HIPAA
And Public Health

HIPAA

The purpose for HIPAA (Health Insurance Portability & Accountability Act) is to protect the confidentiality, integrity, and availability of an individual’s medical information.

Hybrid Entity

Public Health (PH) is considered to be a hybrid entity. PH has activities that are covered and other activities not covered by HIPAA.

Public Health & Privacy Rule

The rule recognizes the need for public health authorities and others responsible for ensuring the Public's health and safety to have access to sensitive medical information.

Examples of Health Services

- ✓ Family Planning
- ✓ STD*
- ✓ TB*
- ✓ Child Health
- ✓ Dental
- ✓ Child Lead Poisoning Screening & Case management* (*hybrid)

Public Health Functions

- ✓ Public Health surveillance
- ✓ Program evaluation
- ✓ Emergency preparedness
- ✓ Outbreak investigations
- ✓ Direct health services
- ✓ Public Health research

Sharing Medical Information

- Reporting of disease, injury, and vital events (e.g., birth or death)
- Conducting Public Health surveillance, investigations and interventions such as a person who may have been exposed to a communicable disease or may be at risk for contracting or spreading a disease or condition

Sharing Medical Information

- Reporting child abuse or neglect to a public health or other government authority legally authorized to receive reports
- A person subject to jurisdiction of the Food and Drug Administration (FDA) concerning the quality, safety, or effectiveness of an FDA-related product or activity for which that person has responsibility

Password

- ✓ Use strong passwords (at least 6 characters, containing a combination of letters or numbers)
- ✓ Change your passwords
- ✓ Do not share your passwords
- ✓ If you MUST write down your passwords
  - Store it in a secure location
  - DO NOT store under your desktop or post it

How is PHI transmitted?

- ✓ By sight
- ✓ By face-to-face interactions
- ✓ By fax
- ✓ By email
- ✓ By phone
- ✓ By mail

Minimize Visual Misuse of PHI

- ✓ Clean desk policy
- ✓ Placing medical charts with name faced inward in chart holder
- ✓ Turning monitors away from general public
- ✓ Restricting access to areas where PHI is openly displayed
- ✓ Shredding documents before putting in trash

Face-to Face Use of PHI

- ✓ Conduct conversations in areas apart from others
- ✓ Speak in a low clear voice
- ✓ If referencing a document, don’t show document to another if there is information that the other should not have
- ✓ Make sure no documents are left behind before ending conversation

Faxing Sensitive Medical Information

- ✓ Call to let the receiver know when you are ready to send fax
- ✓ Verify fax number before sending
- ✓ Use a cover sheet
- ✓ Verify that the information was received
- ✓ Fax sensitive medical information only when absolutely necessary
- ✓ Document if it was unintentionally sent to the incorrect number

Use of email

- ✓ Verify the email address before sending
- ✓ Confirm with the receiver that the receiver’s email account is password protected
- ✓ Set your email setting to notify you when an email has been received and opened

Sharing PHI Over the Phone

- ✓ When caller is calling only to confirm details already known by the caller, do NOT volunteer new information
- ✓ Take the organization's name and main number, the caller's name and caller's extension number. Hang up. Call them back – immediately if its an emergency
- ✓ To confirm the caller is who they say they are, check the individual's record and confirm details such as DOB, address, etc

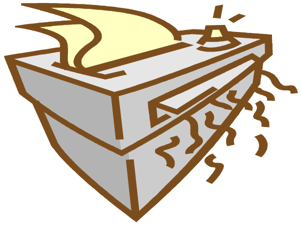
Use of mail

- ✓ Always address confidential material to named addressee
- ✓ Mark the package to show that it contains private information
- ✓ Verify the postal address to which you are sending the PHI
- ✓ Tape seals to the package and sign with your signature over the tape

Appropriate Disposal of Data

All sensitive medical information needs to be properly and appropriately disposed.

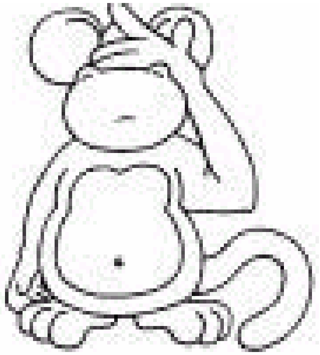
- ✓ NO PHI should be placed in the trash
- ✓ CD ROM disks must be rendered unreadable by shredding, breaking
- ✓ All paper with PHI must be properly disposed of….possibly cross-cut shredder



Physical Safeguards

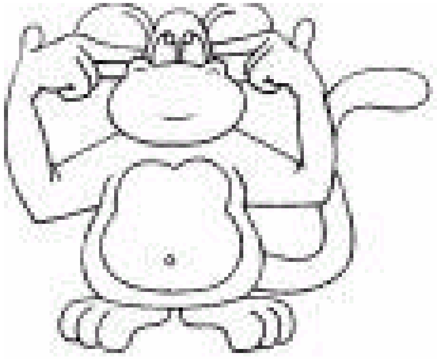
- ✓ Use appropriate facilities & security
- ✓ Workstations Use & Security policies
- ✓ Fax machines, copies and printers are physically secured
- ✓ Servers and mainframes must be protected and access controlled

Something to Keep in Mind

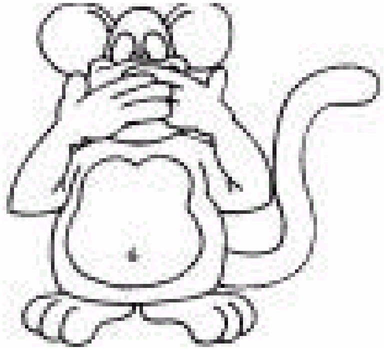


PHI should be seen by only those who are authorized to see it.

Something to Keep in Mind



PHI should be heard by only those who are authorized to hear it.



PHI should be transmitted or shared with only those who are authorized to receive it.

Enforcements for Privacy and Security

- ✓Enforced by different agencies
  - ✓Office of Civil Rights (OCR) enforces privacy with civil penalties
  - ✓Department of Justice (DOJ) enforces privacy with criminal penalties
  - ✓Center for Medicare/Medicaid (CMS) enforces security

What Are the Penalties?

HIPAA calls for severe civil and criminal penalties for noncompliance, including:

- ✓ Fines up to $25K for multiple violations of the same standard in a calendar year
- ✓ Fines up to $250K and/or imprisonment up to 10 years for knowing misuse of sensitive health information

Summary

- ✓ ALL sensitive medical information needs to be treated as confidential
- ✓ Comply with DHSS and DPH policies and procedures
- ✓ Information should only be accessed and shared by authorized staff
- ✓ Protect all information and report any misuse of protected health information

Resources

- ✓ HIPAA Coordinator
- ✓ http://www.hhs.gov/ocr/hipaa/
- ✓ http://www.dhss.delaware.gov/dhss/dph/hipaa.html
- ✓ http://www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf

Questions?

Contact:

Office for Civil Rights
Region III
800-368-1019
Fax 215-861-4431