HIPAA Awareness For Medical Facilities

Presented by:

Cathy Montgomery, RN

EXCELLENTIA ADVISORY GROUP

What is HIPAA?

HIPAA, which stands for the American Health Insurance Portability and Accountability Act of 1996, is a set of rules to be followed by doctors, hospitals, and other health care providers.

The 5 Rules of HIPAA(1996)

1. Privacy Rule (4/03)
2. Security Rule (4/03)
3. Transaction Rule (10/03)
4. Identifiers Rule (5/07)
5. Enforcement Rule (3/06)

ARRA

- American Recovery and Reinvestment Act of 2009
- Updated to include HITECH Act
- Requires HHS to audit providers and their business associates' compliance with HIPAA

HIPAA Omnibus Rule

More news!
"Omnibus"
affects The HITECH Act as well as the Security Rule

HIPAA General Rules

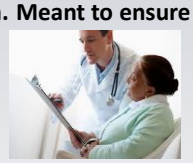
- Elect a Privacy Officer
- Have written Policies & Procedures
- Business Associates must sign agreements
- Employee training
- Patients receive written privacy notices
- Design a complaint system
- Evaluate your organization's risk

Privacy Rule

- The Privacy Rule establishes national standards to protect individuals' medical records and other personal health information. The Privacy Rule applies to health plans, health care clearinghouses, and health care providers that conduct health care transactions electronically.

Privacy Rule

- The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. Meant to ensure TRUST.



Privacy Rule

"individually identifiable health information"

PHI or ePHI

- *Any form* (electronic, paper, or oral)
- Past, present, or future (includes genetic info)
- Physical, mental, payment

*Identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual!!!

Examples of Individually Identifiable Information

- Names
- Geographic locations smaller than a state
- Birth date (except for a year)
- Telephone or fax number
- Email address
- Biometric identifiers
- Social security number
- Medical record # or account #
- Photographs
- License number/VINs
- URLs/IP address
- Health plan beneficiary number

Privacy Rule

- Makes sure that the right information is flowing to the right people at the right time.
- The Privacy Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

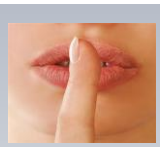
Privacy Rule Action Plans

- Minimum Necessary – only share as much as necessary to get the job done

*Does not apply to disclosures of PHI to other healthcare providers for treatment

- De-identify info when possible

Privacy Rule Action Plans



- Keep conversations private
- If you happen to see a patient in any public place, be very careful in greeting them. They may not want others to know they have been a patient
- Being sure you are in a private area when listening to or reading your messages

Ways to Protect Privacy

- Not leaving information on answering machines or emails because you don't know who can get your messages. Knowing who you are speaking to on the phone. If not sure get a name and number to call back after you find out it is OK to do so. Leaving only your name and your number on message machines when you are asking patients to call you back.

Ways to Protect Privacy

When calling patients in waiting rooms for appointments or talking to them in our healthcare facilities, talk to them in a way that does not disclose their full name, doctor, or reason for their visit to others who may overhear.

Ways to Protect Privacy

- Being sure no one can see your computer screen while you are working.
- Never sharing your access code.
- Logging off when not working on your computer.
- Changing your code and notifying your supervisor if your code becomes known by anyone else.

Ways to Protect Privacy

Even when a patient has someone with them, they may not want that person to hear their private information, so ask the person to wait outside. If the patient requests them to stay, that is OK.

Ways to Protect Privacy

Do not post patients' names and diagnosis or doctor's name and private information in any public areas such as waiting rooms, nursing stations, or assignment boards.

Ways to Protect Privacy

Never leave documents unattended.

