HIPAA and Confidentiality:

Confidentiality as related to health care dates back to the Hippocratic Oath:

"And whatsoever I shall see or hear in the course of my profession, as well as outside my profession…if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets."

Confidentiality is a precept of the Hippocratic Oath and the American Medical Association's Code of Ethics.

Not only is a breach of confidentiality unethical, it is also illegal.

All information concerning patients is referred to as *privileged information* and should only be shared with the hospital employees who are caring for that patient.

"HIPAA" stands for the Health Insurance Portability and Accountability Act of 1996.

History of HIPAA

- Congress passed this landmark law to provide consumers with greater access to health care insurance, to protect the privacy of health care data, and to promote more standardization and efficiency in the health care industry.

- While HIPAA covers a number of important health care issues, this informational series focuses on the Administrative Simplification portion of the law – specifically HIPAA's Electronic Transactions and Code Sets requirements.

Confidentiality

- Individuals have the right to personal and information privacy.
- Confidentiality involves earning and maintaining trust.
- Confidentiality and privacy are synonymous.

There are four parts to HIPAA's Administrative Simplification

Electronic transactions and code sets standards requirements

- Transactions are activities involving the transfer of health care information for specific purposes.
  - Under HIPAA Administration Simplification if a health care provider engages in one of the identified transactions, they must comply with the standard for that transaction.
  - HIPAA requires every provider who does business electronically to use the same health care transactions, code sets, and identifiers.
  - HIPAA has identified ten standard transactions for Electronic Data Interchange (EDI) for the transmission of health care data.

- Code sets are the codes used to identify specific diagnosis and clinical procedures on claims and encounter forms.
  - The CPT-4 and ICD-9 codes that you are familiar with are examples of code sets for procedure and diagnosis coding.
  - Other code sets adopted under the Administrative Simplification provisions of HIPAA include codes sets used for claims involving medical supplies, dental services, and drugs.

Privacy requirements

The privacy requirements govern disclosure of patient protected health information (PHI), while protecting patient rights.

Security requirements

The security regulation adopts administrative, technical, and physical safeguards required to prevent unauthorized access to protected health care information. The Department of Health & Human Services published final instructions on security requirements in the Federal Register on February 20, 2003. The deadlines for compliance are April 20, 2005, and April 20, 2006 for small health plans.

National identifier requirements

HIPAA will require that health care providers, health plans, and employers have standard national numbers that identify them on standard transactions.

The Employer Identification Number (EIN), issued by the Internal Revenue Service (IRS), was selected as the identifier for employers and was adopted effective July 30, 2002.

The remaining identifiers, such as the national patient identifier, are expected to be determined in the coming year.

Terms to Know

- Use – sharing PHI within the entity that maintains the information.
- Disclosure – release or transfer of PHI, providing access to or divulging PHI in any other manner outside the entity holding the information.

Covered Entities:

The law applies directly to three groups referred to as “covered entities”.

1. Health Care Providers
2. Health Plans
3. Health Care Clearinghouses

Health Care Providers: Any provider of medical or other health services, or supplies, who transmits any health information in electronic form in connection with a transaction for which standard requirements have been adopted.

Health Plans: Any individual or group plan that provides or pays the cost of health care.

Health Care Clearinghouses: A public or private entity that transforms health care transactions from one format to another.

Notice of Privacy Practices (NPP)

Written notice provided to all patients:

1. Describes patient rights
2. Details PHI uses and disclosures
3. States how PHI is maintained

Posted in prominent locations

Protected Health Information (PHI)

Health information is any information whether oral, written or electronic, regarding a patient.

Information can be related to past, present, or future physical or mental health conditions.

Examples of PHI

- Names
- Address (home, work, email, etc.)
- Dates (birth, death, admission, discharge)
- Numbers (social security #, medical record #, phone #, health plan #, etc.)
- Any other unique identifying number, characteristics, or code.

Confidentiality means keeping all privileged information private.

This includes information pertaining to a patient's:

- A. Diagnosis
- B. Medical history
- C. Lifestyle

While at work, discussion of patient records should not be discussed in elevators, gift shop, cafeteria, hallways, and/or parking lots.

