the author of entry/the Facility Privacy Director or designee will provide the individual with a timely, written denial (Attachment A completed) that contains:

a. The basis for the denial;

b. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

c. A statement that, if the individual does not submit a statement of disagreement, the individual may request that the Agency provide the individual's request for amendment and the denial with any future disclosures of the record entry and that is the subject of the requested amendment; (this would require a notation on the on-line patient information)

d. A description of how the individual may complain to the Agency pursuant to the complaint procedures (see the Agency's Notice of Privacy Practices) if the individual disagrees with the denial; including providing the name and telephone number of the Facility's Privacy Officer and the Secretary of the U.S. Department of Health and Human Services.

Denial Disputes/Disagreements Process

a. The Agency shall permit the individual to submit to the Facility Privacy Officer a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement.

b. The Facility Privacy Officer or his designee may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the Agency shall provide a copy to the individual who submitted the statement of disagreement.

Record Keeping

Medic will maintain as a part of the record:

a. The individual's request for an amendment;
b. The Agency's denial of the request;
c. The individual's statement of disagreement, if any; and
d. The Agency's rebuttal to the designated record set, if any.

Future Disclosures of PHI

a. If the individual has submitted a statement of disagreement, then the Agency shall include either the material appended in accordance with the Denial Disputes section of this policy, or an accurate summary of such information, with any subsequent disclosure of the entry to which the disagreement relates.

b. If the individual has not submitted a written statement of disagreement, then

the Agency shall include the individual's request for amendment and its denial with any subsequent disclosure of PHI (e.g. electronic disclosure), only if the individual has requested such action.

c. When a subsequent disclosure does not permit the additional material to be included with the disclosure, the Agency may separately transmit the material to the recipient of the standard transaction.

Attachment A

MEDIC
Mecklenburg EMS Agency

Request for Health Information Amendment

To request an amendment to your health information, complete this form in its entirety (items 1 – 13) and submit to the Medic FPO, 4525 Statesville Road Charlotte, North Carolina. The Facility Privacy Officer or her designee will respond to your request within 60 days of receiving your written request.

1. Patient Name:

_____

2. Birth Date: _____

3. Patient/Legal Representative Address (Street, City, State and Zip Code:

_____

_____

4. Describe the information you want amended: _____

_____

5. Date(s) of information to be amended (i.e., date of service) _____

6. Check reason for request: ↑Information is incorrect ↑Information is incomplete ↑Information is outdated

7. How is the current information incorrect, incomplete, or outdated?

_____

8. What should the information say to be more accurate or complete? _____

_____

9. Do you know of anyone who may have received or relied on the information in question (i.e., physician pharmacy, hospital, health insurance, etc.): ↑Yes ↑No

10. If yes, please provide name(s), address (es), of the organization(s) or individual(s)

_____

_____

1. Signature: _____
2. Today's Date: _____
3. Patient/Legal Representative_____

Amendment has been:↑ Accepted↑ Denied
If denied, check reason:
↑ PHI was not created by Medic
↑ PHI is not part of the patient's designated record set
↑ Federal Lab forbids release of PHI in question to patient for review or inspection.
↑ PHI is accurate and complete
Signature: _____

Print name & title:

_____

Comments:

Printed on the back side of the individual's copy

If your request to amend health information is denied, please be advised that you have the right to:

1. Submit a written statement disagreeing with the denial. The statement should be submitted to:

   Mecklenburg EMS Agency
   Facility Privacy Officer
   4525 Statesville Road
   Charlotte, North Carolina 28269

2. Or if you chose *not* to complete a statement of disagreement, you may request that the Agency provide your request for amendment and the denial with any future disclosures of the health record information that is being questioned.

3. Please contact the Facility Privacy Officer at 704-943-6080 with any concerns or questions regarding this amendment process.

4. If you do not feel your request for amendment and the Agency's amendment process adequately addressed your concern, you may review the Agency's Notice of Privacy Practices for resolution options.

Attachment B

INTEROFFICE MEMORANDUM

To: [Click **here** and type name]
From: Author of Patient Care Record Entry
Subject: Patient's request for amendment or correction to their health record information
Date:

cc: [Click **here** and type name]

We received a request from an individual who feels that the health information contained in their medical record is incorrect or incomplete. In accordance with the HIPAA Privacy Rule, a patient has the right to request an amendment to their health record information. However, Medic may deny the request for amendment if the record entry that is the subject of the request:

- Is accurate and complete;
- Would not be accessible to the individual in accordance with applicable State and Federal laws.
- Is not part of the individual's health record kept by or for the Agency; or
- Was not created by the Agency, unless the individual provides a reasonable basis to believe that the originator of the record entry is *no* longer available to act on the request.

We have attached the individual's request for amendment (Request for Health Information Amendment form) and the corresponding health record information for your review. Please evaluate the attached information and make a determination regarding acceptance of the patient's request. If needed, attach any corresponding health record information and forward this information to the appropriate department for further evaluation.

After final review and evaluation, on the attached Request for Health Information Amendment form, please indicate whether the patient's request should be 'accepted' or 'denied'. If denied, please indicate the reason for the denial, sign, and date. **A copy of the amendment request form should be mailed to the individual requesting the amendment, by the Medic employee who signs the amendment form no later than _____(15 days from receipt of the request).**

A copy of this form should also be provided to the Facility Privacy Director for documenting completion of the request and the Agency's HIPAA responsibilities.

7.12 Verifying the Identity of a Person Requesting Patient Information
Effective 2/1/09, 01/10/2013

POLICY

MEDIC shall take reasonable efforts to verify the identity of the person requesting Patient Information and the authority of such person to have access to Patient Information.

PROCEDURE

A. Verification of Requests for Patient Information

1. These verification requirements apply to all requests for access to or disclosure of Patient Information, including disclosures for treatment, payment and health care operations *if MEDIC has not previously identified the requestor*. Unless an exception described in **Section G** below applies, MEDIC shall make reasonable efforts to verify the identity or authority of any person who asks for access to Patient Information if MEDIC does not know the identity or authority of the person asking for access to Patient Information.

2. MEDIC shall obtain any documentation, statements or representations, whether oral or written, from the person requesting the Patient Information when such documentation, statement or representation is required as described in subsequent sections of this policy.

3. If the patient who is the subject of the Patient Information is not available to advise regarding the disclosure, MEDIC will exercise professional judgment in determining whether making the requested disclosure without written proof of the requestor's identity and authority is in the patient's best interests. For example, if requiring written proof of identity or authority would create an enormous burden, such as when a family member is seeking to locate a relative in an emergency or disaster situation, MEDIC may disclose Patient Information upon representation of the relationship and without such proof. In such cases only the Patient Information pertinent to the receiver's role in the patient care can be provided.

B. Requests Made in Person

1. MEDIC shall use best efforts to verify an individual's identity by examining a form of photo identification. Acceptable forms of photo identification are: driver's license; military identification; passport; or state issued identification card.

2. If the individual requesting disclosure of Patient Information does not have valid photo identification, or if MEDIC needs additional information to verify the authority of such individual, then MEDIC may ask for other evidence to verify the identity or authority of the individual requesting Patient Information.

    a. When an individual requests disclosure of his or her own Patient Information, MEDIC shall compare the individual's signature to the signature on file in the individual's medical record.
    b. MEDIC may ask an individual certain personal information (e.g., date of birth or mother's maiden name) to further verify the identity or authority of the individual.

3. MEDIC may require students to provide written documentation of status as a student (i.e., dated letter signed by the lead instructor) before permitting the student to

participate in the ride-along program thus having access to Patient Information.

4. If a public official makes a request for Patient Information in person, MEDIC shall require the presentation of an agency identification badge, official credentials, or other proof of government status to verify the identity of an individual. Additional proof may be required to confirm the individual's authority to obtain Patient Information for legitimate purposes (e.g., Division of Health Service Regulation).

    a. MEDIC requires that the following information be collected when a disclosure is made to a person acting on behalf of a public official: a written statement on appropriate government letterhead indicating that the person is acting under the government's authority, or other evidence or documentation of agency (e.g. contract for services, memorandum of understanding, or purchase order) that establishes that the person is acting on behalf of the public official.
    b. MEDIC will obtain any documentation, statements, or representations, whether oral or written, that is/are a condition of disclosure and will include such information as part of the permanent medical record.
    c. If disclosure is conditioned on such documentation, statements or representations from the person requesting the Patient Information, MEDIC may reasonably rely upon such information if it appears to meet the applicable requirements.

C. <u>Requests Made By Telephone</u>

1. MEDIC shall *not* honor a request by telephone for disclosure of Patient Information unless the requestor demonstrates that there is an emergency situation.

2. MEDIC will make a reasonable effort to verify that Patient Information disclosed in emergency situations is released to the individual/entity authorized to receive it. For example:

    MEDIC may look up the phone number in the telephone book to verify the identity of the individual/entity before calling the requestor back.

    MEDIC may call the requestor back through the main switchboard/operator rather than through a direct phone number to verify the identity of the caller.

D. <u>Releases via Voice Mail</u>

1. MEDIC will make reasonable efforts to verify that the correct telephone number has been dialed / called.

    a. Verify that the telephone number and/or name on the recording matches the information listed for the individual you are calling.
    b. Limit the information disclosed to the following unless an authorization is obtained allowing for release of more patient information.
    c. "This is [name] calling from Mecklenburg EMS Agency. Please return my call. I may be reached at [give your phone number]"

2. MEDIC *shall not disclose Patient Information* on an answering machine.

E. <u>By Fax Transmittal</u>

1. MEDIC will make reasonable efforts to verify that any fax transmission is sent to the appropriate destination. Reasonable efforts include all of the following for any fax transmission:
    a. Restating the fax number to the requestor.
    b. Double-checking the fax number before pressing the send key.
    c. Calling prior to faxing so that the requesting individual can go to the fax machine to receive the information.
    d. Calling to verify that the fax was received by the intended individual.

    2. MEDIC will remind individuals and entities that are frequent recipients of Patient Information to notify MEDIC if the recipient's fax number will be changing.

    3. MEDIC departments shall periodically verify the identity and authority of individuals and entities that receive routine communications. To reduce errors in transmission from misdialing, when possible MEDIC shall pre-program, test and verify destination numbers with dummy information.

    4. MEDIC shall use a cover page containing a confidentiality and privacy statement when transmitting any Patient Information. (Attachment A).

F. <u>In Writing (includes Mail)</u>

1. When an individual makes a written request for disclosure of his or her Patient Information, MEDIC will compare the individual's signature that appears on the disclosure request to the signature that appears in the individual's medical record. MEDIC may contact an individual to further verify the identity or authority of the individual as necessary. If MEDIC cannot verify the identity or authority of an individual, then MEDIC shall return the request for disclosure and ask for additional personal information (e.g., date of birth or mother's maiden name).

2. If a public official makes a written request for disclosure of Patient Information, then MEDIC may accept the request if written on the appropriate government letterhead provided the authority of the public official can be verified (e.g., a request made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority).

G. <u>Exceptions</u>

1. Routine communications between providers and patients or providers and other Providers, where existing relationships have been established do *not* require special verification procedures.

7.12

Mecklenburg EMS Agency
www.medic911.com

Fax

To: [Click **here** and type name] **From:** [Click **here** and type name]

Fax: [Click **here** and type fax number] **Phone:** [Click **here** and type phone number]

Phone: [Click **here** and type phone number] **Pages:** [Click **here** and type # of pages]

Re: [Click **here** and type subject of fax] **Date:**

_ Urgent _ For Review _ Please Comment _ Please

Reply

CONFIDENTIALITY NOTICE:
If you are not the intended recipient or the person responsible for delivering it to the intended recipient, you are hereby notified that you are not authorized to read, print, retain, copy or disseminate this message, any part of it, or any attachments. This facsimile message may contain information that is confidential, privileged, proprietary, or otherwise legally exempt from disclosure or use.

Any disclosure or use of this facsimile message by any person other than the intended recipient or person responsible for delivering it to the intended recipient may constitute a Federal criminal offense punishable by imprisonment up to 10 years or fines up to $250,000.

If you have received this message in error, please destroy this message and any accompanying attachments in their entirety without reading the content and notify the sender immediately by telephone of the inadvertent transmission, by calling collect if located outside the calling area. There is no intent on the part of the sender to waive any right or privilege that may be attached to this communication. Thank you for your cooperation.

7.13 Anti-Virus Policy

Effective 11/1/05; Revision 2/19/09, 01/10/2013

POLICY

To define the process in which Mecklenburg EMS Agency will protect the operating environment from potential virus outbreaks.

PROCEDURE:

In order to safeguard Medic assets, certain countermeasures must be taken to minimize the possibility of a virus outbreak. The following items should be performed:

Installation

K. The corporate standard virus software should be used on all Medic assets to include but not limited to desktop and laptop computers, Intel-based servers, and Exchange mail servers. Although the Macintosh platform is not a support operating system at Medic, software will be provided for use on these systems. Additional platforms will be added as software for alternate platforms is made available.
L. This software will be installed as part of the corporate image on personal computers to ensure conformity across platforms. If the corporate image is not suitable for the device onto which the software should be loaded, a CDROM will be provided with specific installation instructions by Information Security. On Intel-based and Exchange servers, an installation procedure with documented settings for all systems should be maintained.
M. Signature updates (DAT's) will occur via an automated process to ensure systems are kept up-to-date.
N. Remote access systems (employees only) will be allowed to take the corporate software home to install.
O. Remote access users will also be notified bi-weekly of updated signature files via e-mail.
P. Set virus software to always scan a floppy diskette for viruses before using it.

Precautions

Q. NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then empty your trashcan.
R. Delete spam, chain, and other junk email without forwarding, in accordance with the Medic *Acceptable Use Policy*.
S. Never download files from unknown or suspicious sources. (including program code)
T. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
U. Back-up critical data and system configurations on a regular basis and store the data in a safe place.
V. If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
W. New viruses are discovered almost every day. Check major websites for new viruses.
X. Periodically check the Medic *Anti-Virus Policy* for any possible changes.

Current Corporate Standard Virus Software

Workstations: Symantec Endpoint Protection 11
Servers: Symantec Endpoint Protection Manager
Exchange: IronPort C150

7.14 Assigned HIPAA Security Responsibility

Effective 11/1/05; Revised 2/19/09, 01/10/2013

POLICY

To identify the security official responsible for the development and implementation of the policies and procedures required under subpart the HIPAA Security Rule.

PROCEDURE:

A. The HIPAA Security contact Mecklenburg EMS Agency is:

Name: Sharon Taulbert
Title: Deputy Director of Professional Services
Address: 4425 Wilkinson Boulevard, Charlotte, NC 28208
Phone: 704-943-6086
E-mail: SharonT@medic911.com

B. The duties shall include, without limitation, the following:

1. To coordinate the implementation of appropriate administrative, physical and technical safeguards to protect the confidentially, integrity and availability of electronic protected health information (EPHI).
2. To verify that the security management, auditing and monitoring programs have been implemented as designed.
3. To oversee the development, distribution and implementation of Agency security policies and procedures.
4. To periodically review policies and initiate needed updates.
5. To monitor for significant changes in the law and modify policies as appropriate.
6. To identify and respond to known security incidents; mitigate, to the extent practicable, harmful effects of security incident; and document security incidents and their outcomes.
7. To implement a security awareness and training program.
8. To coordinate security activities with privacy activities within the Agency.

