GOVERNANCE

Privacy Official

Written Policies and Procedures

Documentation About Compliance

Workforce Training

Routine Assessments

CONFIDENTIALITY AND SNOOPING

Be discrete in your communications involving PHI.

Don't leave your workstation unattended without locking access to your account.

Contain your curiosity – never snoop into people's records.

Use caution and get the patient's permission prior to discussing PHI in front of others.

DISCLOSURES

PHI may be disclosed only with the person's authorization unless an exception applies.

Mandatory Disclosures

Some mandatory disclosures without a patient's authorization include:

- to a patient who requests PHI from his or her own records

- when required by law
- to report abuse

- to HHS for a compliance investigation

Permitted Disclosures

Some permitted disclosures without a patient's authorization include:

- to deal with a serious and imminent threat to the health or safety of the person or the public

- to respond to law enforcement requests for data

- for treatment, payment, and healthcare operations (TPO)

HIPAA'S SCOPE

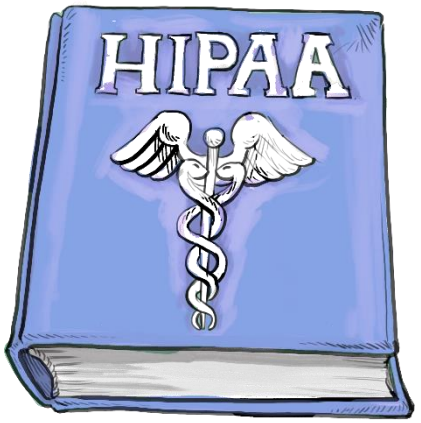
Covered Entities (CEs)

- Healthcare Providers
- Health Plans
- Healthcare Clearinghouses

Business Associates (BAs)

people or entities that create, receive, maintain or transmit PHI on behalf of a CE

Business Associate Agreement (BAA) required to transfer PHI to BA



PATIENT RIGHTS

Notice

receive notice of our privacy practices

Access and Copy

access their information and make a copy of it

Amendment

request an amendment to their records

Restrictions

request restrictions on certain uses and disclosures

File a Complaint

with privacy officer or HHS

Accounting for Disclosures

Patients have a right to find out about disclosures of their PHI during the past 6 years, so you must log non-TPO disclosures of PHI, whether intentional or accidental.

PROTECTED HEALTH INFORMATION (PHI)

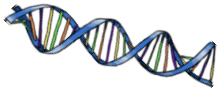
PHI is any individually identifiable health information in any form:

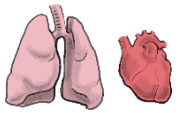
oral

electronic

paper

Information is identifiable if it provides a "reasonable basis" to identify a person.





"Health information" means relating to any past, present, or future health condition or to healthcare or to payment for healthcare.

MINIMUM NECESSARY RULE

Use only the minimum necessary amount of PHI for the purpose of the use.

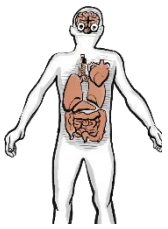
Some exceptions:

- PHI used or disclosed to the patient
- PHI used or disclosed for treatment purposes
- PHI disclosed as required by law

AUTHORIZATION

A valid authorization includes:

- who is disclosing the PHI
- who is receiving the PHI
- what PHI is being disclosed
- reason for disclosure
- how long the authorization will last
- signed and dated by the person



SECURITY

Appropriate administrative, technical and physical safeguards to protect the privacy of PHI.

DATA BREACH

A data breach is an impermissible use or disclosure that compromises the security or privacy of unsecured PHI (not properly encrypted).

CE must notify HHS and affected patients "without reasonable delay" — and no later than 60 days after discovering the breach.

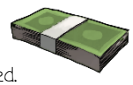
BAs that suffer a breach must notify the CEs that supplied them with the PHI.

ENFORCEMENT

Civil enforcement by the Office for Civil Rights (OCR) at the Dep't of Health and Human Services (HHS).

Fines

Fines can be more than $1.5 million per provision violated.



Imprisonment:

Violations with a malicious motive can lead to personal fines or imprisonment.

TEACHPRIVACY www.teachprivacy.com

Workforce awareness training by Prof. Daniel J. Solove