Health Insurance Portability and Accountability Act (HIPAA) Volunteer Training

Privacy & Security Protection of Public Health Patients Information During a Disaster

Protected Health Information

All employees and **volunteers** are to **safeguard the confidentiality of patients' health information** maintained in any form including **medical records, electronic systems, oral or written communications.**

What is HIPAA?

- Health Insurance Portability and Accountability Act
- Considered the most significant federal healthcare legislation since Medicare was enacted in 1965
- HIPAA creates national standards for privacy and security of patient information
- HIPAA defines certain patient rights such as the patient's right to access her/her medical record information

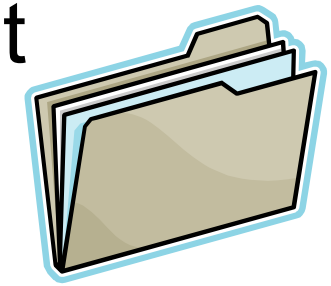
HIPAA? FERPA? What's the Difference?

- Health Insurance Portability and Accountability Act (HIPAA)
  - protects patient rights to privacy regarding health-related information such as the patient's right to access her/her medical record information
    ->> Health care setting

- Family Educational Rights and Privacy Act (FERPA)
  - protects the privacy of students' "education records" which also *includes certain students' health records --> School setting*

Privacy Notices

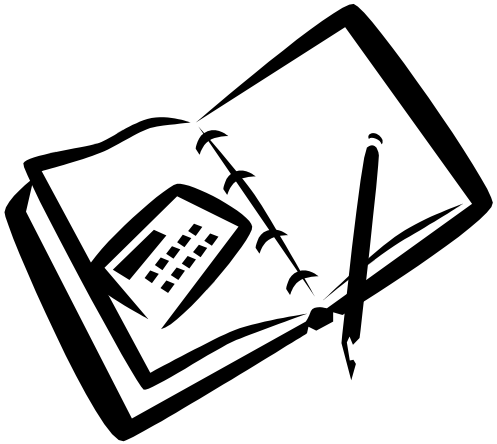
- HIPAA requires covered entities to provide patients with notices of their privacy practices and to document that this was done.



- The *General Consent Form* is used to communicate privacy practices and patient rights. Standard form for SCHD.

Disclosure Logs

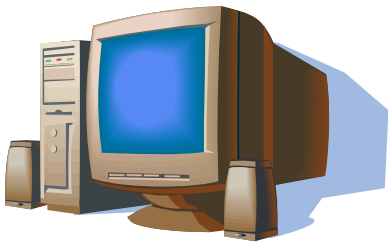
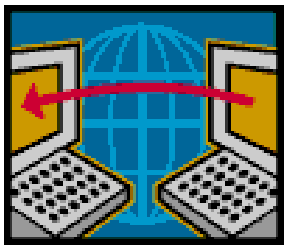
- HIPAA requires covered entities to keep records of disclosures of patient information



Why HIPAA?

- Requires covered entities to
  - develop security standards to control access
  - assure security of electronic protected health information (EPHI) from accidental or intentional disclosure to unauthorized persons



Security Standards

- To protect information from being altered, damaged or destroyed accidentally or deliberately
- To provide for emergency operations and disaster recovery of computer systems

Who must comply?

- Health care providers and staff who conduct certain health care transactions electronically
- Health Care Insurance Plans
- Health Care Clearinghouses

What if we DO NOT comply?

- Employment penalties ranging up to termination and charges
- Non-Compliance
  - $100 for each violation
  - Maximum of $25,000 per year per incident
- Unauthorized Disclosure or Misuse of Patient Information
  - Penalties up to $250,000
  - Prison time up to 10 years

What Information is Protected?

- **P**rotected **H**ealth **I**nformation (PHI)
  - Information about individuals or patients and their past, present or future health conditions
  - All information about patients maintained in electronic paper or oral format

- **E**lectronic **P**rotected **H**ealth **I**nformation (EPHI)
  - Information about patients that is kept in electronic form on computers

The HIPAA Security Policies of the Health Department safeguard this information.

What are Examples of PHI?

- Protected Health Information (PHI) is any information that can identify the individual

- Examples include:
  - Name
  - Address
  - Social Security Number
  - Date of Birth
  - Medical Record Number
  - Medical diagnosis
  - Chief complaint

Examples of Non-Compliance & Unauthorized Disclosures

- One sheet of paper containing PHI left at the front desk and visible to others (sign-in sheet) – Privacy
- One computer system left unattended while logged in – Security
- Knowingly releasing medical record or other PHI to unauthorized individuals - Privacy
- Selling PHI to marketing firms - Variable
- Faxing of PHI to an unsecured office fax machine Security
- Verifying to unauthorized entity the enrollment, diagnosis, or treatment of another individual - Variable

More Examples of Non-Compliance & Unauthorized Disclosures

- Medical Records area left unattended and door open to a public hall – Privacy
- A medical provider sharing their system access code with a another to read a report about a colleague – Security
- Driving with *unsecured* medical records or other patient PHI in vehicle - Privacy
- Leaving medical records on one's desk in an unlocked office in an area with public access - Privacy
- Discarding any public health **computer** in any manner other than by direct transfer to IT staff - Security

Permitted Uses and Disclosures

- Permitted for TPO
  - **T** Treatment
  - **P** Payment
  - **O** Health Care Operations
- Required Disclosures
- To the patient
- To HHS Department for compliance