7.15 Communications Environment Acceptable Use Policy

Effective 5/23/00; Revised 2/19/09, Revised 04/02/2012, 01/10/2013

SUMMARY STATEMENT:

Mecklenburg EMS Agency (Medic) relies on its Communication Resources to support its business processes and functions. To ensure that Medic Communication Resources are used properly by its employees, independent contractors, agents, and other Users, Medic has implemented the following: Communications Environment Acceptable Use Policy (see Section K below for defined terms used in this Policy).

POLICY GUIDE

PROCEDURE:

K. Applicability

1. The rules and obligations described in this Policy apply to all Users of Medic Communication Resources, wherever they may be located.

2. An authorized representative of each group not covered by the *Medic's HR Policy and Procedures Manual* (e.g., affiliates, vendors, contractors, etc.) will be required to sign the *Business Associates Agreement* form verifying that all employees of their company performing work at Medic must abide by this Acceptable Use policy.

L. General Responsibility

1. It is each User's duty to use Medic's Communication Resources responsibly, professionally, ethically, and lawfully.

2. Each User is responsible for the security of the Communications Environment. This responsibility extends to the content of the communications the User generates, disseminates or solicits through any Medic Resource. This can include but is not limited to written reports, email, voicemail, and verbal communication.

M. Prohibited Activities

1. Communication of Confidential Information
Communicating patient identifiers unless you are involved in the patient's treatment, obtaining payment for services rendered or healthcare operations involving the patient such as quality assurance, credentialing, or utilization review is strictly prohibited by Federal Law. No user may use their authorized access to confidential

business or patient information for any purpose other than normal duties as defined by their job description. Users will not discuss, either verbally, written or electronically any confidential or patient identifiable information unless it is in the process of their normal duties and the recipient is properly authorized to receive such information. Users shall not transmit over, email or make available to the Internet any confidential business or protected health information without the use of appropriate encryption technology. Transmittal of patient information via Medic Communication Resources is subject to federal law under the Healthcare Information Portability and Accountability Act (HIPAA) and the Medic Patient Rights policies for Confidentiality, including but not limited to administrative policies *Protection, Release, and Review of Protected Health Information (PHI).*

2. *Inappropriate or Unlawful Content*
Content that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, discriminatory, hostile, suggestive, defamatory, or otherwise unlawful or inappropriate may not be downloaded or sent by e-mail or any other form of electronic communication (such as Internet postings, newsgroups, voice mail, paging system, music, graphic and video files, etc.) or displayed on or stored in any Medic Communications Resource. Medic has implemented Internet blocking software to restrict access to inappropriate Internet sites. The Internet is a worldwide network of computers that contains millions of pages of information, some of which may contain offensive or inappropriate material.

   It is also a violation of Medic Policy to download, view, share or send content that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, discriminatory, hostile, suggestive, defamatory, or otherwise unlawful or inappropriate while on duty at Medic, regardless of ownership of the devices used.

3. *Prohibited Uses*
Medic Communication Resources may not be used for dissemination or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (viruses), political material, or any other use prohibited by this Policy.

4. *Waste of Communication Resources*.
Users may not deliberately perform acts that waste Communication Resources or unfairly monopolize Communication Resources to the exclusion of other Users. These wasteful acts include, without limitation, sending non business related mass distribution e-mails or chain letters, subscribing to non-business related mailing lists, spending excessive amounts of time on the Internet, playing computer games, listening to unauthorized radio broadcasts over the Internet, or otherwise creating unnecessary network traffic.

   (a) Exception:
      a. Occasional, limited, appropriate personal use of Communication Resources is permitted when the use does not:
         a. Interfere with the User's work performance or departmental standards
         b. Interfere with any other User's work performance
         c. Have an undue impact on the operation of the Agency’s Communications Environment
         d. Violate any other provision of this or any other Agency Policy.
      b. Personal use is subject to the same business scrutiny
         a. The Communication Resources and User accounts are issued to Users to assist them in the performance of their jobs.

b. Users do not have an expectation of privacy in anything Users create, store, send, or receive on Communication Resources.
c. Users expressly waive any right of privacy in anything Users create, store, send, or receive on the Communication Resources, through the Internet or any other Agency computer network.
d. Users understand that Medic may use human or automated means to monitor use of its Communication Resources. All information passing through Medic's Communications systems becomes the property of the Agency and can be monitored for the legitimate business needs of the organization.

5. *Misuse of Software*
Users *may not* do any of the following without prior approval of the Director of Administration:
(1) Copy software for use on home computers
(2) Provide copies of software to any non-Medic entity
(3) Install software on any Communications Resource
(4) Download unauthorized software or files from the Internet to any Communications Resource
(5) Modify, revise, transform, or adapt any licensed software

6. *Altering Identity*
Users must not alter the "From:" line or other attributes of origin information in e-mail, messages, or postings. Users must identify themselves honestly and accurately when sending e-mail.

7. *Use of Electronic Devices*
The use of electronic devices such as camera phones, digital cameras or tape recorders to transmit or record images or conversations without the explicit permission and acknowledgement of all parties is prohibited. Personal electronic communication devices (e.g., cell phones, pagers, etc.) should either be turned off or operated in silent mode and should not be answered when it would interfere with job responsibilities. Exceptions may be made by management in an emergency or other unusual circumstance. The use of personal electronic equipment in patient care areas must adhere to all applicable facility safety policies.

N. Policy Violation

1. Reporting:
(a) A User should notify the Agency's Director of Administration if he or she feels that security may have been compromised in any way. Such as:
(i) In the event Users nonetheless encounter inappropriate material on the Internet.
(ii) Receipt of unwanted or inappropriate communication or solicitations from an outside source.
(iii) Users who become aware of any misuse of software or violation of copyright law should immediately report the incident.

Possible misuse of Patient identifiable information must be reported to the Director of Administration.

2. Violation Investigation

(a) The Agency's Director of Administration is responsible for conducting investigations into any alleged Communications compromises, incidents, or problems.

3. Disciplinary Action
   (1) Any violation of this Policy may lead to disciplinary action. Disciplinary action will be based on the severity and context of the violation and shall be in accordance with existing Agency policies and/or appropriate legal action.
      (i) Disciplinary action may include without limitation, verbal or written reprimand, termination of employment and/or appropriate legal action.
      (ii) The Agency's Director of Administration or IT staff may deny or revoke communication privileges if there is a reasonable belief that a violation has occurred.
      (iii) Security privileges may be restored only after consultation between the Agency's Director of Administration, Agency IT Task Group and/or Senior Management personnel.
      (iv) Workforce members who access and/or obtain patient specific information on any patient other than the patients they are treating, billing for or performing Agency's business operations for, will be in violation of the HIPAA Privacy law.

O. New Applications

1. The Agency's IT staffs have the responsibility for maintaining the Agency's Communications Environment which includes the installation of software.

2. Users responsible for implementing new applications, services or hardware should contact the Agency's Director of Administration or designee to discuss security guidelines.

3. Such guidelines should be used to determine if the new application, service or hardware complies with current industry standards for security configuration and architecture.

P. Business Access

1. Access shall be granted to Communication Resources per the function as described in the job description.

   All systems access privileges shall cease when a User's employment or association with Agency terminates. All system access privileges shall be promptly revoked at the time the User's employment or association terminates. In the case of termination by Medic of the User, all access privileges are denied immediately upon notification. Use of information gained during association or employment with Medic in any form ceases when the relationship with Medic terminates.

2. Passwords
   (i) *Login Accounts.* A unique, separate login account consisting of an ID and password is required for each User of the Communication Environment, unless otherwise approved by Agency's Director of Administration. Users are required to change passwords upon initial login, and as often as required by the IT department.
   (ii) *Responsibility for Passwords*. Users are responsible for safeguarding their passwords for access to Agency's Communication Resources. Individual passwords should not be printed, stored online, on a Personal Data Assistant

(PDA) or given to others. *Users are responsible for all transactions made using his or her user ID.* No User may access the Agency's Communications Resources using another User's account. Users may disclose his or her user ID to an IT Representative during troubleshooting as required but should not reveal their password in any instance.

(iii) *Passwords do not Imply Privacy*. Use of passwords to gain access to the Agency's Communications Resources does not imply that Users have an expectation of privacy in the material they create or receive on the Agency's Communication Resources.

Q. Security

1. *Physical Security.* Users shall take all reasonable and prudent measures to physically secure all Communication Resources. Users shall not open or attempt to open the encasement of any Communication Resources, nor otherwise circumvent any lock system that secures the device or its components. Laptop PC Users should use the provided lock to secure the laptop at all times. Smaller devices, such as PDAs, Smart Phones, or the like, should remain with the owner at all times or locked in a secure place when not in use. Devices should be stored in a vehicle's trunk while being transported. Never leave items lying in a vehicle that are visible from the outside. Report any lost or stolen Communications Resources including mobile devices such as laptops, cell phones, Blackberries or personally owned devices used to connect to the MEDIC network to the IT Department immediately, preferably within 24 hours.

2. *Downloading Patient Identifiable Information.* Users shall take all reasonable and prudent measures and are responsible to ensure the safety and confidentially of all patient identifiable information that is downloaded to any communications device, e.g. PDA, laptop, etc. Reasonable measures include but are not limited to: storing large files and databases only on network shares, password protection for sensitive files, implementing encryption for permanently stored files, and employing additional measures as directed by the Agency's Director of Administration in specific policies. Any non-Agency person that downloads patient identifiable information, for example a consulting physician, is considered a covered entity and is solely responsible for protecting the safety and confidentially of the data.

3. *Users will not add any type of device* (such as a modem, cable, Digital Subscriber Line, wireless interface, thumb drives, etc.) to any Communications Resource without prior approval from the Agency's Director of Administration. All vendor access must be made through an approved network access method. *No direct vendor connections are allowed without the expressed approval of the Agency's Director of Administration.* On systems where patient identifiable information is stored, such vendor will have to sign a business associate agreement.

4. *Accessing Other Computers and Networks.* A User's ability to connect to other computers or networks does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems and their job description. Users should not view any information without proper prior authorization via job description functions.

5. *Computer Security.* Each User is responsible for ensuring that the use of external computers and networks, such as the Internet, does not compromise the security of the Agency's Communication Environment. This duty includes taking reasonable precautions to prevent intruders from accessing the Agency's Network without authorization and the introduction and spread of viruses. Users shall take

reasonable measures to protect data on any computer that is used to store business sensitive and/or patient identifiable information (home computers, computers at remote locations, etc.). Reasonable measures include but are not limited to: storing large files and databases only on Agency network shares, password protecting sensitive files, implementing encryption for permanently stored files, storing computers in locked rooms and buildings, preventing direct access by non-Agency employees, and employing any additional measures as directed by the Agency's Director of Administration in specific policies.

6. *Communication Security*. Users shall not connect to the Agency's Network by any means other than by those specifically defined by the Agency's Director of Administration. Personally owned computers should not be connected to the Agency's Network without prior approval of the Agency's Director of Administration, IT Manager, or IT Security. Users shall not disable Communication Resources functions (passwords, virus scan, distribution software) implemented by the Agency.

7. *Network Security*. Users will not conduct network mapping, discovery, port scans, traffic analysis, traffic logging or any other information gathering/discovery technique from any Agency Communication Resources device unless that action is specifically authorized in their normal duties and responsibilities and approved by the IT department.

8. *Monitoring.* Monitoring is a right, but not a duty, of the IT Task Group. Monitoring includes all activity on the Agency's Communication Resources including but not limited to, reviewing Internet Sites visited, reviewing content downloaded/uploaded by Users to/from the Internet, reviewing phone records, reviewing computer activity, and reviewing email sent and received by Users.

9. *Circumventing established security.* Users may not attempt to circumvent the Agency's data protection measures or attempt to uncover security loopholes. Users may not gain or attempt to gain unauthorized access to restricted areas or files on the Agency's Communication Resources. Users should not tamper with any software protections or restrictions placed on computer applications, files or directories. Users must immediately report suspected network, hardware or software security vulnerabilities to IT. User must not attempt to demonstrate or exploit suspected security vulnerabilities. Users may not download or use hardware or software security or "hacker" tools.

10. *Internet Representation.* Users shall not use the Agency's name, symbol, logo, or any confusingly similar graphic on any Internet presence (Email, Web-based publication, etc) without prior and specific written consent of the Agency's management.

11. *Virus Detection*. Viruses can cause substantial damage to computer systems. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the Agency's computing environment. To that end, Users should not disable virus protection software installed on Agency's Communications Resources. Users should comply with virus software update announcements as required, and report suspected virus activity to the Agency's IT department as soon as possible. Any User that is unable to receive regular, automated virus updates is required to manually update the virus protection software at least bi-weekly.

12. *Malicious Destruction of the Agency's Software/Hardware*: Medic has invested considerable resources in software and hardware to provide the Communications Environment needed by the employees. Users shall not maliciously destroy or

otherwise damage/delete any software licensed to or owned by, or any hardware owned leased, or otherwise in the possession of the Agency. Any such damage or destruction shall subject the User to disciplinary action under this Policy. In addition, the Agency reserves the right to seek compensation through legal action for any damages maliciously caused by the User.

13. *Encryption of mobile devices:* All MEDIC issued mobile communication resources - laptops, tablets, smartphones, Blackberries, PDAs, etc – that access the MEDIC network, including email, will be provisioned with IT Security approved encryption software. All other access by a personally owned device is strictly prohibited. Employees are prohibited from utilizing any method to circumvent this requirement such as installing software on their computer to locally synchronize their email on to a personal device without the approval of IT Security.

R. Intellectual Property Rights

Any information developed or compiled by the User, including such things as writings, spreadsheets, databases, regardless of form and any invention, discovery, development, modification, system, program, or design that results from the use of the Agency's Communication Resources by the User shall be the exclusive property of the Agency.

S. Policy Governing Specific Applications:

Following is a list of specific applications and how each should be used acceptably by the Agency Users. This is by no means an exhaustive list of applications. The general spirit set forth below should be applied consistently across any new technologies, or new uses of technologies. If the situation or technology you are concerned about is not listed below, please read the Conversation/Discussion section, think about how it applies to the situation of concern and contact either the Agency's Director of Administration for specific direction regarding the acceptable use of your application.

1. Conversation/Discussion (At work or home)
   Information collected for the Agency business purposes which includes but is not limited to the treatment, billing, hospital operations and improvement of patients well being shall not be shared inside or outside the business environment with any unauthorized individual(s), group of individuals or organization etc. As with any communication of Protected Health Information (PHI - information that alone or collectively identifies a patient), *the person communicating the information and the person receiving the information must be authorized to receive and handle the information*.
   Two applications should be considered:

   (a) Telephone: The telephone is considered a device for communication. The restriction in the Conversation/Discussion section of this policy applies to this application regardless of the circumstances.

   (b) Incidental Disclosure (overheard conversation): The HIPAA Privacy Law of 1996 does allow for conversations between two authorized persons occasionally to be overheard by unauthorized persons. However, each Agency Workforce member has the responsibility to control conversation contents and environment to minimize disclosure of PHI to unauthorized individuals. This can be

accomplished by selecting the proper information, audience, room and voice volume to convey PHI.

2. Patient Lists/Reports:
   Schedules, VIP lists and any other lists of patients **are** to be used strictly by the Agency staff for treatment, payment and health care operations.
   (a)

3. Voicemail
   (a) *Voicemail Setup*. Each User should record an internal and external greeting in accordance with the guidelines presented in training. Users should also change the voicemail password from the system default.
   (b) *Voicemail Usag*e. Users should not include confidential information in voicemail messages (including but not limited to patient identifiers or associations with patient identifiers which might disclose a patient's diagnosis or treatment).

