PATIENT CARE AND PRIVACY

Patient Care
Each patient will be treated as an individual and with dignity and respect at all times.

Privacy
Patients have a right to personal privacy, as protected by the Health Insurance Portability and Accountability Act, and all employees, volunteers and students must protect the confidentiality and security of patient information. Accessing patient information for non-job-related use is strictly prohibited. MEDIC maintains policies and procedures to specifically address privacy and security matters, including how to appropriately use and share patient information.

What is HIPAA?
HIPAA, the Health Insurance Portability & Accountability Act, is a civil rights law that gives patients important rights with respect to their protected health information (PHI).

What is PHI?
PHI includes any information that is created or received while a healthcare worker is providing treatment, processing payment or performing other healthcare operations. PHI relates to the past, present or future physical or mental health of a patient and can be contained in electronic, written and oral communications.

Records requests and requests for PHI are handled through HR/Risk and Safety. Never provide or release HIPAA/Privacy Protected information unless authorized to do so.

MEDIC OUR PATIENTS. OUR PEOPLE. OUR STEWARDSHIP. OUR PURPOSE.

PATIENT INFORMATION IS EVERYWHERE

Patient information is not just in paper or electronic records. Here are some examples of other places you might find patient information:

- Financial records
- Fax sheets
- Data used for research purposes
- Prescription bottle labels
- Photograph or video recordings of a patient

MEDIC OUR PATIENTS. OUR PEOPLE. OUR STEWARDSHIP. OUR PURPOSE.

PHI: PATIENT IDENTIFIERS

HIPAA protects information that alone or combined may identify a patient, the patient's relatives, employer, or household members. Health information that includes even ONE patient identifier is PHI and is protected under HIPAA.

Examples:

- Name
- Address
- Date of Birth
- Telephone numbers
- Fax numbers
- Email addresses
- SSN
- Account number
- Photographic images

SHARING PATIENT MEDICAL INFORMATION

Sometimes it's okay to talk in front of family and friends. Sometimes it's not okay.

It's okay to:	It's not okay if:
• Share only necessary information when family/friends are involved in the patient's care • Examples: – The patient's caregiver is onsite and the patient doesn't object to them hearing the conversation – The patient's adult family member is present and has questions – The patient's spouse needs treatment care information – You need family input to make healthcare decisions in an emergency situation	• The patient asks you not to talk to his/her family about his/her condition • A family member wants a copy of the patient's transport. This requires a written authorization from the patient. • A curious co-worker is calling to know what's going on. Only friends and family designated by the patient are allowed to get information.

INCIDENTAL DISCLOSURES

Sometimes, as part of your job, you use or disclose patient information that may be overheard or inadvertently seen by someone else. These situations are called *incidental disclosures.*

Some examples of how to limit incidental disclosures while still appropriately using patient information to care for patients include:

- Keeping your voice down when discussing patient information with partner or patients in non-private areas.
- Only displaying limited information or turning computer screens away from public view in areas where others might see them.

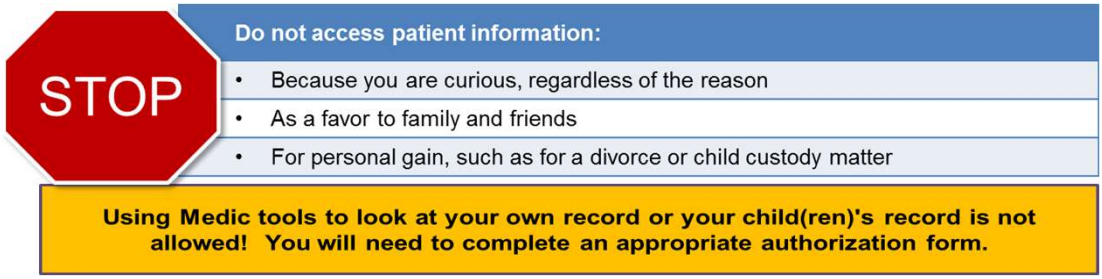
ACCESSING PATIENT INFORMATION

Remember this acronym for accessing patient information:

TPO = Treatment, Payment, Operations

Patient Protected Health Information (PHI) should only be accessed for legitimate treatment, payment or healthcare operation reasons (quality, education, risk management, etc.).

All other uses or disclosures require an authorization, an exception or a law!



TAKING CONFIDENTIAL INFORMATION OFFSITE

If you take confidential information outside of Medic, you must protect it.
You are responsible for all patient information in your possession!