In all states, certain patient information is exempt by law and reports to proper authorities are required without patient consent: (Mandated Reporting)

- Births and deaths (filed with state registrar)
- Emergencies
- Injuries caused by violence
- Threats of serious bodily harm to another that may reasonably be believed
- Murder
- Child abuse (physical/sexual)
- Vehicular accidents involving drug/alcohol

A reportable communicable or sexually transmitted disease:

1. The list of reportable communicable diseases varies with state, but those most likely to mandate reporting by state statues are: tuberculosis, hepatitis, AIDS, rheumatic fever, typhoid fever, tetanus, meningococcal meningitis, diphtheria, anthrax, malaria, poliomyelitis, smallpox, brucellosis, leprosy, rubella, plague
2. Reportable sexually transmitted diseases generally include: gonorrhea, syphilis, chlamydia, genital warts.
3. Some states require non-communicable diseases reported in order to track incidence, (suspected) causes and treatments: cancer, congenital metabolic disorders, epilepsy.

Disclosure of medical information to insurance companies is made only with patient consent.

Pre-employment physicals do not signify a doctor-patient relationship (unless the physician renders treatment).

- The doctor may release medical information relevant to employer's decision to hire

- Physicians who perform autopsies or have access to autopsy reports should maintain confidentiality of HIV status except when state laws regarding disclosure to public health and at-risk third parties are appropriate.
- HIV Tests and related information are sensitive and legally protected information.

Health professionals should respect confidentiality when treating competent minors

- Allow minors to verbally consent to medical care
- Confidentiality of minors may be ethically breached when parents need to be informed of treatment or serious illness.

It must always be remembered that medical records are legal documents:

- All information must be factual
- Questionable information should be labeled as opinion or assumption
- Information that is not relevant to care of patient should not be recorded
- Erasures are not allowed:

  1. errors should be crossed out with single line so that mistake is still readable

  2. correct, legible information can be inserted, initialed, and dated

  3. explanation for correction may be included

Computers and Confidentiality

Computerized patient data has led to attempts by some firms to use the information for marketing purposes.

- Health professionals are offered incentives to participate.
- Participation violates confidentiality and ethical codes concerning gifts to health professionals from industry.
- Information Security includes protections for safeguarding data.
- Securing information on computers involves more than just protection of software

- Many different individuals who work in hospitals have access to patient's records and health care providers must create stringent safeguards to maintain computer confidentiality:
  - Limited personnel who have access to records
  - Use of codes to prevent access to certain information
  - Requirement of passwords to access specific information
  - Constant monitoring of computer use

Breach of confidentiality

- A breach is an unauthorized acquisition, access, use, or disclosure of unsecured PHI which compromises the privacy, security, or integrity of the PHI.
- PHI is unsecured if it is NOT encrypted or rendered unusable, unreadable, or indecipherable to unauthorized individuals.
- Breaches in confidentiality include loss of public confidence

HIPAA Rules

- When you use it
- When you disclose it
- When you store it
- When you see it on your computer
- when you share it with another provider
- When it is lying on your desk
- When you are talking about it in any public area
- When you are talking about it over the phone

Understanding Use and Disclosures:

Covered entities may use or disclose PHI for their own TPO

T – treatment

P – payment for health care

O – operations activities

Ways in which medical professionals can guard patient confidentiality:

- Health care professionals have both and ethical and legal obligation to protect personal identifiable information
- Never disclose information to a third party without signed consent (this includes insurance companies, attorneys, employers, curious neighbors)
- Do not decide confidentiality on the basis of personal approval of thoughts and actions of the patient.
- Never reveal financial information about a patient including account balance—this is confidential!

- When talking on the telephone to a patient, do not use the patient's name if others in the room might overhear.

- When leaving a message on a home answering machine or at a patient's place of employment, simply ask the patient to return a call. No mention should be made concerning results of medical tests. It is inadvisable to leave a message with a coworker or receptionist for the patient to call an oncologist, OB-GYN specialist, etc.

- Do not leave medical charts or insurance reports where patients or office visitors can see them.

When can PHI be discussed?

- Discussing PHI for treatment of a patient
- Discussing care with clinical instructor
- De-identified PHI during pre and post conferences
- De-identified PHI in class presentations, case studies, etc.