4. Email Usage

   (a) Email Equipment and Software Standards

      (i) *Only Mecklenburg EMS Agency Equipment/Software Permitted*.
      (ii) *Unauthorized Equipment/Software*. No unauthorized software or hardware may be used to communicate with Patients without the expressed written consent of the Agency's Director of Administration .

   (b) Patient Confidentiality
      (1) *State & Federal Law*. The Agency Employees shall observe all North Carolina and Federal laws pertaining to Patient confidentiality when communicating with a Patient via E-mail.
      (2) *Agency Employees to Restrict Access*. When communicating with a Patient via E-mail, the Agency Employees shall take all reasonable measures to restrict access to such communications so as to safeguard Patient confidentiality.
      (3) *Patient's E-mail Address Confidentiality*. The Agency Employees shall not divulge any Patient's E-mail address unless the Patient expressly authorizes such disclosure in writing.

   (c) Patient Communication via E-mail.
      The Agency Employees shall not communicate with a Patient via E-mail unless the Patient has indicated his or her consent to such communication by signing a hard-copy paper version of the electronic mail communication request and a consent form.
      (i) *The Agency Employees shall place the Patient's signed E-mail Consent Form in the* Patient's medical record.
      (ii) A Patient may withdraw his or her consent to using E-mail communication at any time by delivering a written withdrawal of consent to the Agency Employees.
      (iii) The Agency Employees shall act promptly to affect such Patient's withdrawal of his or her consent to engage in E-mail communication with the Agency Employees and to place the Patient's written withdrawal in the Patient's medical record.

(iv) No Patient is compelled to use E-mail. The Agency Employees shall not attempt to compel or coerce any Patient to communicate with the Agency Employees via E-mail.

Other Required Email Footers.

(i) *External Disclaimer. Email sent from the Agency's network to any outside address will have an approved disclaimer banner attached at the end of the* correspondence.

5. Faxing

Unless otherwise arranged through Legal counsel, transmission of Protected Health Information (PHI), in any media, including facsimile, may be performed only as allowed in this policy by personnel who are trained to perform release of information, have ongoing staff training and quality monitoring of release of information activities

(a) When PHI May Be Released Without Authorization

(i) Qualified Agency personnel may send PHI by facsimile when:

(i) The original record or mail-delivered copies will not arrive in time to meet the immediate needs of patient care, or

2. When PHI is urgently required by a third-party payer and failure to fax the records could result in loss of reimbursement.

(ii) Facsimiles may not be sent to patients, parents or legally authorized representatives of patients.

(iii) Authorization

a. Except as authorized by law or in the event of a medical emergency, or as otherwise permitted by law, an authorization signed by the patient or patient's legally authorized representative must be obtained before releasing PHI.

b. If the fax is being sent for purposes of payment (including third-party reimbursement), patient care or medical treatment purposes, the patient's signed consent obtained at registration serves as authorization.

c. If the fax is being sent for any other purposes, a separate authorization for the release of information must be signed (by the patient or his or her legally authorized representative) prior to the fax being sent.

(iv) <u>Limit Release</u>

Agency personnel shall limit information transmitted to the minimum amount reasonably necessary to meet the requestor's needs or to accomplish the purpose for which the request is made.

(v) <u>Sensitive Information</u>

Agency personnel may not send by fax especially sensitive medical information (i.e., AIDS/HIV information, mental health and developmental disability information, alcohol and drug abuse information, and other sexually transmissible disease information) without specific written authorization by the patient or legally authorized representative or court order.

a. <u>Documentation of Release</u>

All releases of PHI shall be documented in the medical and/or financial record.

b. Documentation shall include:

1. Date of the release,

2. What information was released (i.e., progress notes 6/6/01),

3. To whom the information was released,

4. Purpose for the release, and
5. How the release was carried out (fax, photocopies mailed, etc.)

(vi) Cover Page

The cover page accompanying the fax transmission must include the following confidentiality notice:

CONFIDENTIALITY NOTICE:

If you are not the intended recipient or the person responsible for delivering it to the intended recipient, you are hereby notified that you are not authorized to read, print, retain, copy or disseminate this message, any part of it, or any attachments. This facsimile message may contain information that is confidential, privileged, proprietary, or otherwise legally exempt from disclosure or use.

Any disclosure or use of this facsimile message by any person other than the intended recipient or person responsible for delivering it to the intended recipient may constitute a Federal criminal offense punishable by significant imprisonment and/or significant fines.

If you have received this message in error, please destroy this message and any accompanying attachments in their entirety without reading the content and notify the sender immediately by telephone of the inadvertent transmission, by calling collect if located outside the calling area. There is no intent on the part of the sender to waive any right or privilege that may be attached to this communication. Thank you for your cooperation.

(vii) Verification of Destination

The Agency will take reasonable steps to verify that the fax transmission is sent to the appropriate destination, such as:

1. Obtain/restate fax number to requestor.
2. Double check fax number before pressing the send key.
3. Call prior to faxing so that the requesting individual can go to the fax machine to receive the information.
4. Call to make sure fax was received by intended individual.
5. Remind individuals/entities who are frequent recipients of protected health information to notify you if their fax number is to change.

(viii) Location of Fax Machines

a. Fax machines must be in secure areas.

b. The Department Director or Manager will be responsible for limiting access to fax machines.

(ix) Handling Received Faxes

a. Each department is responsible for the proper handling of incoming faxes.

b. Faxes should not be left sitting on or near the fax machine, but rather distributed to the proper recipient expeditiously.

(x) Mis-directed Faxes

Misdirected faxed documents must be reported immediately via an incident report submitted to the Director of Administration.

(xi) Audit of Speed Dial Numbers

(i) Each Agency department will periodically check all speed dial numbers and computer database fax numbers to verify that the numbers are current, valid, accurate, and that the recipient is still authorized to receive PHI.

(ii) This audit shall be documented showing the date performed and the individual performing the audit.

T. Policy Exceptions

Exceptions to this Policy can be made with written approval of the Director of Administration.

7.16 Computer Incident Response Policy

Effective 11/1/05; Revised 4/2/09, 01/10/2013

POLICY

Mecklenburg EMS Agency depends on networked Communication Resources to support its business processes. To ensure that its Communication Resources are protected from unauthorized usage, malicious outside intrusion and inappropriate or damaging use by employees, independent contractors, agents, and other Users, it has established this Computer Incident Response Policy. This document outlines the organization, function and actions to be taken by the Information Technology Security Task Group in response to attacks, misuse, and threats to Communication Resources.

PROCEDURE:

A. Mission Statement - The IT Security Task Group will protect Communication Resources from unauthorized and malicious attack by prompt intrusion event identification, concise and accurate reporting to management authority, and elimination of system vulnerabilities. Evidence of intrusion will be retained for possible dispensary, legal or criminal prosecution. As conditions dictate, IT Security Task Group will be responsible for:

1. Responding to all computer incidents or suspected incidents using an organized, formal investigative process.
2. Conducting a complete investigation free from bias.
3. Quickly confirm or dispel whether an intrusion or security incident actually occurred.
4. Assessing the damage and scope of the incident.
5. Controlling and containing the incident.
6. Collecting and documenting all evidence related to an incident.
7. Maintaining a chain of custody.
8. Seeking additional resources, both internal and external, as the situation dictates.
9. Protect privacy rights established by law and/or corporate policy.
10. Provide liaison to proper law enforcement and legal authorities.
11. Maintain appropriate confidentially of the incident to protect the organization from unnecessary exposure.
12. Provide management with incident-handling recommendations that are fully supported by facts.

B. High Alert Viruses: IT Security Task Group will not be responsible for high alert viruses. Response to a high alert virus is covered under a separate policy.

C. Definition of an attack: An attack on Medic Communication Resources is defined as an unauthorized access, usage, virus, denial of service attack, repeated contact of an investigative nature or any attempt to map, define services, post files or control the function of a Medic resource outside of normal business operation or without expressed written permission of the Assistant Director of Operations or designated representative

D. IT Security Task Group organization
   1. The members of the Task Group will consist of a team leader, normally the on-call personnel from the Information Technology Department, and members from the various teams associated with the particular type of incident. These can be, but are not limited to members of the following teams: Account Administration, Desktop Support, Exchange, Server, UNIX, and Infrastructure. Team members will be selected on an as-needed basis by the Assistant Director of Operations and are included or excluded from significant elements of the investigation as necessary

based on a need-to-know basis by the team leader. The group will normally consist of the on-call members of those teams unless otherwise directed.

2. In the event of an incident (as described in B), notification of the Assistant Director of Operations or designated representative is imperative. Notification may be generated by the existing IT Security Task Group alert procedures.

E. Actions upon threat/attack

1. IT Security Task Group initial Actions:
   (1) Upon notification, the Task Group Leader will analyze all available information to characterize the intrusion or attack. Specific information will be collected including, but not limited to: What attacks were used to gain access, what systems were compromised, what was done after access was gained, what is intruder currently doing, and when the intruder or the attack was stopped/eliminated
   (2) As soon as the Task Group Leader is aware of the nature of the attack/intrusion, they should report to the Assistant Director of Operations with the following information: Date/Time of attack, classification of attack, and possible extent. Based on the available information, the Assistant Director of Operations, after conferring with Administration, will decide on whether to continue operation and monitor the intrusion or actively counter the intrusion either by denying service or disconnecting or shutting down and restoring systems. The Assistant Director of Operations will make periodic update reports based on discovered information and progress.
   (3) The Task Group Leader will also communicate with the Medic Administration, team members and any other parties that need to be aware of the incident utilizing secure communication means whenever possible. Assignment of additional personnel from the various teams should be coordinated with the Assistant Director of Operations in conjunction with this notification.

2. Subsequent Actions
   (1) The Task Group should begin to collect data and copies of log files for analysis. If possible, these should be retained on CD media for later review and possible use in legal proceedings. Collection and retention of such data should be documented and personnel noted who had contact during the review process
   (2) The Task Group will inform the Assistant Director of Operations as soon as possible. The Assistant Director of Operations, working in conjunction with the Task Group, will determine what other teams, users, vendor(s), etc. need to be notified based on the type of incident and the affected systems.

3. Attack Containment
   (1) The Task Group will attempt to contain the intrusion or attack and determine which of the following actions to take based on the decision of the Assistant Director of Operations:
      (a) Isolate the affected systems
      (b) Isolate the affected network segment
      (c) Shut down the affected system
      (d) Disable system services
      (e) Change passwords
   (2) The IT Security Task Group will continue to monitor system and network activities to insure and verify that other systems have not been compromised. They will pass on the monitoring to the appropriate teams to allow restoration of files or transfer from backup data.

(3) The Task Group will search other systems for intrusion within the same network IP range or trusted domain, using the same common network services and finally the same operating system, examining significant system logs to identify common symptoms with the affected systems
(4) As necessary, the Task Group will coordinate with the appropriate teams to eliminate means of access and related vulnerabilities, assuming the worse case scenario. The appropriate team member responsible should complete a review of trusted files by any analysis tools or trusted cryptographic checksums, normal file size, dates. The team members should report to the Task Group team Leader when the review is completed.

4. Information Control/Evidence Handling
(1) As part of the collection and preservation of information the IT Security Task Group should identify the following data and document: The name of the system, the date and time of each incident and any action taken
(2) The IT Security Task Group will preserve evidence by first copying each file or system backup and archiving the original evidence onto read-only media and to a specific folder or volume that is protected from general access. The IT Security Task Group will then work only with copies of original data, limiting access only to specific IT Security Task Group team members, pertinent management personnel and law enforcement agencies. Evidence handling should be on a need to know basis.

5. Final actions
(1) The IT Security Task Group will coordinate with individual teams to return systems to normal. If the attack investigation is ongoing, a decision to either complete intrusion detection or continue operations will be made by the Assistant Director of Operations or above. The IT Security Task Group should monitor the appropriate team securing a trusted backup, setup of system and application services, system validation and monitoring/steps against future intrusion.

F. Individual Team member responsibility upon notification

1. Assistant Director of Operations - will report incidents as necessary to Administration. Additional information will be disseminated to the client population as needed.

2. IT Security Task Group Leader - will verify alert, notify the Assistant Director of Operations and begin to collect data using IT Security Task Group Incident Report booklet. The IT Security Task Group Leader will alert the Assistant Director of Operations as per the booklet criteria and confer on team size and plan of action. As additional personnel are needed, the IT Security Task Group Leader will contact them and brief each team member individually or in a group if possible, designating tasks to be assigned, and giving a deadline for each task.

3. Individual Team members - If selected for the IT Security Task Group, each team member will report to the IT Security Task Group Leader completion of tasks assigned and not disclose the nature or substance of the IT Security Task Group without the expressed consent of the Assistant Director of Operations or the IT Security Task Group Leader.

4. Authority to Act - The IT Security Task Group has the responsibility to investigate and report any and all intrusions to existing systems, to document any affected systems, but not to disable or disconnect without the approval of the Assistant Director of Operations.

G. Reporting

1. As stated in Section D above, the IT Security Task Group Leader will report as soon as possible the nature of the attack/intrusion. He should report to the Assistant Director of Operations with the following information: Date/Time of attack, classification of attack, and possible extent. Based on the available information, the Assistant Director of Operations, after conferring with Administration, will decide on whether to continue operation and monitor the intrusion or actively counter the intrusion either by denying service or disconnecting or shutting down and restoring systems.
2. At the conclusion of a reportable incident, the IT Security Task Group involved will conduct an After Action Review of the incident to determine what existing measures were adequate and what measures and actions need improvement. The final written version of this review should constitute the final report of the incident and be submitted to the Assistant Director of Operations.
3. If the IT Security Task Group Leader determines that law enforcement agencies should be notified of the incident, IT Security Task Group Leader will first obtain approval from the Assistant Director of Operations before notifying the pertinent agencies.

7.17 Disposal Procedures for Patient Information

Effective 11/1/05; Revised 4/2/09, 01/10/2013

POLICY

This policy sets forth the procedure for properly disposing of any material that contains protected health information.

Agency employees will properly dispose of any material that contains protected health information in a collaborate effort with all departments and units that generate such materials.

PROCEDURES

1. Paper:
   All paper on which is recorded protected health information (patient individual identifiers) will be deposited in a locked confidential shred bin. The contents of the bins will be collected for shredding.

2. Electronic PHI:
   These items should be disposed of in accordance with the IS Electronic Data Cleansing Policy.

   Examples include:
   Servers, PCs, Laptops, PDAs, Medical Monitoring Equipment, Routers, Network Monitoring Devices, Storage Area Network Devices, Cell Phones, Faxes, Printers, Diskettes, CD-ROMs, ZIP Drives, VHS Tapes, and any other material/devices containing PHI.

3. Miscellaneous – Any other items labeled with patient information should have the information marked out or the label peeled off. Disposal methods listed above or in other more specific policies (ie. Hazardous Waste) should then be followed.

4. EKG Strips: Strips should be disposed of in the HIPAA bins at the hospital or in the confidential shared bins at Post 100 at the end of the shift.