- **Store, file, shred, or destroy according to your departmental policy.**
- **Make sure fax numbers are correct and use a cover sheet with a confidentiality statement.**

Privacy Rule Action Plans

Privacy Notices

- **Provide at initial visit**
- **Available upon request**
- **Post in general areas**
- **Explain how the CE may use and disclose PHI**
- **Explain how to file a complaint**
- **Go through individual rights**

Privacy Rule Physical Security

- **Lock offices and file cabinets**
- **Screen PHI from public view**
- **Attention to detail if charts are mobile**

Privacy Rule
Technical Security

- Don't share passwords
- Log off
- Encrypt data
- Inventory laptops
- Cell phones and other personal devices
- Thumb drives
- Special considerations for disposal of items

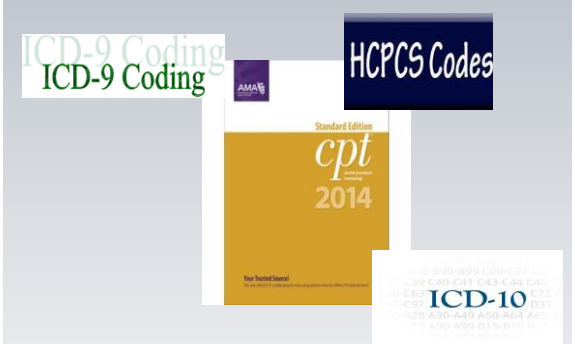
Security Rule

Also addresses the privacy protection of electronic protected health information.

3 aspects of security:

1. Administrative Safeguards
2. Physical Safeguards
3. Technical Safeguards

Transaction Rule



Identifiers Rule

Three Unique Identifiers

- Employer Identifier (EIN #)
- Provider Identifier (NPI#)
- National Health Plan Identifier (NHI#)

Enforcement Rule (ARRA HITECH ACT)

5 Areas of Concern

1. Covered entities and business associates now treated equally
2. Mandatory reporting
3. Restrictions on sales and marketing
4. Criminal and civil penalties
5. Business Associate Contract requirements

Protected Health Information

Personal information cannot be released to individuals or companies interested in marketing ventures without the patient's written permission. For example:

- Names of patients on antihypertensive drugs cannot be released to a company marketing nutritional products to lower blood pressure.
- Names and addresses of pregnant women cannot be provided to infant formula companies.
- Contact information of previous patients cannot be used to raise money for a hospital building campaign.

HIPAA Criminal Penalties

Types of Violations

1. Did not know
2. Reasonable cause
3. Willful neglect - corrected
4. Willful neglect - uncorrected

Sources of Breaches

1. Misplaced or stolen laptop computers
2. Improper disposal of PHI
3. Careless handling of paper records
4. Release of unencrypted PHI
5. Unauthorized access to PHI
6. Hacking

Data Security

1. Encryption
   - Hard Drives must be NIST-certified and use AES hardware encryption with two-key access to read/write data on the hard drive.
2. Destruction (hard drives)
   - First degaussed, then destroyed.
3. Destruction (paper)
   - High Security shredder

Breaches Affecting 500 or More Individuals

- As required by section 13402(e)(4) of the HITECH Act, the Secretary of HHS must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches.

Consequences of Data Breach

- Fines and penalties for violating federal laws (HIPAA/HITECH) and state laws

- Reputational harm
- Costs to respond and defend
- Contract obligations
- Government investigation
- Private lawsuits

Basic HITECH Notice Rules

- Must provide notice of breach of unsecured PHI to affected individuals, HHS, and in some cases, media. (PHI is secured only if it has been destroyed or encrypted.)
- "Breach" is:
  - The acquisition, use, or disclosure of PHI in a manner not allowed by HIPAA and
  - That poses a significant risk of financial, reputational, or other harm to the affected individual.

What is "Significant"

- Who impermissibly used PHI, or to whom was it disclosed?
- What steps were taken to eliminate or minimize the risk of harm to the affected person?
- Was the PHI returned without being accessed?
- What was the nature, type, and amount of PHI disclosed?

Notice Must Be Given to Affected Individuals

- Without unreasonable delay, but never more than 60 days after learning of the breach.
- In writing by mail or, if the individual has agreed, by email.