If you must take confidential information offsite:
❑ Take as little patient information needed to do the work
❑ Remove confidential and patient information from your vehicle or lock in your car. Never leave information in view or unattended!
❑ Keep a list of what patient information you take. Return all patient information as soon as possible.
❑ Do not take patient information into a public place, such as a restaurant or coffee shop.
❑ Secure patient information in your home. Do not let others (including family and friends) view or access it.
❑ Notify your Supervisor or the Corporate Privacy Officer immediately if patient information or confidential information is lost or stolen. Notify IT if you lose an electronic device.

DISCARDING PATIENT INFORMATION

You take care of patients, so take care of their information. Protect our patients - think before you throw patient information away.
Discard anything that contains patient information into a confidential shred bin.

Paper	Labels	Electronic PHI
• Throw away all paper containing patient information into a locked shred bin.	• Throw away removable labels containing patient information into a locked shred bin.	• Contact the IT Department for proper disposal of electronic PHI.

Be on the lookout for: Personal information that patients may have left behind in the ambulance or trash cans (such as discharge instructions, prescriptions and other information) must be placed in a shred bin.

SOCIAL NETWORKING

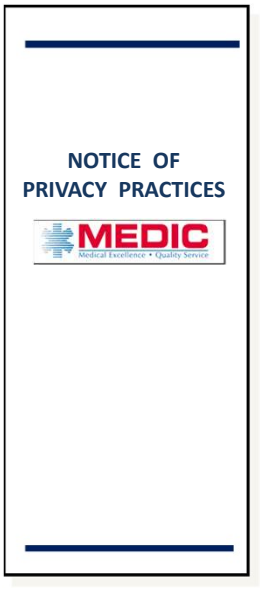
Social media is a great tool that allows individuals to communicate via networking sites such as LinkedIn, Facebook, Twitter, and Pinterest. It is important to remember that the internet is a public domain and information posted via social media can be permanent and may have a broadcasting effect. You have an obligation to safeguard PHI regardless of the setting!

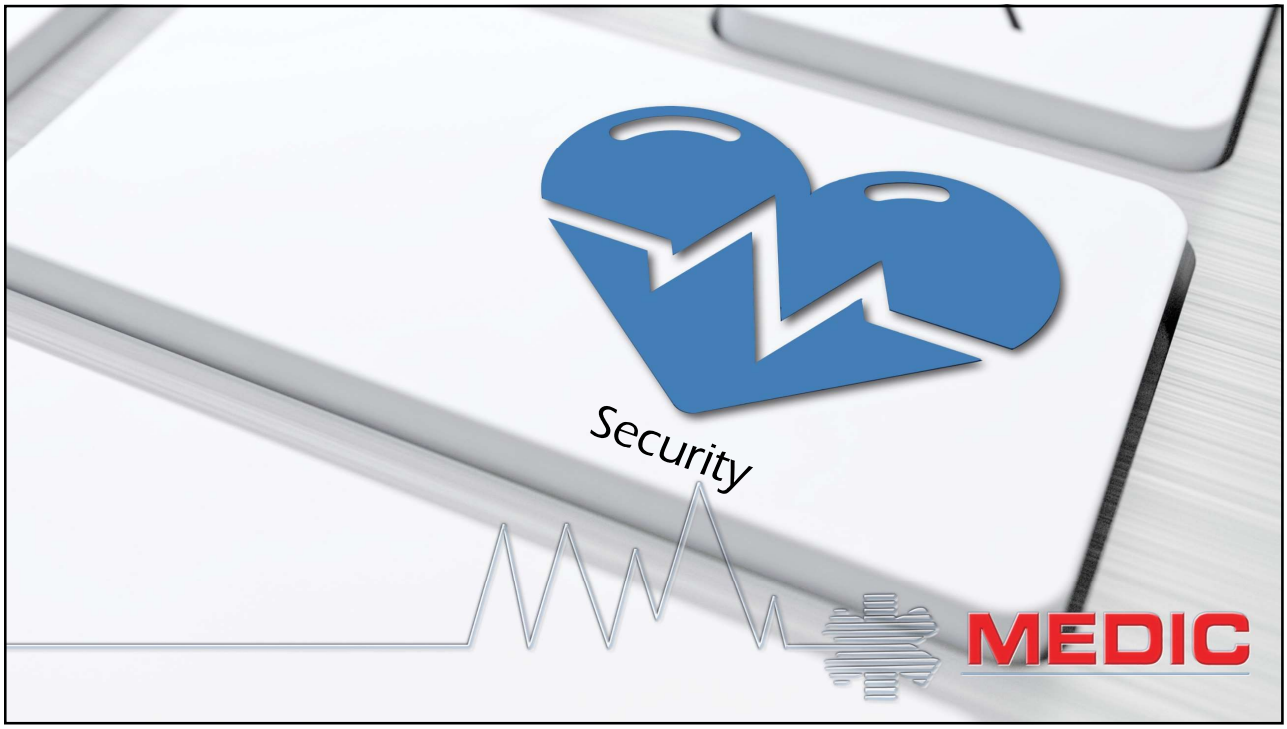
- ❑ Never communicate patient information through social media. It is not allowed and will result in disciplinary action, including sanctions and end of employment.
- ❑ Never post identifying information about patients **or their images**. **Removing a patient's name is not enough to make the patient anonymous.**
- ❑ Look at the photo backgrounds. Photos taken may accidentally show a patient, computer screens or internal information.
- ❑ Do not "friend" patients on social media.