7.18 HIPAA Audit Procedures for the Siren ePCR System

Effective 2/19/09, 01/10/2013

POLICY

To insure compliance with HIPAA Guidelines and to protect the privacy of our patients while maximizing the ability of necessary parties to access patient care record information, the following procedures have been implemented:

Username / Password Assignment

It will be the responsibility of each facility requesting electronic patient care report access to determine who should be given access to the Medic Siren ePCR Web Access Portal. All requests for usernames and password will only be accepted from the specified administrative contacts.

All requests for user access must contain the following information:

- First and Last Name
- Employee ID Number
- Email Address
- Contact Phone Number

Upon request, the administrative contact will be given a unique username and password for the requested user. All users will be set up with accounts that will automatically expire after six months. It is the responsibility of the user to contact Medic Electronic Documentation staff with a requested password change prior to the six month expiration date. If a password change is not requested within that period of time, the user account will expire and access will be denied until the password has been changed.

Furthermore it is the responsibility of the administrative contact at each facility to update the Electronic Documentation Coordinator of any changes in user status, including the immediate notification of any personnel who are no longer granted access due to changes within the facility including termination.

MEDIC reserves the right to deny access to any party if deemed necessary and appropriate according to agency policy or state and/or federal regulations.

Quarterly HIPAA Audit Procedures

The following procedures will be followed at the beginning of each quarter to assure compliance within the HIPAA Guidelines:

1. The “View Siren User Date Created” script will be run for the quarterly period.

   This script will show the auditor every user that logged in and the date of access during that quarterly period.

2. The “View Siren Edits” script will be run for the quarterly period.

   This script will show the auditor every PCR that had fields edited during the quarterly period.

3. The “View Siren Web ePCR Access Audit” script will be run for the quarterly period. Five (5) patients from each facility granted access will be randomly selected and the script run against their electronic records.

This script will show the auditor every user that logged in and viewed the specific patient care report during that quarterly period of time.

HIPAA Violation Complaint Audit

In the event that a potential HIPAA violation via electronic access is identified, the following procedures will be implemented to provide an audit of access.

1. Patient or Patients are identified to Electronic Documentation or Operations staff.

    a. Staff will perform a lookup of the patient in the ePCR system to confirm the record's presence.
    b. The Patient ID will be identified from each requested record (at top of screen)

2. IT Manager or IT Security Specialist will be notified and given Patient ID numbers for audit.

3. The "View Siren Web ePCR Access Audit" script will be run on each specified Patient ID. The resulting output of the script will be given to the requesting facility or party for analysis.

    This script will show the requesting party every user that logged in and viewed the specific patient care report for the requested period of time.

7.19 HIPAA Security Training Policy

Effective 11/1/05; Revised 2/19/09, 01/10/2013

POLICY

The Agency will implement security awareness and training program for all members of its workforce as required under the HIPAA Security Rule.

PROCEDURES:

Various methods will be used to educate and reinforce proper security practices to the Agency workforce, including but not limited to the following:

1. Security Training
    - All new staff members will receive Security training upon beginning employment as part of new employee orientation.
    - Annual re-orientation will be accomplished primarily through annual testing with a graded post-test.

2. On-going training and awareness methods may include but are not limited to the following:

- Articles in departmental specific newsletters or memorandums
- E-mail reminders, notices, and updates
    - Specialized training or presentations for targeted departments or teams

An Intranet website with security and HIPAA related information

7.20 Information Security Management Plan Policy
Effective 11/1/05; Revised 2/19/09, 01/10/2013

I. PURPOSE:

The purpose of the **Information Security Management Plan** is to provide a safe and secure environment for all electronic patient information. The Information Security Management Plan is also established to minimize the risk of property loss due to criminal activity ***and unauthorized physical access to, tampering, and theft of protected data.***

The mission of Mecklenburg EMS Agency is to create and operate a comprehensive system to provide health care and related services including education for the benefit of the people it serves. Consistent with the mission, the Agency's Board, Medical Staff, and Administration have established and provide ongoing support for the Information Security Management Program described in this plan.

II. SCOPE

The Information Security Management Plan establishes the parameters within which a safe and secure environment is established, maintained and improved for all departments / services of Mecklenburg EMS Agency. This plan addresses administrative issues such as program structure, reporting requirements, specific responsibilities and general security information and staff education programs. These and other elements of the Information Security Management Plan are all directed toward managing the activities of the staff so risks are reduced, and staff can respond appropriately in emergencies. Security coverage is provided to Mecklenburg EMS Agency through the Agency Information Systems Department 24/7.

III. AUTHORITY / REPORTING RELATIONSHIPS

The Administration of Mecklenburg EMS Agency appoints an assigned HIPAA Security Officer to develop, implement, and monitor the information security management program for all departments / services of the Agency. Other designated members may include representatives from administration, clinical areas and support services. The Agency's Information Security Officer's responsibilities are developed and reviewed as part of the annual evaluation.

The Human Resources Department and Department Supervisors, Managers and Directors are responsible for orienting new personnel to the department and informing them of specific information security procedures. Managers and Directors of security-sensitive areas will train their personnel in departmental or job-related security procedures or precautions. Managers and Directors are provided with appropriate security program guidelines and are directed to maintain a current awareness of the Information Security Program, and to ensure its effective implementation within their department.

Each employee is responsible for following the guidelines set forth in the Information Security Program. Employees complete annual HIPAA education regarding security in the workplace and are responsible for understanding how the material relates to their specific job requirements. Employees are instructed to practice security measures (system property, reporting abuse of property and/or suspicious situations, etc.).

OBJECTIVES

1. Complete Incident Reports for all security related incidents.
2. Evaluate physical security equipment, its proper use and implementation.
3. To provide services that contributes to the protection of system property.

4. To prevent crime through appropriate security measures.
5. To prevent unauthorized physical access to, tampering, and theft of protected data.

INTENT PROCESSES

Addressing Security Issues

An assessment is conducted annually by the Information Security Officer for the Agency.

Incident Reporting

The Information Security Management Program documents security-related incidents. Incident Reports are completed by the Information Systems Department. Summary notifications of Security Incidents relating to electronic data and theft of communication equipment will be forwarded to the Information Security Officer.

Data Access

Staffs are identified in terms of assigned usernames and passwords to allow access to electronic information systems. Only authorized access to protected data is allowed as defined by the Agency.

Access and Egress Control

Access to protected data and electronic information systems is controlled by the Information Services Department and all associated policies and procedures.

Personnel Responsible for Information Security Management Plan

The Administration of the Agency assigns an officer responsible for overseeing information security related responsibilities.

Annual Evaluation

The Information Security Officer has overall responsibility for coordinating the annual evaluation process and effectiveness of the Information Security Program.

Emergency Security Procedures

The Agency maintains complete policies and procedures for actions to be taken in the event of an information security incident or failure.

Events that would be of interest to media are referred to the Public Relations Department. The Information Security Officer is dispatched to assist the media specialist as appropriate for the incident.

The Information Security Officer or designee will coordinate with Information Services to allow access to vendor and Medic personnel to the facility for the purpose of restoration and recovery of lost data and equipment in accordance with Information Services disaster recovery plans

Orientation/Training Process

New Employee Orientation: HIPAA Security Education/Orientation and Training program begins with the New Employee Orientation program for all new employees, which includes emergency procedures for minimizing security risks, and incident reporting. It continues on an ongoing basis with departmental-specific training, job-specific security/safety training, and a series of programs required for all employees on an annual basis.

Annual Continuing Education: The Annual HIPAA Education program for the Agency includes self-directed learning modules. These modules contain learning materials, a test, and answer key. These modules can be used by individual employees or as a guide for group presentations. Modules are reviewed/revised as necessary. New modules are developed when the need is identified. All staff of the Agency is required to participate in an annual mandatory training program.

Department Specific Training: Managers/Directors are responsible for ensuring that new employees are oriented to departmental specific policies and procedures and specific job related hazards. Personnel in security-sensitive areas are responsible for describing or demonstrating processes for minimizing security risks and reporting procedures for security incidents.

7.21 Information Security Risk Management Policy
Effective 11/1/05; Revised 2/19/09

POLICY
Medic will implement security measures sufficient to reduce risks and vulnerabilities to reasonable and appropriate levels to comply with subpart §164.306 (a) of the HIPAA Security Rule. Selection and implementation of such security measures will be based on a structured risk management process. Risk management is a continuous process and all implemented security measures will work to ensure the confidentiality, integrity and availability of Medic's information systems and be commensurate with the identified risks.

PROCEDURE:

A. Medic will utilize a number of methods and sources to identify potential risks to its information systems, including:

   a. Standing technology review committees, including: Information Technology Task Force and the Incident Response Team.

   b. By one of the following teams involved with information services support and/or compliance: Corporate Compliance Internal Audit, Corporate Compliance HIPAA Privacy, Corporate Compliance Hot Line, Human Resources, IT Department, and strategic Vendors and Third Party Partners.

   c. Triggered reviews based upon suspicious events or normal activity thresholds being exceeded.

   d. Periodic reviews, audits or vulnerability assessments conducted by the IT Department, IT Task Force, Incident Response Team, or an authorized third-party.

B. Medic's risk management process includes the following steps:

   a. *Risk prioritization.* Based on the risks defined by Medic's risk analysis, risks will be prioritized on a scale from high to low based on the potential impact to information systems and the probability of occurrence. When deciding what Medic resources should be allocated to identified risks, highest priority will be given to those risks with unacceptably high risk rankings.
   b. *Security method selection.* Medic will determine the most appropriate, reasonable and cost-effective security method(s) for reducing identified risks to Medic's information systems.
   c. *Assignment of responsibility.* Medic's workforce members who have the appropriate expertise will be identified and assigned responsibility for implementing selected security method(s).
   d. *Security method implementation.* Selected security method(s) will be correctly implemented.
   e. *Security method evaluation*. Selected security method(s) will be regularly evaluated and revised as necessary.
   f. *Documentation*. The results of risk analysis will be documented and securely maintained.

C. Audit Controls – The level or degree to which audit controls will be implemented will be determined through the risk assessment process.

D. Integrity Controls – The level or degree to which data authentication and integrity controls will be implemented will be determined through the risk assessment process.

7.22 IT Electronic Data Cleansing Policy
Effective 11/1/05; Revised 2/19/09

POLICY
To ensure that all electronic storage devices or media is properly cleansed of business sensitive or patient confidential data before leaving the possession of the data owner. Simply deleting a file or formatting the media is not sufficient to prevent someone from utilizing off-the-shelf utilities to recover the data. This applies to both devices/media that are being transferred or returned to inventory for redeployment and to storage components, e.g. hard disk drives, which are being replaced or repaired under third-party maintenance agreements.

PROCEDURE:

Before any electronic device with internal storage – servers, PCs, laptops, PDAs, medical monitoring equipment, routers, network monitoring devices, storage area network devices (SAN), cell phones, faxes, printers, etc. - is transferred outside the immediate department, returned to surplus inventory, or discarded, the storage media must be cleansed in a manner that prevents anyone from being able to recover business sensitive or patient confidential data from the device. This procedure applies to electronic portable storage media as well, such as: diskettes, CD-ROMs, ZIP drives, etc. For suggestions on which method is best suited for specialized media, please contact the Information Technology Department.

A. Compliance

1. Electronic storage devices: Servers, PCs, Laptops, hard disk drives:

    a. **INTERNAL TRANSFER:** Any device that is transferred between internal departments should be reformatted and reloaded with an Information Services approved image prior to redeployment.

    b. **EXTERNAL DISPOSAL:** Devices being disposed of must follow data cleansing methods set forth by Medic IT Department.

    c. All personnel must either use an approved data cleansing method on all Agency devices or obtain approval from the Agency Assistant Director of Operations to use an equivalent software program or method. If the system is non-operational or can't be booted up, the hard disk must be physically destroyed by crushing, drilling, or incinerating.

2. Telecommunications equipment: Routers, switches, key systems, PBXs, etc.

    Refer to Medic Electronic Equipment Disposal Policy.

3. Other electronic storage devices: Copiers, PDAs, Fax Machines, Routers, Medical Monitoring devices, etc.

    Other electronic devices that contain any type of electronic storage must also have their disk/ROM cleaned by a method approved by the IT Department before the device is transferred from the current owner's possession. For inquiries on methods for data cleansing, please contact the IT Department.

4. Portable Media

    Portable media (tapes, CD-ROMs, DVDs) may be destroyed by crushing, incinerating, shredding, or melting.

B. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.23 Information Services Security Policy
Effective 11/1/05; Revised 2/19/09

POLICY
This document describes the policies and procedures used by Mecklenburg EMS Agency (Medic) to protect the confidentially, availability, and integrity of the electronic protected health information it creates, receives, maintains, or transmits. These safeguards are intended to protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

As an organization defined as a "covered entity" Medic will follow all standards, requirements and implementation specifications of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

PROCEDURE:

A. Security Management Process

Medic has established Policies and Procedures to prevent, detect, contain and correct security violations in accordance with §164.308 (a)(1).

1. Risk Analysis – Medic has performed an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information.
2. Risk Management – Medic has implemented a formal risk management process to identify risks and vulnerabilities and reduce them to a reasonable and appropriate level to comply with §164.306(a) as defined in the *Information Security Risk Management Policy*.
3. Sanction Policy – Medic has implemented appropriate sanction policies to address workforce members who fail to comply with the security policies and procedures as defined in the *Sanctions Policy* and *Communications Environment Acceptable Use Policy.*
4. Activity Review – Medic's Information Technology Task Group conducts and/or directs the review of information system activity, such as audit logs, access reports, and security incident tracking reports on a schedule established based on the results of the risk management process.

B. Assigned Security Responsibility

Medic has identified and designated the Security contact who is responsible for the development and implementation of the policies and procedures in accordance with §164.308 (a)(2) as defined in the *Assigned HIPAA Security Responsibility policy.*

C. Workforce Security

Medic has implemented policies and procedures to ensure that all members of this organization's workforce have appropriate access to electronic protected health information, as provided under §164.308 (a)(4) of this section, and to prevent those workforce members who do not have access under this subpart from obtaining access to electronic protected health information in accordance with §164.308 (a)(3).

1. Authorization and/or Supervision – All access to protected health information must be specifically authorized and/or, if deemed necessary, directly supervised.
2. Workforce Clearance Procedure – Medic performs background checks (including criminal background checks), reference checks and check against duly authorized

licensing, disciplining and sanctioning authorities on each individual who is a candidate for employment by Medic.

3. Termination Procedures – Medic has implemented a practice for terminating access to electronic protected health information when the employment of a workforce member ends.

D. Security Awareness and Training

Medic has implemented a security awareness and training program for all members of this organization's workforce, including management in accordance with §164.308 (a)(5).

1. Security Reminders – Implementation of periodic security updates.
2. Protection from Malicious Software – Implementation of procedures for guarding against, detecting, and reporting malicious software.
   a. Medic utilizes a multi-layered anti-virus strategy; virus checking is performed on mission critical Intel servers, e-mail servers, desktops.
   b. Intel servers , e-mail servers, and desktops receive updated virus signatures.
   c. Virus signatures are distributed in real time as available from the Virus software's update server and manually when circumstances (i.e. high alert virus outbreak) dictate.
   d. Periodic training of all workforce personnel.
3. Password Management – Implementation of procedures for creating, changing, and safeguarding passwords as defined in the *Communications Acceptable Use Policy.*

E. Security Incident Procedures

In accordance with §164.308 (a)(6) Medic has implemented policies and procedures to identify and respond to suspected or known security incidents, and mitigate, to the extent practicable, harmful effects or security incidents that are known and document security incident outcomes. Written policies have been developed for the following contingencies:

1. Information Technology Task Group
2. High Alert Virus
3. Software Vulnerabilities and Patch Management

F. Contingency Plan

Medic has implemented the necessary mechanisms required in accordance with §164.308 (a) (7) and Medic bases contingencies on the likelihood of occurrence, impact to operation and ability to implement the needed remedies. A contingency plan is the only way to protect the availability, integrity and security of data during unexpected negative events. The Agency has established and implemented policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information (EPHI).