Incidental Use and Disclosure

Incidental Use and Disclosure covers communication needed to provide effective patient care such as:

- Dry Erase Boards at nurses stations
- Doctors conferring with patients' families
- Waiting room sign-in sheets
- Patient charts at bedside

Minimum Necessary

Access to confidential patient information is allowed if you follow the simple **"NEED TO KNOW"** rule:

1. If you need to see patient information to perform your job, access to this information is OK.
2. If you do not "need to know" confidential information to perform your job, you are NOT permitted to access it.
3. If you access confidential patient information, even your own or that of a family member, you can be subject to corrective action, including termination or dismissal from an educational program.

Common Exposures

- Printed or electronic information left in public view
- Patient charts left on counters
- PHI in regular trash
- Records accessed without a "need to know"
- Unauthorized individuals hearing sensitive patient information such as diagnosis or treatment
- Incorrect phone number when sending a fax
- Laptop or PDA unattended/lost/stolen
- Sending PHI outside of hospital/healthcare system without encryption
- Not signing off, sharing passwords

Hospital Directory Information

The patient has a choice on whether or not they want to be listed in the directory or not.

1. The patient's first name, last name is given then their location in facility and general condition (i.e. stable)can be given.

2. Transfer the call to location where the patient is in the facility.

3. Transfer the call to the patient's room

4. A patient can change their mind at any time.

"Opting Out" - also known as Not for Publication status

These patients will not receive mail, phone calls, flowers, or visitors as we cannot confirm or deny the patient is in the facility.

Safeguard All PHI

- Assure proper disposal of PHI by placing in secure containers for future shredding:

  Examples:

  - surgery schedules
  - daily patient census
- Always log off or lock the computer whenever leaving the workstation.
- Use a password protected screensaver as an additional safeguard.
- Lock office doors when you're going to be away from your workstation for long periods of time.

Safeguard Passwords

- Never share Login ID and/or password.
- You are responsible to any activity that occurs under your password
- Protect your computer access
- You are responsible for keeping your password secure.

Special Tips

- Protecting the PHI is the responsibility of everyone.
- Be sensitive to confidential information.
- Think before you talk about patient specific information.
- Keep information to yourself if you see or overhear PHI.
- Elevators, hallways, cafeterias, gift shops, or other common areas are not places to share PHI.

Social Networking

- Because social media sites, such as Facebook and Twitter, enable people to easily and instantly share information with friends, family and others around the world, we all must remember to protect patient information.

- Even the smallest amount of information that could possibly identify a patient may not be shared.

Cell Phone and Texting

- Cell phone use and privacy can represent a security and privacy risk:
  - Most cell phones have cameras and there's a privacy concern that pictures will be taken of patients or patient information.
- Text messaging is not secure and represents a security risk if the text message includes PHI.

Students:

- NO pictures or videos while in the health care setting.
- No audio recording are to be made in the health care setting.

Failure to Comply

- Civil and Criminal penalties
- Exclusion from participation in Medicare programs
- Damaged reputation
- Place accreditation at risk
- Lawsuit for breach of confidentiality

Penalties If You Do Not Comply

- Non-compliance is a civil offense that carries a penalty of $100 per person per violation and a maximum of $50,000 per year per incident.
- Unauthorized Disclosure or Misuse of Patient Information under false pretenses or with the intent to sell, transfer, or use for personal gain, or malicious harm is a criminal offense.
- Penalties for criminal offenses can be up to $250,000 in fines and up to 10 years in prison.

THE OFFICE OF CIVIL RIGHTS (OCR) within the Department of Health and Human Services (HHS) enforces the civil penalties.

THE DEPARTMENT OF JUSTICE is responsible for enforcing the criminal penalties.

Criminal Penalties

- For health plans, providers, clearinghouses, and business associates that:
  - Knowingly and improperly disclose information
  - Obtain information under false pretenses
- Penalties can apply to any "person"
- Penalties are higher for actions designed to generate monetary gain.

Individual Consequences

Individual committing HIPAA violations can:

1. Lose opportunities to participated in education programs
2. Lose professional licenses
3. Be subject to criminal conviction
4. Be subject to civil suit
5. Be fired from their job

Who to Call?

- Each health care facility that is covered by the Privacy Rule will have a HIPAA Privacy Officer.
- Specific contact information is not provided for all health care agencies.
- Students should contact their instructor or the Privacy Officer for questions related to HIPAA.

- HIPAA protects health insurance coverage, improve access to care.
- Ensures the privacy of healthcare information.
- Restricts the use and disclosure of healthcare information.

HIPAA violations can ruin careers