Permitted Uses and Disclosures

- As required by law
- Law enforcement purposes
- To avert serious threat to health and safety
- Certain public health activities
- To report victims of abuse neglect, domestic violence or injury
- Judicial proceedings
- Worker's compensation

Release of Protected Health Information Form

- Other uses and disclosures require the patient's specific authorization (and signature) using the **Release of Protected Health Information Form**
- Regardless to use, Disclosure Log must be used

Minimum Necessary Standard or Need to Know Rules

- The Privacy Rule limits employees' access only to:
  - the type of PHI needed to perform their jobs
  - disclosures to other entities for only the PHI needed to achieve the intended purposes

- Minimum Necessary Standard does not apply for:
  - Disclosures made to a patient for his own record
  - Does not apply uses or disclosures required by law

Not Subject to HIPAA

- HIPAA excludes individually identifiable health information contained in
  - Employment Records of a covered entity
  - Education records covered by the Family Education Rights and Privacy Act (FERPA)

10 Deadly HIPAA-Related Sins

1. Thou shalt not discuss or disclose any patient information with others, including family or friends, who do not have a need to know the information.
2. Thou shalt only access patient information for which you have specific authorization to access in order to do your job.
3. Thou shalt not make inquiries for patient information for other persons who do not have proper authority.
4. Thou shalt keep your computer password confidential and not share it with anyone or knowingly use another person's password instead of your own for any reason.
5. Thou shalt control physical access to medical records and other areas with patient information including computers, fax machines, printers, copiers and file cabinets.

10 Deadly HIPAA-Related Sins

6. Thou shalt not discuss or disclose any patient information with others, including family or friends, who do not have a need to know the information.
7. Thou shalt always use a cover sheet that includes a confidentiality statement when faxing medical information.
8. Thou shalt understand the requirements regarding transmission of **ENCRYPTED** patient information via email internally only.
9. Thou shalt not make any unauthorized transmission, inquiries, modifications or purging of patient protected health information in any system.
10. Thou shalt log off or prohibit screen access which contains any patient protected health information prior to leaving any computer or terminal unattended.

It is your duty as **volunteer** to report any breach of confidentiality that you observe.

Best Practices for Privacy and Security of Health Information

Security of EPHI

- Create a good password
  - (8 characters in length with a combination of letters, numbers and symbols)
- Keep the password confidential.
  - Do not share passwords.
- If you must write passwords down in order to remember them, put them in a safe place.

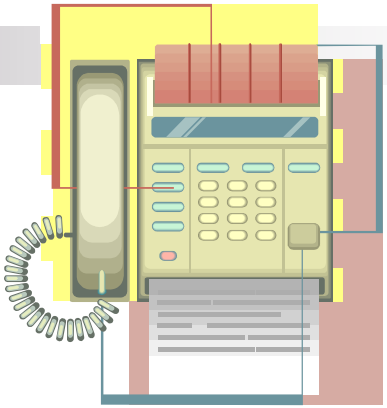
PHI at the Workplace and Volunteer Response Efforts

- Turn computer monitors away from general public.
- Restrict access to areas where PHI is openly displayed.
- Turn PHI face down when you step away from your desk.
- Place unneeded PHI like labels and encounter forms in the SHRED-IT bin in your work area.
- Seek private areas to share confidential information.

Faxing PHI

- Fax can be a high security risk if not used properly.
- Patient medical information (with the exception of information related to HIV and STDS) may be transmitted via fax when needed for IMMEDIATE PATIENT CARE ONLY.
- Always use a cover sheet that includes a confidentiality statement.

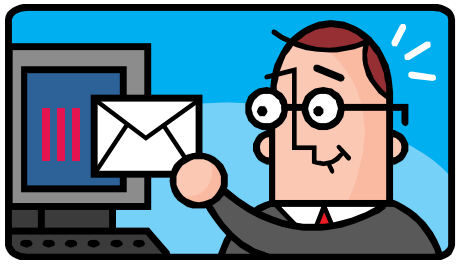
Faxing PHI



- Verify identity of person to whom you are faxing information.
- Ensure faxes can be received in a **secure** manner that limits unauthorized access to information.
- Pre-program frequently used numbers.

Emailing PHI

- Email can be a high security risk if not used properly.
- Protected Health Information (PHI) via email may be sent internally but it MUST be ENCRYPTED to be sent outside the department.



Transporting PHI

- Never leave PHI unattended at off-site locations.
- Maintain PHI in a secure enclosure such as a briefcase or carrying case.
- Keep PHI out of public view when transporting in car or van.




Transporting PHI - Examples

1. Relocating medical record from one clinic to another.
2. Transporting the client records completed during a home visit.
3. Transporting pre-packaged and labeled medications to a community-based client

Privacy of PHI

- Never access information that you are not specifically authorized to access.
  - The department monitors work stations for correct use of PHI.
- Treat all PHI confidential even when you learn it accidentally.

Physical Security and Access

- Only workforce members and authorized visitors are to be allowed access to SECURE AREAS where PHI is kept.

- Visitors should be appropriately monitored and escorted to assure that they do not access confidential information.

Physical Security

- Physical access to sensitive office equipment should be controlled - including computers, printers, copiers, fax machines, and file cabinets.

- PHI must not be left unattended on computer printers, copiers and fax machines.

HIPAA Compliance for Volunteers

- Each volunteer must comply with HIPAA regulations
- Volunteers are required to sign a HIPAA confidentiality agreement
- When warranted attend advanced HIPAA re-currency training for updates

And finally…

- We have a legal, moral and ethical responsibility to protect patient information as if it were our own.

- HIPAA is everyone's responsibility.