1. Data Backup Plan – Backup copies of all EPHI on Mecklenburg EMS Agency electronic media and information systems must be made regularly.
   a. Backup of EPHI on Agency information systems and electronic media is stored in a secure remote location, at a sufficient distance from Medic facilities to escape damage from a disaster at Medic Data Center.
   b. Backup copies of EPHI stored at secure remote locations must be accessible to authorized Medic employees for timely retrieval of the information.
   c. The backup media containing EPHI at the remote backup storage site must be given an appropriate level of physical and environmental protection consistent with the standards applied to EPHI physically housed at the Agency's Data Center.

2. Medic's disaster recovery plan is currently being developed to recover its information systems if they are impacted by a disaster. The plan will be reviewed regularly and revised as necessary. The plan will include:
   a. The conditions for activating the plan.
   b. Identification and definition of Agency workforce member responsibilities.
   c. Resumption procedures (manual and automated) which describe the actions to be taken to return Medic information systems to normal operations within required time frames.
   d. Analysis of the relative criticality of specific applications and data in order to determine the order in which information systems will be recovered.
   e. Notification and reporting procedures.
   f. A maintenance schedule that specifies how and when the plan will be tested, as well as the process for maintaining the plan.

G. Evaluation

Medic has a 3rd party vendor to perform periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that will establish the extent to which the security policies and procedures meet the requirements of the Security Standards in accordance with §164.308 (a)(8).

1. Vulnerability Testing - The Agency is currently implementing security tools to periodically test its production servers for host vulnerabilities. Baseline scans of desktops are conducted to determine the status of deployed updates by the Microsoft Update Server. Additionally, the Production Environment is periodically tested in order to discover unexpected conditions. Unexpected results from vulnerability testing are reported to the Agency to ensure proper resolution.
2. Log File Analysis – The Agency is currently evaluating products to import and parse key log files such as firewalls, VPN Reports, Anti-virus, and remote access , and Security event logs to be reviewed frequently for unexpected, suspicious activity and raise alerts if such activity is detected.
3. Security Reviews – Currently Medic is planning to review high-risk systems and/or processes on an established schedule to ensure their compliance and readiness.
4. If any intrusion is detected, the Information Technology Task Group will be notified immediately

H. Business Associate Contracts and Other Arrangements

In accordance with §164.306, Medic may permit a business associate to create, receive, maintain, or transmit electronic protected health information on this organization's behalf only if we obtain satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information and in accordance with §164.308 (b)(1).

I. Facility Access Controls

Medic has implemented policies and procedures to limit physical access to the electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed in accordance with §164.310(a)(1).

1. Contingency Operations – Establishment and implementation on an as needed basis procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an

emergency.

2. Facility Security Plan – Implementation of policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.
    a. Data Center: An environmentally controlled data center with 24/7 security in the form of on-site personnel and card-key only entry into the facility. Currently access to the server room is via key card entry to the CMED communications center. All access to the communications center is logged by Threshold Security Software. Plans are underway to place card reader on entry door to server room.
3. Access Control and Validation Procedures – Implementation of procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision.
4. Maintenance Records – All modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks) must be requested through a formal process as defined at each facility.

J. Workstation Use and Security

The *Communications Environment Acceptable Use Policy* specifies the proper functions to be performed and the physical safeguards for workstations that can access electronic protected health information in accordance with §164.310(b) and §164.310(c).

K. Device and Media Controls

Medic has implemented policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of our facility, and the movement of these items within the facility in accordance with §164.310(d)(1).

1. Disposal – Implementation of policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored - *Information Services Electronic Data Cleansing Policy.*
2. Media Re-Use – Implementation of procedures for removal of electronic protected health information from electronic media before the media are made available for re-use – *Information Services Electronic Data Cleansing Policy.*
3. Accountability – Medic maintains a record of the movements of workstation and server hardware for final disposal.
4. Data Back-Up and Storage – Information Technology personnel determines on a case-by-case basis if the creation of a retrievable, out-of-cycle backup of electronic protected health information is necessary before movement of equipment.

L. Access Control

1. Medic has implemented technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4) and in accordance with §164.312(a)(1).

2. Unique User Identifier – Assignment of a unique name and/or number for identifying and tracking user identity as required by the C*ommunications Environment Acceptable Use Policy.*
3. Automatic Logoff – While automatic logoff capabilities vary widely across different systems, automatic logoff will be implemented when available and may be supplemented by the workstation operating system automatic screen savers activated after a designated period of inactivity. The length of inactivity to initiate the automatic

logoff and/or screen saver will be determined by risk analysis and will vary depending upon the environment, e.g. public areas will have a shorter time frame while private office settings will have a longer time frame.

4. Encryption and Decryption – The transmission of protected health information across an open network, e.g. the Internet, is prohibited. The Agency has implemented a variety of encryption mechanisms for safely transmitting protected information; they include:
    a. Secure Sockets Layer (SSL)
    b. Virtual Private Networks (VPN)
    c. Secure File Transfer Protocol (SFTP)
    d. Other options may be utilized upon approval by the IT Department

M. Audit Controls

Medic has implemented hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information in accordance with §164.312(b).

N. Integrity

Medic recognizes the importance of protecting information assets against improper or unauthorized alteration or destruction and will utilize the many integrated technical integrity mechanisms in today's hardware and software such as error-correcting memory, read after write disk storage, cyclical redundancy checks, input validation ranges, etc. to comply with §164.312(c).

O. Person or Entity Authentication

Medic has implemented procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed in accordance with §164.312(d). These include:

1. Unique User ID required for access to protected health information
2. Two factor authentication required for remote access
3. When access is needed for support or maintenance activities, Vendors must coordinate with their designated Medic liaison to have their account activated for an agreed upon time frame.

P. Transmission Security

Medic has implemented technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network in accordance with §164.312(e).

1. Integrity Controls
    a. Medic utilizes standard network protocols such as CRC, check sum calculations and message hashing to ensure data integrity during transmission.
    b. The necessity for additional integrity checks will be determined on a case-by-case basis based upon a risk analysis.
2. Encryption
    a. Transmission over "open networks", e.g. The Internet, will use an approved encryption method as outlined in *Communications Environment Acceptable Use Policy.*
    b. The necessity for encryption of data at rest or during transmission within the Agency private network will be determined on a case-by-case basis based upon a risk analysis.

7.24 IT Software Vulnerability Response Policy

Effective 11/1/05; Revised 2/19/09

POLICY

Mecklenburg EMS Agency will utilize a multi-layered approach - blocking, patching, and antivirus-based defenses - for responding to publicized threats to its key computerized systems and information services infrastructure that are deemed high-risk. Any response will be based on the characteristics of the individual threat, where the threat is in its life cycle and will follow the principle of “least disruption” to applications and systems.

PROCEDURE

A. The Information Technology Department will actively monitor various national security sources such as US-CERT and SANS, as well as strategic vendors like Cisco, Microsoft, McKesson, Cerner, etc to learn of publicized threats and vulnerabilities that are considered to be high-risk.

B. Upon learning of a high-risk vulnerability or threat, the IT Task Group, working in conjunction with the Assistant Director of Operations, will determine the appropriate response based on the characteristics of the threat and where it is in its life cycle in order to protect the Agency communications environment while causing the least disruption to applications and systems.

C. Once a high-risk threat has been declared and communicated, the various teams accountable for supporting the impacted systems and applications will be responsible for taking the necessary steps to mitigate the threat and provide periodic status reports until their efforts are completed.

D. All Alerts will be communicated via e-mail. The updates will be comprised of communication by the IT Task Group, and final changes will be the responsibility of Assistant Director of Operations. All communication to update status, will the responsibility of the IT Task Group. The IT Task Group has the responsibility to keep the Assistant Director of Operations up to date during the Alert timeframes.

7.25 Password Policy

Effective 11/1/05; Revised 2/19/09

POLICY

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Mecklenburg EMS Agency's entire corporate network. As such, all Mecklenburg EMS Agency employees (including contractors and vendors with access to Mecklenburg EMS Agency systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

SUMMARY

This policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Mecklenburg EMS Agency facility, has access to the Mecklenburg EMS Agency network, or stores any non-public Mecklenburg EMS Agency information.

PROCEDURE

1. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed every 120 days. The recommended change is on a quarterly basis.
2. All user-level passwords (e.g., email, web, desktop computer, domain level, etc.) must be changed at least every six months. The recommended change interval is every four months.
3. Passwords must not be inserted into email messages or other forms of electronic communication.
4. All user-level and system-level passwords must conform to the guidelines described below.

A. Guidelines

Passwords are used for various purposes at Mecklenburg EMS Agency. Some of the more common uses include: network accounts, system accounts, screen saver protection, voicemail password, and remote access logins. Everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

1. The password contains less than eight characters
2. The password is a word found in a dictionary (English or foreign)
3. The password is a common usage word such as:
   a. Names of family, pets, friends, co-workers, fantasy characters, etc.
   b. Computer terms and names, commands, sites, companies, hardware, software.
   c. The words "Mecklenburg EMS Agency", "sanjose", "sanfran" or any derivation.
   d. Birthdays and other personal information such as addresses and phone numbers.
   e. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
   f. Any of the above spelled backwards.
   g. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

1. Contain both upper and lower case characters (e.g., a-z, A-Z)
2. Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
3. Are at least eight alphanumeric characters long.

4. Are not a word in any language, slang, dialect, jargon, etc.
5. Are not based on personal information, names of family, etc.
6. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards
Do not use the same password for Mecklenburg EMS Agency accounts as for other non-Mecklenburg EMS Agency access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Mecklenburg EMS Agency access needs. For example, select one password for the network login and a separate password for IT systems.

Do not share Mecklenburg EMS Agency passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Mecklenburg EMS Agency information.

Here is a list of "don't":

1. Don't reveal a password over the phone to ANYONE
2. Don't reveal a password in an email message
3. Don't reveal a password to the boss
4. Don't talk about a password in front of others
5. Don't hint at the format of a password (e.g., "my family name")
6. Don't reveal a password on questionnaires or security forms
7. Don't share a password with family members
8. Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Agency IT Department.

Do not use the "Remember Password" feature of applications (e.g., OutLook, Internet Explorer).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Blackberry's or similar devices) without encryption.

If an account or password is suspected to have been compromised, report the incident to the Agencies IT Department and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by IT or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.26 Remote Access Policy
Effective 11/1/05; Revised 2/19/09

POLICY
This policy is to define standards for connecting to Mecklenburg EMS Agency's network from any host. These standards are designed to minimize the potential exposure to Mecklenburg EMS Agency from damages which may result from unauthorized use of Mecklenburg EMS Agency resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Mecklenburg EMS Agency internal systems, etc.

PROCEDURES

A. Compliance

This policy applies to all Mecklenburg EMS Agency employees, contractors, vendors and agents with a Mecklenburg EMS Agency-owned or personally-owned computer or workstation used to connect to the Mecklenburg EMS Agency network. This policy applies to remote access connections used to do work on behalf of Mecklenburg EMS Agency, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

B. General Responsibility

1. It is the responsibility of Mecklenburg EMS Agency employees, contractors, vendors and agents with remote access privileges to Mecklenburg EMS Agency's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Mecklenburg EMS Agency.
2. General access to the Internet for recreational use by immediate household members through the Mecklenburg EMS Agency Network on personal computers is not permitted. The Mecklenburg EMS Agency employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Mecklenburg EMS Agency's network:
    a. Virtual Private Network (VPN) Policy
    b. Wireless Communications Policy
    c. Acceptable Use Policy

C. Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases.
2. At no time should any Mecklenburg EMS Agency employee provide their login or email password to anyone, not even family members.
3. Mecklenburg EMS Agency employees and contractors with remote access privileges must ensure that their Mecklenburg EMS Agency-owned or personal computer or workstation, which is remotely connected to Mecklenburg EMS Agency's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. Mecklenburg EMS Agency employees and contractors with remote access privileges to Mecklenburg EMS Agency's corporate network must not use non-Mecklenburg EMS Agency email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to

conduct Mecklenburg EMS Agency business, thereby ensuring that official business is never confused with personal business.

5. All hosts that are connected to Mecklenburg EMS Agency internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.

D. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.27 Telecommunications Electronic Equipment Disposal Policy

Effective 11/1/05; Revised 2/19/09

POLICY

This policy prohibits disposal of telecommunication equipment without prior removal of sensitive data. Only equipment that has met the criteria of this policy or has been granted an exclusive waiver by IT Department is approved for disposal.

PROCEDURE

A. Compliance

This policy covers all telecommunication equipment (e.g., routers, switches, PBXs, key system, etc.) used/owned by Medic. Equipment provided and maintained by 3rd party vendors do not fall under the purview of this policy.

To comply with this policy, telecommunication equipment must:

- For routers and switches, delete the configurations.
- For key systems, reset the systems database.
- For PBXs, perform a system upgrade and use the “default” database.
- For any other telecommunication device, follow the vendor recommendations for removal of data.

B. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.28 Virtual Private Network (VPN) Policy

Effective 11/1/05; Revised 2/19/09

POLICY

This policy is to provide guidelines for Remote Access or Virtual Private Network (VPN) connections to the Mecklenburg EMS Agency network.

PROCEDURES

A. Compliance

This policy applies to all Mecklenburg EMS Agency employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Mecklenburg EMS Agency network. This policy applies to implementations of VPN that are directed through a VPN Concentrator.

B. General Responsibility

Approved Mecklenburg EMS Agency employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Mecklenburg EMS Agency internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a public/private key system with a strong passphrase.
3. Currently, RADIUS authentication to the domain is being implemented to allow users to login with their domain credentials.
4. Dual (split) tunneling is permitted; only the traffic to the local MEDIC lan is tunneled, all other traffic bypasses the VPN encryption.
5. VPN gateways will be set up and managed by Mecklenburg EMS Agency IT Department.
6. All computers connected to Mecklenburg EMS Agency internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard; this includes personal computers.
7. Users of computers that are not Mecklenburg EMS Agency-owned equipment must configure the equipment to comply with Mecklenburg EMS Agency's VPN and Network policies
8. VPN users will be automatically disconnected from Mecklenburg EMS Agency's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
9. The absolute connections times to the network vary.
    a. Medic - max 10 hours
    b. Vendors – max 12 hours
    c. Wireless – max 8 hours
    d. NRG – max 4 hours
10. Simultaneous logins are limited to 2

D. Enforcement : Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

I have read and understand the acceptable use policy, and will abide by it while I am connected to the Medic network.

Signature: _____

Print Name:_____

Date: _____

7.29 Wireless Communications Policy

Effective 11/1/05; Revised 2/19/09

POLICY

This policy prohibits access to Mecklenburg EMS Agency networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Agency's IT Department are approved for connectivity to Mecklenburg EMS Agency's networks.

PROCEDURES

A. Compliance

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of Mecklenburg EMS Agency's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Mecklenburg EMS Agency's networks do not fall under the purview of this policy.