PATIENT RIGHTS

All patients have the right to:

Receive a copy of a Notice of Privacy Practices (NPP). English and Spanish copies are available. You may find these notices in the acrylic holders inside the back of every ambulance.
Request that we limit the use or release of their information. Request that their communications be confidential.
Review and/or receive a copy of their patient transport records.
Request an amendment (change) to their patient transport records.
Request an accounting showing when and with whom their information has been shared.
File a privacy complaint against a healthcare provider, insurer and the U.S. Government.
Be informed when the privacy of their patient information has been breached.
Pay for their services in full and request that their healthcare provider not share information with their health plan. Medic must agree to this type of restriction for qualified situations.





SECURITY 101

NEVER share your user ID and password with anyone.

- Do not respond to email, phone or other requests for your user ID and password. No one from Information Services, including the Help Desk, will EVER ask for this.
- Do not share your password with co-workers, including new employees that may not have access yet.

DO NOT open, forward, or reply to email messages from unknown or suspicious senders.

- Look for spelling and/or grammatical errors
- Look for request for personal information "Our records indicate that your account was overcharged. You must complete the following form within 7 days to receive your refund."
- Be on the lookout for alarming messages: "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, confirm by clicking on the link below."

Use different passwords for different accounts.

- Keep social networking sites (e.g. Facebook, Twitter, and Pinterest) separate from online banking.
- Keep personal accounts separate from Medic accounts (e.g. social networking sites and online banking).

Ba a safe Internet user

- Look for https:// when entering PHI, credit card information, or other sensitive information online.
- Do not click on pop-ups (advertisements, warnings, etc.).
- Do not download unapproved software.
- Be cautious when downloading documents; be sure you are on a site you know and trust.

Contact the IT Support Center Immediately IF:

- You accidently clicked on a suspicious link or replied to a suspicious email.
- You suspect that someone knows or is using your password.
- You receive unusual error messages or pop-up boxes.
- You lost your laptop, smartphone or any other Agency issued mobile devices.

MEDIC OUR PATIENTS. OUR PEOPLE. OUR STEWARDSHIP. OUR PURPOSE.

WHAT IS PHISHING?

"Phishing" is the act of sending an email pretending to be from an online store (Amazon, eBay), a financial institution (Chase, SunTrust), or even the Help Desk with the intention of gaining personal information from the recipient. Like traditional fishing, it relies on a computer user to take the bait.

Did you know that email phishing is the easiest way for criminals to steal information?

The Phisher forges email addresses to look genuine

The Phisher entices you with an urgent request

The Phisher adds links that appear to connect to a real bank but brings you to a counterfeit site to take your information and money!

MEDIC OUR PATIENTS. OUR PEOPLE. OUR STEWARDSHIP. OUR PURPOSE.

EXAMPLES OF PHISHING MESSAGES

Below are some sample messages you might see from a phishing scam:

To: you@medic911.com

We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below:
www.donotclicklinksfromunknownsenders.com

To: you@medic911.com

During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information.

To: you@medic911.com

Dear Account Holder;

Your current password will expire in the next 24 hours, you are here by directed to kindly click on Sign in to kindly reset your password or you will lose access to your account soon as your password expires.

NOTE: Your login will time out after 60 minutes. Your responses will be lost if you do not click on the "Sign in" button before 60 minutes lapses. There is no prompt when your 60 minute session has expired. Please save extensive comments periodically and check your time.

When in doubt, do NOT click on the emails!

Forward questionable emails to: ITSecurity@medic911.com

SECURING WORKSTATIONS

When using a workstation, including the crew lounge:

- NEVER leave it unattended. Unauthorized people might see information or start typing under your login.
- NEVER let anyone use your login and password. It will show up as you! This is a violation of Medic policy.
- Lock your workstation every time you walk away so others, including co-workers and visitors, cannot access or change information. This will also prevent people from accessing information under your login credentials.