Substitute Notice

- What if provider has incomplete or out-of-date contact information for affected individuals?
  - For 10 or more individuals, provider can post notice on its website or publish in major print or broadcast media where the affected individuals likely reside.
  - For fewer than 10 individuals, provider can give notice by alternative form of written, telephone, or other means.

Contents of Notice

- Description of the breach (what happened)
- Type(s) of information disclosed
- Steps effected individuals should take to protect themselves from potential harm
- What the provider is doing to investigate the breach, mitigate the harm, and prevent further breaches
- Contact information for the provider (including a toll-free number if substitute notice is provided on a website or by media)

Notice to HHS

- Submit electronically through HHS website
- If breach affects 500 or more individuals, notify HHS secretary without unreasonable delay and no later than 60 days after breach
- Otherwise, notify HHS no later than 60 days after the end of the calendar year in which the breach occurred
- Expect an investigation

Notice to Media

- For breach affecting more than 500 residents of a state, provider must give notice to prominent media outlets serving that state
- Notice must be provided without unreasonable delay and no later than 60 days following discovery of the breach
- Must include the same information required for the notice to individuals

Notice by Business Associate

- Business associates must notify provider if breach occurs
- Notice must be given without unreasonable delay and no more than 60 days after discovery
- Notice must include identification of each individual affected and any information provider needs to include in its notice to individuals

State Laws

- 46 states have enacted data security laws: http://www.ncsl.org/default.aspx?tabid=13489
- Requirements vary by state, but many include PHI, employee data, and consumer data
- Notice required to affected state residents, state attorney general, and consumer agencies
- Challenge: Multi-state breach

Prevention Strategies

- Develop HIPAA/HITECH privacy and security compliance program
- Educate your staff about privacy requirements and practices
  - Establish rules for and monitor access to PHI
  - Impose penalties for improper access to PHI
  - Periodic refresher training

Prevention Strategies - 2

- Minimize use of unsecured PHI
  - Encrypt all electronic PHI
  - Shred paper, film, or other hard copy media
- Negotiate strong contracts with business associates
  - Time to notify provider of breach
  - Duty to investigate breach
  - Business associate responsible for costs related to breach notification
  - Indemnification

If a Breach Occurs

- Act promptly to:
  - Determine if a breach occurred
  - Mitigate any harm
  - Provide required notices
  - Cooperate with any government investigation

Definitions

- Protected Health Information (PHI) or Protected Medical Information (PMI): This is any data about the patient that would tend to identify the individual: name, hospital #, SSN, diagnosis, lab results, past or current photos, etc, etc.
- Privacy Officer (PO): Each facility will have an employee who is responsible for implementing and enforcing this law. Some may have one over a multi-facility network (Seton) others one at each site (St. David's Partnership). As a nursing student, this individual (after your instructor or preceptor) could be your point of information regarding HIPAA.
- Covered Entity (CE): This includes any health plan, healthcare provider, agency that processes claims, and any company that subcontracts with them are covered by this law.

Definitions

- Release/Disclosure: These are terms used in describing the release of PHI to other CEs for TPO, treatment, payment, or health care operations.
- Accounting of Disclosure (AOD): The patient has the right to have an AOD for his PHI or PMI.
- Directory: This is CE's census or list of patients used by volunteers and operators to direct visitors.
- Business Associate: Any person or entity that performs certain functions or activities that involves the use or disclosure of PHI on behalf of or provides services to a covered entity. A member of a covered entity's workforce is not a business associate.

Excellentia HIPAA Services

✓On Site Risk Assessments

✓HIPAA Corrective Action Plans

✓Virtual Assistance for Policies & Procedures

QUESTIONS?

Excellentia Advisory Group
cathy@excellentiagroup.com
636-875-5088 ext. 105

Like us on Facebook
http://www.facebook.com/#!/pages/Excellentia-Advisory-Group/132294686823771

twitter Follow Us on Twitter
http://twitter.com/#!/excellentiagrp