B. Requirements

All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by Agency's IT Department. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be configured and tested by the Agency's IT Department.

C. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8.1 Agency Vehicle Policy
Effective 4/22/05

Purpose
To insure safe and appropriate use of Agency vehicles

Policy
Employees required to use any Agency vehicle must adhere to the guidelines set forth in the departmental driving policy. Specific information on the Agency's driving policy should be directed to a supervisor or the Risk & Safety Specialist.

Agency vehicles are intended for use in the conduct of Agency related business or activities that promote the Agency or facilitate efficiency.

1. Requirements to operate Agency vehicles:

   Non-Emergency Vehicles - Possess a valid U.S. state driver's license and to maintain insurability with the Agency's insurance carrier.

   Emergency Vehicles - Possess a valid U.S. state driver's license, successfully complete the Agency's approved driving course (i.e. NAPD) and maintain insurability with the Agency's insurance carrier.

   The Agency and/or insurance carrier shall periodically review each employee's motor vehicle record. Any employee found to be an unacceptable risk or liability may be required to attend remedial driver training. If the Agency's independent insurance carrier declares the employee to be uninsurable, the employee will be precluded from operating Agency vehicles. The ability to operate a vehicle is a job requirement for most Agency employees, specifically, but not limited to field medics and support services staff. Loss of driving privileges may disqualify these employees from continued employment with the Agency.

   Employees must immediately report to the Agency any traffic violation, conviction or accident that occurs outside of employment.

2. Employees shall not operate Agency vehicles while under the influence of medications and/or substances that are known to impair central nervous system (CNS) functions (i.e., judgment, physical coordination and/or reaction time). Included in this categorization are medications that carry warnings against operating vehicles or machinery.
3. Employees involved in vehicular crashes are subject to drug and alcohol testing.
4. Agency vehicles must be operated with due regard and safety for yourself and others.
5. Seat restraints are to be properly utilized at all times by all persons riding in any Agency owned/leased vehicle. All patients are to be secured in the patient compartment area. Person(s) attending patients(s) must wear seat restraints. However, situations may arise where the caregiver(s) will need to disengage the seat restraint to perform a skill or retrieve medical equipment/supplies, etc., after this is completed the caregiver(s) must re-engage the seat restraints. Manufacturer recommendations are to be followed regarding safety restraint systems and air bags.
6. Agency ambulances must utilize a backer whenever available.
7. Agency vehicles are prohibited from passing a stopped school bus with its stop sign extended.
8. Agency vehicles will comply with traffic signals, signs and school crossing guard signals in school zones during school hours or when children are present.

9. Agency vehicles shall not exceed the posted speed limit by more than ten miles per hour. When operating in posted school zones (during school hours) and/or high pedestrian traffic areas, the posted speed limit must not be exceeded.
10. Use of tobacco products are prohibited inside any Agency owned/leased vehicles.
11. Agency vehicles are prohibited from parking in fire lanes unless they are on a patient care assignment.
12. Failure on the part of any Agency employee (driver, witness, passenger, etc.,) to immediately report to a supervisor any vehicle crash or property damage will be subject to disciplinary action that may include termination.
13. Audible and visual warning devices must be utilized when operating in an emergency mode.
14. Employees must adhere to all safe parking principals which include:

- Apply parking brake
- Apply appropriate transmission (park or neutral)
- Utilize wheel chocks, if applicable
- Apply safe positioning of vehicle at scenes and posts
- Active high idle while on calls
- Keep vehicle locked while unattended
- Connect shoreline

8.2 Alphanumeric Pagers

Effective 1/1/99

Purpose

This policy provides guidelines for the use of alphanumeric pagers.

Policy

Each new employee will be given a personal pager at the time of orientation. Pagers must be on and be located where the on-duty employee can be immediately alerted by its activation.

The Agency asks that employees use the pager system to have family contact them for urgent issues during work hours.

Each employee is responsible for the pager at all times. Circumstances surrounding the loss or damage will be reviewed. The employee may be financially responsible for the full cost for replacement.

Employees are required to return the pager along with all other Agency belongings upon termination of employment.

8.3 Benevolent Fund

Effective 3/1/04, Revised 7/1/05, 7/1/07, 8/15/07, 7/16/08, 11/02/2022

Purpose

To provide financial and in-kind assistance for needy Agency employee in the event of personal or family crisis, hardship beyond the employees control, emergency situation, or disaster.

Policy

Agency employees who suffer a Qualifying Hardship are eligible to apply for financial assistance from the Employee Benevolent Fund. Each Agency employee is eligible for maximum assistance of up to $1000.00 every other rolling calendar year. The purpose of the Fund is to provide for payment of basic needs such as food, clothing, housing (including repairs), medical care and funeral expenses caused by a Qualifying Hardship. The Fund is not intended to provide assistance with discretionary or luxury expenses. Employees will be required to substantiate the need and document a Qualifying Hardship. The employee must demonstrate steps taken to mitigate the hardship or situation. The Fund is not intended to be a substitution of wages for employees unable to work.

Eligibility

This Fund is intended for the benefit of any Agency employee who is in good standing, and their immediate family only. “Good Standing” is any employee that has at least 90 days of service, has not received disciplinary action at or above a level 5 in the past 12 months, and/or has no outstanding financial obligations to the agency.

The benevolent committee reserves the right to review submissions on a case-by-case basis for eligibility.

Funding

The Fund is to be financed solely through voluntary contributions by employees and any other person wishing to donate. Employees may hold fundraising activities such as car washes, bake sales, etc. provided: (i) such activities are approved in advance by the Agency and (ii) 100% of all proceeds raised are made payable to the Fund. Employees may also make direct contributions through payroll deductions through the Agency Finance Department. All contributions to the Fund are non-refundable.

Disbursement

Normal disbursement of funds shall not be made until approved by the majority of the Benevolent Fund Committee, with 2/3 of the members voting. In an emergency case the Human Resources Director can approve disbursement of funds with an immediate report back to the committee. Applications for disbursements shall be made through submission of a Request for Funds Form, which is available in the Human Resources Department. The Benevolent Fund Committee shall review each request and, upon completion of such review, approve or disapprove (in whole or in part) each request. The Committee may request additional information from the applicant before making its decision. The Committee has full discretion in approving and disapproving applications for assistance and may consider such things as the relative merits of the request, length of service of the employee, the balance remaining in the Fund, and the number of pending requests for assistance. All decisions of the Committee are final and not subject to appeal.

Financial Disclosing

Employees should assume that contributions to the Fund are not tax deductible and that payments received from the Fund are taxable, unless the employee has received advice from a qualified tax advisor to the contrary. The Committee upon request will publish quarterly and annual reports, which will be made available to employees summarizing the Fund balance and disbursements made.

8.4 Duty Exchanges
Effective 1/1/99

Purpose
To establish guidelines for exchanging work hours which is flexible for employees and which protects the Agency from additional salary expense.

Policy

1. The duty exchange is strictly a contract between employees. The Agency shall not be liable for repayment of time with either compensation time or overtime pay in the event one of the employees fails to comply with the agreement. By signing Duty Exchanges, employees accept responsibility for shift and all consequences for being absent, tardy or no-shows.
2. In the event one or both employees fail to comply with the agreement, the employee will be held responsible for assigned shift and will be charged leave for any time away from work.
3. The switch date and the payback date must both be in the same pay week.
4. The Agency considers this Policy to be a privilege. Any abuse will result in the loss of the privilege.
5. The Duty Exchange Form must be in the supervisor’s office 12 hours prior to the requested dates.

The Duty Exchange Form must have both employees' signatures.

8.5 Housekeeping Duties

Effective 1/1/99

Purpose

To maintain a clean, safe and professional work environment.

Policy

All employees are expected to maintain their work area in a clean, orderly and business-like manner. All staff is also expected to assist in maintaining the appearance and cleanliness of common areas such as hallways, meeting rooms, restrooms and lunch break areas. Specific housekeeping duties may vary according to workstation assignment.

No personal cooking appliances may be used in any Agency facility.

8.6 Inspections and Searches

Effective 1/1/99

Purpose

To ensure safety to all and to protect Agency property

Policy

The Agency reserves the right to conduct searches or inspections of property assigned to an employee and their personal belongings whenever a supervisor/manager has reasonable grounds for suspecting that the search will result in evidence of a violation of Agency policies. Such searches or inspections may include, for example, an employee's locker, desk, computer and Agency assigned vehicles. Search efforts will be conducted by the employee's supervisor/manager and a minimum of one (1) individual designated by the Executive Director.

Employees should not consider any property assigned to them, such as lockers, desks or computers, as their own personal property. This property is owned by the Agency and is subject to search if violations of policy or law are suspected. Employees are not permitted to remove any company property from the premises without the prior written approval of their supervisors.

8.7 Facility Usage by Off-Duty Personnel

Effective 1/1/05

Purpose

To ensure proper use of Agency facilities by off-duty personnel.

Policy

1. Agency facilities are designed for the use of on duty personnel. Due to space limitations, additional personnel who are not on duty could interfere with operations or create a risk of injury to themselves or others.

2. Agency personnel who are not on duty will respect the need of on duty personnel to have priority regarding the use of Agency facilities.

3. Employees who wish to use facilities for off-duty activities (exercise facility excluded) must obtain prior approval from the Executive Director or designee.

8.8 Solicitation and Bulletin Boards

Effective 1/1/99

Purpose

It is the policy of the Agency to prohibit solicitation and distribution on its premises by Agency employees and non-employees, except as allowed under Federal and State law and this policy. The Agency also requires a clean workplace with a professional appearance.

Policy

1. The Agency maintains bulletin boards to communicate Agency information to employees and to post notices required by law. The bulletin boards are to be used for posting Agency information and notices only. The Human Resources Department will be responsible for placing notices or taking down material on bulletin boards.

2. Official postings may be copied and placed by the Human Resources Department in other places and stations in order for the employee to be able to read the information provided.

3. Official postings, such as job opportunities, directives, and policy revisions, will be posted for a minimum of one (1) week.

Solicitation and distribution of literature is prohibited during the working time of either the employee making the solicitation or the targeted employee without approval of the Executive Director.

8.9 Tobacco Use

Effective 10/1/2015, Revised 12/1/07, Revised 06/11/2015

Purpose

Tobacco use has been acknowledged to be a safety and health hazard. For this reason, the Agency is taking a positive step toward establishing and maintaining a healthier and safer environment for patients, visitors, and employees by initiating a tobacco-free environment. This policy provides employees with guidelines for tobacco use.

Mecklenburg EMS Agency employees, contractors, and others performing services for Mecklenburg EMS Agency are prohibited from smoking, using smokeless tobacco (chew, dip, snuff, etc.) and/or electronic or other nicotine delivery devices (electronic cigarettes, cigars, hookahs, pipes, etc.) in:

- Mecklenburg EMS Agency Buildings
- Mecklenburg EMS Agency Grounds/Parking Lots (to include personal vehicles)
- Mecklenburg EMS Agency Vehicles

Employees who violate this policy will be subject to disciplinary action and, if applicable, the higher "Tobacco-Use" premiums for Agency offered health insurance.

A tobacco product excludes any product that has been approved by the United States Food and Drug Administration for sale as a tobacco cessation product and is being marketed and sold solely for such an approved purpose.

Quitting/Cessation Resources

Mecklenburg EMS Agency is committed to providing a healthy work environment. To help achieve this goal, employees are encouraged to seek assistance in cutting back or quitting smoking or other tobacco use. Mecklenburg EMS Agency offers access to and supports voluntary employee participation in a variety of smoking and tobacco-use cessation programs. Please contact a member of the Human Resource Department for additional information.
In addition, the North Carolina Tobacco Use Quitline 1-800-QUIT-NOW (1-800-784-8669) is a free quit support service.

Definitions

For purposes of this policy, the following shall be defined as:

Building—A building or enclosed area leased, owned, or occupied by Mecklenburg EMS Agency (to include all Posts.)

Grounds/Parking Lots—An area leased, owned, or occupied by Mecklenburg EMS Agency including all parking lots (including personal vehicles), sidewalks, greenspace, courtyards, etc.

Vehicle—A vehicle leased, owned, or otherwise controlled by Mecklenburg EMS Agency.

8.10 Travel
Effective 11/1/03

Purpose
Mecklenburg EMS Agency will either pay for or reimburse an employee for expenses incurred on approved business travel. Expenses shall be properly documented, and a timely and accurate accounting shall be made in accordance with this policy.

Travel Authorization Procedures:

Business travel that requires lodging or transportation costs must be approved using the Travel Authorization form.

The Travel Authorization form is available on the Network Drive in the Forms folder. Open the file and save it as a file on your personal network or hard drive.

Section 1: Section 1 should be completed to record and save your airline/hotel/rental preferences on your online Travel Authorization form. This information will be used each time travel is requested and authorized.

Section 2: Complete Section 2 for each instance of business travel. When researching flights, you may indicate flight numbers and/or flight times in the spaces provided. All costs should be *estimated* until travel is authorized and flights/hotel/car is confirmed. If estimated costs are above $300, a purchase order number should be obtained from the Finance Department. When requesting the Agency to pre-pay expenses, please attach a completed check request with the Travel Authorization form. If the travel involves a Saturday night stay over to obtain a less expensive airline ticket, cost justification must be provided. When travel has been authorized, the check request will be sent to the Finance Department for processing.

Section 3: When requesting that travel arrangements be reserved for you, please indicate your request(s) for reservations at the top of Section 3. Complete the remainder of Section 3 when requesting that reservations be made on your behalf using a credit card.

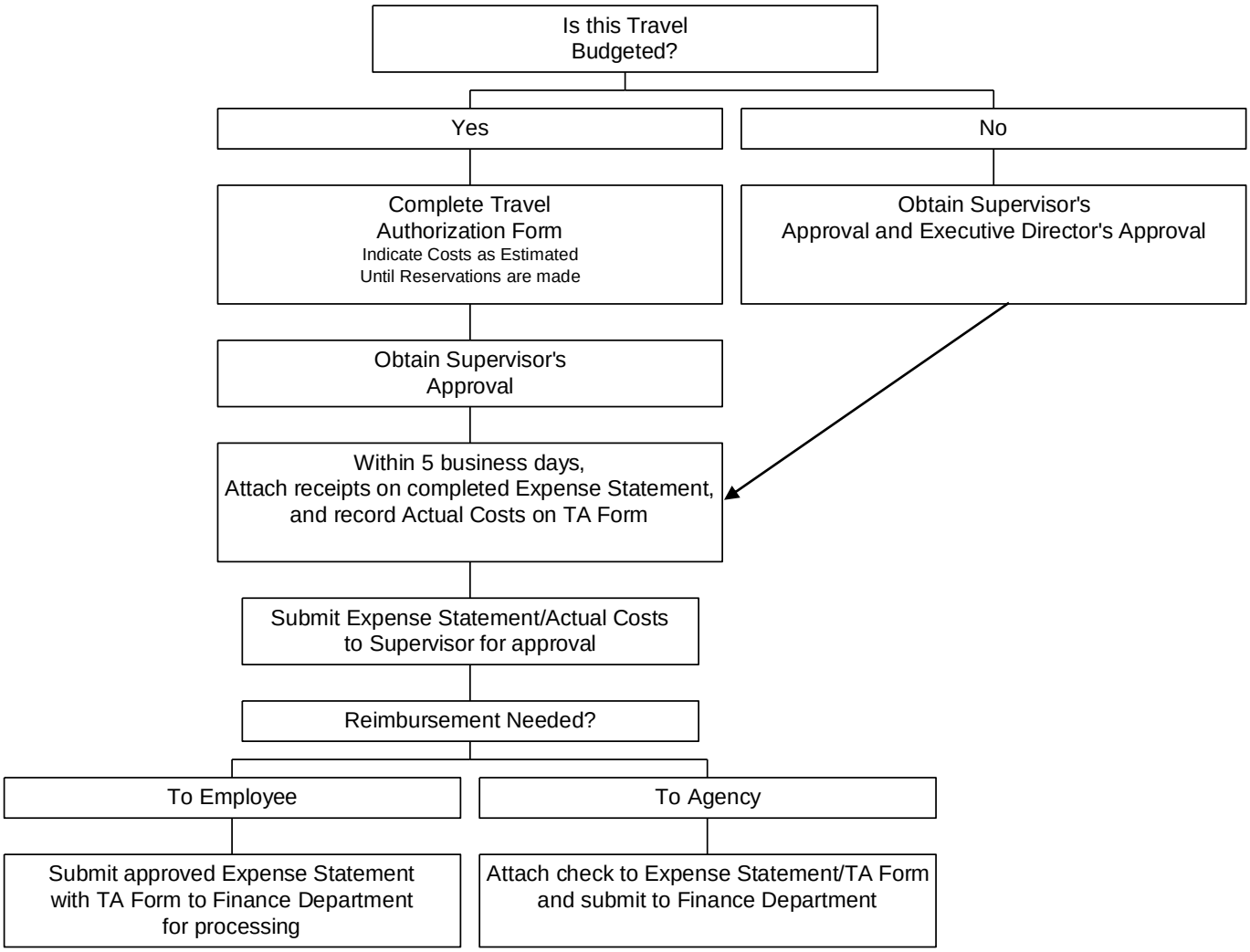
Upon completion of travel:

Reimbursement to employee/employer:
Within five (5) days of completion of travel, attach all relevant receipts to a completed Expense Statement, which also can be found on the Network Drive, in the Forms folder. Update your approved Travel Authorization form, complete the *actual* expenses incurred, and complete Section 4. Attach a copy of your updated, approved Travel Authorization form, and submit to your supervisor for approval. After approval, submit to the Finance Department for processing.

No additional money due:

Within five (5) days of completion of travel, attach all relevant receipts to a completed Expense Statement, which also can be found on the Network Drive, in the Forms folder. Update your approved Travel Authorization form, complete the *actual* expenses incurred, and complete Section 4. Attach a copy of your updated, approved Travel Authorization form, and submit to your supervisor for approval.

Travel Authorization Process



8.11 Usage of Agency Equipment and Resources
Effective 1/1/99

Purpose
To ensure Agency equipment and resources are used for Agency purposes only.

Policy
Agency employees are prohibited from performing any tasks during scheduled work hours and/or utilizing Agency business equipment (phones, fax, copiers, etc.) at any time when the employee's intention is to realize a personal financial gain.

Willful damage, theft or destruction of Agency property is grounds for discipline.

8.12 Weapons

Effective 1/1/99, Revised 3/1/18

Purpose

To provide a work atmosphere that is highly reputable and safe for our employees and customers.

Policy

1. Employees, contractors, and visitors are prohibited from the possession of a firearm, with or without a concealed carry permit, or any other deadly weapon on Agency or County property or in Agency owned or leased vehicles (firearms, explosives, self-defense sprays, knives, etc.).

2. Exceptions are as follows:

    6. Employees and contractors, who are required to possess a weapon as a part of their job duties, are exempt from this provision if approved by the County Security Director and County Attorney's Office. Moreover, sworn law enforcement officers are exempt from this provision if acting in an official law enforcement capacity.

    7. Weapons removed from patients while in transit or on the scene where no police officer is present to take possession.

    8. Kitchen utensils and rescue tools.

3. Any weapon that must be transported should be stored in a vehicle compartment that prevents easy or immediate access to patients and/or passengers.

4. If an employee must handle a weapon it should be done with extreme caution and in a fashion that does not damage criminal evidence. If still on scene, request assistance of any on-scene law enforcement personnel and document the event.

5. Upon arrival at hospital any weapons should be turned over to the police officer/security personnel. Documentation of the officer's name and their department/employer must be made.

6. Employees with a concealed handgun permit may, nevertheless, secure their handgun on County or Agency property in a locked, private vehicle within a trunk, glove box, or other enclosed compartment or area within or on the private vehicle to prevent easy or immediate access to patients and or passengers.

7. While off-duty, employees with concealed handgun permits may carry their guns on County parks and recreation facilities subject to the same restrictions as other members of the public.

RIGHT TO SEARCH

Mecklenburg EMS Agency reserves the right to search Agency vehicles, Agency work spaces, and other property owned, operated, or controlled by the Agency. Any illegal object found will be turned over to law enforcement authorities.

8.13 Workplace Safety and Violence in the Workplace

Effective 1/1/99

Purpose

To create a safe working environment for all Agency employees

Policy

It is the policy of the Agency to prohibit workplace violence. Workplace violence includes, but is not limited to, harassment, threat, and physical attack or property damage. Harassment is defined as behavior or communication designed or intended to intimidate, menace or frighten another person. Threat is an expression of intent to cause physical or mental harm. Physical attack is defined as unwanted or hostile physical contact such as hitting, fighting, pushing or shoving. Property damage is defined as any intentional damage to property which includes property owned by the Agency, employees, visitors and vendors.

Employees are prohibited from use or possession of a weapon of any kind on Agency property or while on duty. All violators, employees and non-employees will be prosecuted to the fullest extent of the law.

Employees who engage in workplace violence will be subject to immediate disciplinary action.

The Agency reserves the right to search Agency vehicles, Agency work areas and other Agency property. Any illegal object found will be turned over to law enforcement authorities.

8.14 Employee Response to an Active Shooter in the Workplace
Effective 8/4/14

Purpose
To provide guidance to employees on how to react and respond to an incident involving an active shooter in the work place. Active shooter situations are unpredictable and evolve quickly. Typically, the immediate deployment of law enforcement is required to stop the shooting and mitigate harm to victims. Because active shooter incidents are often over within minutes, prior to the arrival of law enforcement on the scene, individuals must be prepared both mentally and physically to deal with an active shooter situation.

Definitions

Active Shooter:	An individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearms(s) and there is no pattern or method to their selection of victims.
Work Place:	The work place includes both buildings at Agency headquarters (Post 100) as well as Agency post locations across Mecklenburg County and facilities that Agency employees utilize (i.e. hospitals, nursing homes, assisted living centers, Charlotte-Douglas International Airport, etc…) as part of job responsibilities.

Policy/Procedure

<u>How to Respond When an Active Shooter is in Your Vicinity:</u>

Employees suddenly confronted with an active shooter situation should quickly determine the most reasonable way to protect their own life. It is important to remember that customers, clients, vendors and visitors are likely to follow the lead of employees and managers during an active shooter situation in any Agency facility.

1. **Evacuate**
   If there is an accessible escape path, attempt to evacuate the premises. Be sure to:
   - Have an escape route and plan in mind
   - Evacuate regardless of whether others agree to follow
   - Leave your belongings behind
   - Help others escape, if possible
   - Prevent individuals from entering an area where the active shooter may be
   - Keep your hands visible
   - Follow the instructions of any police officers
   - Do not attempt to move wounded people
   - Call 911 when you are safe
   - Notify CMED of an active shooting in progress

2. **Hide out**
   If evacuation is not possible, find a place to hide where the active shooter is less likely to find you. Your hiding place should:
   - Be out of the active shooter's view
   - Provide protection if shots are fired in your direction (i.e. an office with a closed and locked door)
   - Not trap you or restrict your options for movement

   To prevent an active shooter from entering your hiding place:

- Lock the door
- Blockade the door with heavy furniture

If the active shooter is nearby:
- Lock the door
- Silence your cell phone and/or pager
- Turn off any source of noise (i.e., radios, televisions, portable radios)
- Hide behind large items (i.e., cabinets, desks)
- Remain quiet

If evacuation and hiding out are not possible:
- Remain calm
- Dial 911, if possible, to alert police to the active shooter's location
- If you cannot speak, leave the line open and allow the dispatcher to listen

3. Take action against the active shooter

As a last resort, and only when your life is in imminent danger, attempt to disrupt and/or incapacitate the active shooter by:
- Acting as aggressively as possible against him/her
- Throwing items and improvising weapons
- Yelling
- Committing to your actions

How to Respond When Law Enforcement Arrives:

Law enforcement's purpose is to stop the active shooter as soon as possible and disrupt any further loss of life and injury. Officers will proceed directly to the area in which the last shots were heard. Officers may arrive in teams. They may wear regular patrol uniforms or external bulletproof vests, Kevlar helmets, and other tactical equipment. Officers may be armed with rifles, shotguns and handguns and may also use pepper spray or tear gas to control the situation. Officers may also shout commands, and may push individuals to the ground for their safety.

When law enforcement arrives:
- Remain calm, and follow officers' instructions
- Put down any items in your hands (i.e. bags, jackets)
- Immediately raise hands and spread fingers
- Keep hands visible at all times
- Avoid making quick movements toward officers such as holding on to them for safety
- Avoid pointing, screaming and/or yelling
- Do not stop to ask officers for help or direction when evacuating, just proceed in the direction from which officers are entering the premises

Information to provide to law enforcement or 911operator:
- Location of the active shooter
- Number of shooters, if more than one
- Physical description of shooter(s)
- Number and type of weapons held by the shooter(s)
- Number of potential victims at the location

The first officers to arrive to the scene will not stop to help injured persons. Expect rescue teams comprised of additional officers and emergency personnel to follow the initial officers. These rescue teams will treat and remove any injured persons. They may also call upon able-bodied individuals to assist in removing the wounded from the premises.

Once you have reached a safe location or an assembly point, you will likely be held in that area by law enforcement until the situation is under control, and all witnesses have been identified and questioned. Do not leave until law enforcement authorities have instructed you to do so.

Considerations for Managers and Supervisors During an Active Shooter Situation:

Employees and non-employees are likely to follow the lead of managers and supervisors during an emergency situation in an Agency facility. During an emergency, managers and supervisors should be familiar with this Emergency Action Plan, and be prepared to:

- Take immediate action
- Remain calm
- Lock and barricade doors
- Evacuate staff and non-employees to a safe area if it is possible to do so

After the active shooter has been incapacitated and is no longer a threat, Agency management should engage in post-event assessments and activities, including:

- An accounting of all individuals to determine who, if anyone, is missing and potentially injured
- Determining a method for notifying families of individuals affected by the active shooter, including notification of any casualties
- Assessing the psychological state of individuals at the scene, and referring them to health care/crisis counseling specialists accordingly
- Identifying and filling any critical personnel or operational gaps left in the organization as a result of the active shooter

An active shooter in the workplace may be a current or former employee, or an acquaintance of a current or former employee. Managers, supervisors and coworkers may notice characteristics of potentially violent behavior in an employee. If you believe an employee or coworker exhibits these characteristics, please notify any supervisor, manager or deputy director immediately.

Good Practices for Coping With a Possible Active Shooter Situation at any Location:

- Be aware of your environment and any possible dangers
- Take note of the two nearest exits in any facility you visit
- If you are in an office, stay there and secure the door
- If you are in a hallway, get into a room and secure the door
- As a last resort, attempt to take the active shooter down. When the shooter is at close range and you cannot flee, your chance of survival is much greater if you try to incapacitate him/her.

CALL 911 WHEN IT IS SAFE TO DO SO!

8.15 IT Restore Policy

Effective 7/1/2015; Revised 7/21/2015

Purpose

The IT backup system is in place for disaster recovery in case of hardware or software failure, or other catastrophic events, which does not include the end users' hardware.

A back-up is a snapshot in time when the last back-up procedure was completed.

Policy

Some restorations will need supervisor/manager approval and can be labor and resource intensive.

To request file restoration, please put in a Service Desk Ticket at http://servicedesk.medic911.com.

Current Corporate Standard for Backup Software:

- Symantec Backup Exec 2014 SP1

8.16 Facility Indoor Air Temperature Policy
Effective 3/1/2018

Purpose
In an effort to conserve energy while providing a comfortable and productive workplace, an indoor air temperature policy maintains allowable temperature set points for Agency facilities.

Policy
During the heating season, ambient room temperature shall not be more than 70 degrees Fahrenheit (+/-2 degrees) during normally occupied hours. This means in reality the temperature may be between 68-72 degrees. Night setback temperatures will be determined by facilities staff based on the building systems ability to recover, but will be in the 55 degree range.

During the cooling season, ambient room temperature shall not be less than 76 degrees Fahrenheit (+/-2 degrees) during normally occupied hours. This means in reality temperature may be between 74-78 degrees. Night setback temperatures will be determined by facilities staff based on the building systems ability to recover, but will be in the 85 degree range.

On rare occasions heating and air conditioning temperatures may be allowed to vary from the allowable range, depending on the building's technology, building layout, the efficiency of the system, and outside temperature & humidity conditions.

Select rooms, such as the ambulance bay, sound stages or server/data storage rooms may require special indoor design environments outside of the limits established within this policy. It is not the intent of this policy to limit or not support these special uses.

Building occupants can contribute to their own comfort by wearing seasonally appropriate clothing.

8.17 Telework Policy
Effective 2/1/2023

Purpose
To provide a viable, flexible work option when appropriate for both the employee and the Agency. Teleworking is not an entitlement nor a company-wide benefit and in no way changes the terms and conditions of employment.

Policy and Procedures
Teleworking: The practice of working at home or away from an employee's assigned work location, is an alternative work arrangement that the Agency may offer to eligible employees when it is determined to be advantageous for both the employee and the Agency. Teleworking does not change the basic terms and conditions of employment with the Agency, and employees are subject to the same policies and procedures that apply when working at the Agency facility. Teleworking is not a benefit or entitlement, but a voluntary alternative work arrangement intended to enhance productivity, creativity, employee satisfaction and/or reduce operating costs. Teleworking employees must complete a formal teleworking agreement which must be approved by the appropriate Department Manager/designee. The employee or the Agency may terminate the agreement at any time for any reason. Should the employee terminate the agreement, they must give the department up to two weeks' notice to make any necessary adjustments.

The Department Manager/designee has the authority to approve individual teleworking arrangements consistent with these guidelines and has the discretion to make a final decision on all teleworking arrangements. Department Managers may develop more specific guidelines based upon the business needs of their department, and will be held accountable for department productivity, performance, and attendance while ensuring adequate engagement amongst their team(s). The guidelines must be consistent with the Agency standards as outlined below:

Position Criteria
Department Managers/designees must consider the following criteria when approving a teleworking arrangement:

- Only active full-time or part-time positions are eligible. Those working on a contract, limited part-time and temporary basis are not eligible. Employees approved to work in a light duty capacity may be eligible to telework if assigned to a position in which telework is offered.
- Positions must have well-developed work plans/outline with clear objectives and appropriate measurement criteria to ensure accountability.
- The needs of customers and co-workers can be met from an alternative location.

Employee Criteria
Department Managers/designees must consider the following criteria when approving a teleworking arrangement:

- Employee has thorough knowledge of the job, their expected performance, and telework expectations.
- The Department Manager or designee may approve a new employee to telework based on department specific training and processes. While teleworking, the new employee must demonstrate they are performing successfully and meeting all Agency expectations.
- The Department Manager or designee at their discretion may have new employees complete a training period in the office prior to the approving the employee to telework.
- The employee must review and sign the *Telework Agreement*. Days and hours for teleworking will be specified and agreed upon as part of the *Telework Agreement*.

- Continuation of the teleworking agreement is at the Department Manager's discretion, which takes into account factors such but not limited to: department needs, performance management, performance improvement needs, and the health and safety of employees.
- The employee must meet the same conditions and standards of employment while teleworking as if they were working onsite, including compliance with all policies and procedures, and work expectations. An employee who violates Agency policy or fails to meet work expectations while teleworking is subject to the Agency's performance improvement, progressive disciplinary process, which may include immediate termination for serious violations.
- Employees must be available by all Agency means of communication during scheduled hours, with the exception of their scheduled lunch or break periods.
- The employee must establish and maintain an adequate, safe space to work.
- Teleworking cannot be used as a substitute for dependent care. Employees will not act as the primary caregiver for dependents during scheduled work hours and while teleworking must manage dependent care and other personal responsibilities in a manner that allows them to successfully meet job responsibilities.
- Employees are responsible for minimizing distractions and avoid unapproved schedule changes while teleworking.
- Dual role employees on an approved telework schedule may be required to report to the office or post during periods of need as reserved by Agency administration.

Management Criteria

Department Managers/designees must consider the following criteria when approving a teleworking arrangement:

- Management must be committed to making the teleworking arrangement successful.
- Management must ensure performance expectations, including telework, attendance, and engagement expectations are clearly outlined with performance management. Management will monitor the productivity of employees' teleworking to ensure they are performing consistently at a level that is meeting all expectations of their role and responsibilities.
- Management will maintain the level of employee engagement both individually and within their team by making sure the lines of communication are open and all employees are treated fairly and equitably. It is expected to maintain regimented one on one meetings with direct reports and at a minimum biweekly check-ins with the entire team. Managers and Supervisors have discretion with respect to additional engagement activities and events for their employees, subject to Agency policies and procedures.

Teleworking Requirements:

- Employees are permitted to work from a remote location including home, mobile office or other approved work site location and must agree to work offsite under the terms and conditions of the *Telework Agreement*. In-person business visits, meetings with customers or regularly scheduled meetings with co-workers shall not be held at the home worksite.
- Employees are required to account for all time worked in accordance with the Agency's current timekeeping policies. Overtime hours must be pre-approved and any deviations from the agreed upon schedule must be approved in advance by the department manager or supervisor.
- Random drug testing protocols will remain in place, set forth by the Drug Free Workplace policy. Employees will be sent for testing on a day they report to the office.
- If the teleworking agreement is modified or canceled, the Department Manager/designee is responsible for identifying office space within the department.

Compliance with Law and Policies and Procedures:

Telecommuting arrangements must comply with federal, state and municipal laws that apply to

Agency employees. This includes, but is not limited to, the Fair Labor Standards Act (FLSA) and Occupational Safety and Health Act (OSHA).

Agency Equipment:

- The equipment and supplies necessary to telework will be provided by a combination of both the employee and the Agency. The equipment issued to a teleworker should be sufficient to support the employee's work requirements; however, the Department Manager/designee should make cost effective decisions as it relates to equipment.
- Employees must have the ability to communicate with other employees and customers in a manner consistent with a non-teleworking employee, utilizing any Agency communication methods necessary.
- Agency provided computer equipment that adheres to Agency standards for hardware, software and related equipment will be provided to employees. The specific type of equipment depends on the job and will be recommended by departmental or Agency IT staff for approval by the Department Manager/designee. Work is prohibited from being performed on a device other than what is provided by the Agency. The use of home peripherals such as monitors, keyboards, mice and printers are allowed, as these devices do not store data. Exceptions to this policy are subject to IT review and must be approved as such.
- The Agency is responsible for the maintenance and support of Agency owned equipment, including hardware and software. If IT is unable to repair remotely, any Agency equipment needing repair or software installation must be returned to the Agency facility for service. If there is a delay in the repair or replacement of the equipment or any other circumstance, which would make it impossible for the teleworker to work off site, then the teleworker will report to the Agency facility until the repair has been made, or the circumstance has been corrected. The Department Manager/designee will be responsible for identifying appropriate office space for the teleworker if the Agency office space has been reallocated.

Cyber Security:

- Employees shall follow all Agency IT policies and procedures when working both at the office, as well as from a remote location. This includes using only agency approved software, including but not limited to chat and video conferencing platforms.
- Sharing materials and documentation is necessary when working remotely. Employees should only use approved methods for sharing files which includes email, secure delivery for encryption through email if warranted, OneDrive, network shares and SharePoint locations.
- Personal on-line storage is prohibited for storage of any Agency data.
- All Agency equipment must be secured at the end of the workday which includes logging off or powering down all equipment. Internet connections are inherently insecure, even home networks. Therefore, employees must use the Agency's sanctioned virtual private network (VPN) to connect to the Agency's network before performing any work. Exceptions to this standard should be submitted through the IT Service Desk.
- Employees are responsible for safeguarding all confidential or sensitive material when at home following all HIPAA and PHI compliance policies. This includes protected health information (PHI), personally identifiable information (PII), and Agency proprietary information. Paper copies of documents should be shredded at home, if possible, or securely brought back to the office location for disposal in a secure shred bin.
- Agency equipment should be used for work-related activities only, minimizing activities performed for personal use as described in Medic's Acceptable Use Policy. Additional IT resources when teleworking can be found on the Agency's policies and procedures manual.

Safety
The employee is responsible for establishing and maintaining an adequate and safe workspace and for providing a work environment free of interruptions and distractions that would affect performance. The home office must meet safety guidelines, and the Agency reserves the right to make on-site inspections during normal business hours as defined in the teleworking agreement. The home office should function in the same way and with the same safety awareness as if working at the Agency facility. Employees are expected to follow basic safety precautions in their homes. These include:

- **Walking surfaces** – Keep floor surfaces level and dry. Ensure that carpets are in good condition and secured to the floor. Keep telephone and electrical cords out of walkways. Outdoor walkways, porches, and steps should also be kept clear of obstacles, debris, ice, and snow.
- **Fire Hazards** – Keep combustible materials to a minimum and dispose of trash promptly. Be sure to have a functioning smoke detector and fire extinguisher in the work area. Be sure that all paths of egress are clear of any obstacles. If you use a portable heater, keep it away from combustible materials and be sure that it has a tip over switch in case it tips over. Be sure that all equipment is UL approved.
- **Electrical Safety** – Keep electrical plugs, cords and receptacles in good repair. Use surge protectors with computers. Do not place electrical cords under rugs or heavy furniture. Do not overload extension cords or plugs.
- **Air Quality** – Work in a well-ventilated area.
- **Lighting –** Ensure all lighting is adequate and computer equipment is not subject to glare from lighting or windows.
- **Ergonomics –** Make the work area adjustable to the person working in the space. Maintain proper posture. Be sure office furniture is in good repair.

Since the home office is an extension of Agency workspace during the hours and days established in the teleworking agreement, any on-the-job accidents or injuries will be covered under the Agency's Workers' Compensation Program provided that such accidents or injuries are within the course and scope of the job and occur during the specified teleworking schedule.

Employees must report any work-related accidents or injuries immediately to their supervisor and Risk and Safety, as if working in the normal office environment and report to Concentra for assessment and treatment. Worker's Compensation claims are subject to review and investigation by the Risk Management Division, which reserves the right to inspect home workspaces following any reported on- the-job injury.

Expenses
Normal business expenses incurred while teleworking will fall under the same eligibility/rules of reimbursement as if the expenses incurred in the office. Employees are expected to obtain necessary office supplies when they are at the regular Agency office. Local internet service provider charges will be the responsibility of the teleworker. Other business expenses must be submitted and approved using the normal reimbursement process established by the teleworker's department and the Agency Finance Department.

Emergencies
A teleworking employee may sometimes, but not always, be affected by an emergency requiring the Agency office to close. For example, on a snow day where the Agency releases employees early or opens late, the teleworking employees would be expected to follow their normal work schedule if working at home. If an emergency such as loss of power affects the teleworker's home office for a major portion of the day, the employee may be required to report to the office or take vacation leave if unable to do so. Dual or field employees on an approved telework

schedule may be required to report to the office or post during periods of emergencies.

Residents Outside of North Carolina

Employees who telework from outside of North Carolina must follow IRS regulations as it relates to state taxation. Employees who are approved to telework from their home address in a non-NC residence are required to complete the appropriate state W4 Form the appropriate state Tax Distribution Form which are available on the payroll portal (UKG). It is the employee's responsibility to inform Human Resources if their residence state changes, or there are changes to telework eligibility.

Chapter 9 - Terminating or Retiring from Medic

9.1 Exit Interviews

Effective 1/1/99; Revised 1/1/07

Purpose

To allow terminating employees an opportunity to reflect on their work experiences and to collect information pertaining to benefits.

Policy

The Agency encourages each terminating employee to utilize the exit interview process. This process assists the Agency in identifying any causes of dissatisfaction leading to turnover among employees and ensuring the Corporate Compliance Program has been understood and followed. Whenever improper or illegal conduct is reported, the Agency Compliance Director will initiate an investigation.

When an employee submits a written notice or otherwise announces a resignation, the Human Resources Department will invite eligible employees (voluntary terminations) to participate in the exit interview process. The employee can participate in one of two ways:

a. completing the exit interview questionnaire; or
b. requesting a personal or phone interview with a Human Resources representative

Exit Interviews are conducted in the Human Resources Department with all individuals who choose to leave the Agency. During this interview, employees will be informed about their last paycheck, information regarding reference checks and continued insurance options that are available through COBRA. All Agency property such as name tags, pagers, keys, uniforms and turnout gear will also be collected.

Employees are asked to contact the Human Resources Department to set up an appointment prior to their last day worked.

9.2 Insurance Coverage at Termination or Retirement
Effective 2/1/05

Purpose
Employees leaving the Agency or retiring from the Agency with less than 10 years of service may remain under the group coverage for up to 18 months through the COBRA program and are fully responsible for paying all premiums. These individuals may convert to a non-group plan, if necessary, by contacting the Human Resource Department. Employees who have a minimum of five years of service and are leaving the Agency due to a work related injury or retiring from the Agency due to a work related injury, may remain under the group coverage until eligible for Medicare or age 65 and are responsible for paying all premiums.

Individuals who exercise their option to retire before age 65 may remain under the group coverage until age 65 or eligible for Medicare by paying their portion of the premium cost if they have had a minimum of 10 years of service with the Agency and/or military time credited to NCLGERS. These retirees and retirees at age 65 or over may convert to a Medicare Supplement, if necessary. There is no dental coverage for retirees.

The Agency will reimburse its retirees for medical insurance premiums as follows:

1. Agency retirees under age 65 with 10 but less than 20 years of qualifying service with the Agency and/or military time credited to the NCLGERS have a choice of plan options:

   Standard plan - 50% of the individual premium

   Enhanced plan – 50% of the Agency paid portion of the individual premium. Retirees are responsible for paying their portion of the individual premium.

2. Agency retirees under age 65 with 20 years or more of qualifying service with The Agency and/or military time credited to the NCLGERS have a choice of plan options:

   Standard plan - 100% of the individual premium.

   Enhanced plan – 100% of the Agency paid portion of the individual premium. Retirees are responsible for paying their portion of the individual premium.

3. Agency retirees who are 65 or older at the time of retirement are eligible to participate in the Medicare supplement plan if they have a minimum of 10 years of qualifying service with the Agency and/or military time credited to the NCLGERS. If Agency retirees have 10 years of qualifying service but less than 20 years, the Agency will pay 50% of the individual premium for the Medicare supplement plan. If Agency retirees have 20 years or more of qualifying service, the Agency will pay 100% of the individual premium for the Medicare supplement plan. Medicare eligible retirees may select another Medicare supplement plan in lieu of the Agency's plan and the Agency will reimburse them up to the same percentage and cost that the Agency would have contributed had they been in the Agency's plan. If Medicare eligible retirees opt out of the Agency's plan, they are not eligible to participate in the plan at a future date.

The Agency will not reimburse retirees for medical insurance premiums or allow them to participate in any group insurance plan if the retiree was convicted of or entered a plea of guilty or no contest to a criminal act, which caused financial injury to the Agency. This provision is effective January 1, 1998.

Employees who leave the Agency and retire from another jurisdiction that participates in the North Carolina Local Government Employee Retirement System will not be eligible for Agency retiree benefits.

COVERAGE AT TERMINATION OR RETIREMENT

Employees leaving Mecklenburg County may remain under the group coverage for up to 18 months through the COBRA program and are fully responsible for paying all premiums.

Employees retiring from Mecklenburg County may be eligible to remain on the County's medical insurance. Anyone employed by Mecklenburg County for the first time after July 1, 2010 will not be eligible to remain on the County's medical insurance upon retirement. Please refer to the Benefits section of the Human Resources Policy for a full description of the eligibility requirements.

The County will not reimburse retirees for medical insurance premiums or allow them to participate in any group insurance plan if the retiree was convicted of or entered a plea of guilty or no contest to a criminal act which caused financial injury to the County. This provision is effective January 1, 1998.

Employees who leave Mecklenburg County and retire from another jurisdiction that participates in the North Carolina Local Government Employee Retirement System will not be eligible for Mecklenburg County retiree benefits.

9.3 Terminations - Voluntary

Effective 1/1/99

Purpose

To provide a mechanism to voluntarily separate from the Agency.

Policy

1. Hourly employees should provide two (2) weeks notice. Salaried employees should provide four (4) weeks notice. Failure to provide advanced notice may disqualify the employee from certain re-employment opportunities and other benefits.

2. Notice of termination must be given in writing to the Human Resources Department and copies to the department supervisor.

3. Employees terminating are responsible for returning all Agency property (pagers, cell phones, gear, uniforms, etc.) and settling outstanding accounts before issuance of final pay.

4. Final pay is made on the regularly scheduled payday following the last pay period in which the employee worked.

5. If an employee is rehired following previous termination, the employee must re-qualify for eligibility of employee benefits. Seniority will start on the employee's new hire date. (Some benefits may be mandated by law for continuance.)

6. An unreported absence of two (2) or more scheduled working shifts is considered one form of voluntary termination without proper notice.

7. It is the employee's responsibility to return from a leave of absence. Voluntary termination may be put into effect if the employee has not contacted Human Resources within 24-hours of the expected date of return.

8. Exit interviews will be conducted in Human Resources.

9.4 Termination Appeal Process (In-Voluntary Terminations)

Effective 1/1/05; Revised 9/1/07

Purpose

To provide employees with a mechanism to appeal an involuntary termination decision regarding their employment.

Policy

Full time employees terminated involuntarily have the right to appeal the decision by submitting a request for appeal to the Executive Director. The request for appeal must include the stated reason for termination, on what basis the employee feels the termination was wrong or unfair and the proposed resolution. The request for appeal must be received by the Executive Director within (ten) 10 days from the date of termination. Failure to submit the appeal within the time prescribed shall be deemed to be a waiver by the employee of the right to appeal the termination.

The Executive Director will review the appeal and factors contributing to the termination and render a decision within (ten) 10 days of receiving the request for appeal.

The Human Resources Department will facilitate this process; therefore, employees are asked to contact the Director of Human Resources for assistance.

Employees who are terminated involuntarily during their Employee Introductory Period are not entitled to an appeal process.