HIPAA Privacy and Security Training

By: Charo Jumaoas
SJGH Nursing Deputy Director,
Standards and Compliance Department
Privacy & Security Officer

What is HIPAA?

- Health Insurance Portability and Accountability Act
- Federal Regulation to add protection to health information
- Applicable to all States
- Applicable to healthcare organizations (hospitals, doctors' offices, pharmacies, public health, mental health, substance abuse)

Definitions

- PHI – Protected Health Information
- Use – how we use PHI to care for patient internally
- Disclosure – release of PHI outside of organization (covered entity)
- TPO – Treatment – Payment – healthcare Operations

HIPAA & Patient Rights

- Right to access and to obtain a copy of their health information
- Right to see a list of places where information has been sent
- Right to ask to have medical information changed if it is wrong
- Right to ask to have disclosure of information limited

HIPAA & Patient Rights

- Right to ask for alternatives for communication – cell phone, mail
- Right to file a complaint if patient/client feels than an employee has violated privacy rights
- Employees may file a complaint if they feel that a co-worker has violated a patient's rights, without fear of retaliation

The Privacy Rule

- Protects the right of the patient to control the disclosure of personal information
- Enforces the protection of PHI in all formats
- Requires organizations to develop specific policies and procedures

The Privacy Rule

- Requires organizations to train employees
- Sets the standards for who can access PHI
- Requires organizations to implement safeguards to ensure the protection of PHI

The Security Rule

- The means to control access and protect information from disclosure to unauthorized persons and from unauthorized alteration, destruction, or loss
- The physical protection the organization employs to protect information

The Security Rule

- Ensure the physical protection of PHI in electronic format
- Requires organizations to develop specific policies and procedures
- Requires organizations to train employees
- Sets the standards ensuring that only those authorized have access to PHI
- Requires organizations to implement safeguards to ensure the protection of pHI

Safeguards

- Administrative – Policies and procedures, workforce conduct, security controls, assignment of responsibility, training
- Physical – Locks, Sign-in sheets, restricting access to PHI, off-site computer back-up
- Technical – Encryption and decryption, Integrity of ePHI, Authentication of person signing into the computer, Audit controls, Transmission security, firewalls, etc.

Policies and Procedures

- Safeguards
- Confidentiality of PHI
- Patient rights
- Use & disclosures
- Privacy complaint
- Sanctions
- Mitigation
- Minimum necessary
- Workforce training
- Privacy officer's responsibilities
- Verification of identity
- Access controls
- Documentation requirements
- Workstation Use
- Device and media controls
- Integrity
- Authentication
- Automatic logoffs
- Fax transmission
- Notice of privacy practices

Data Elements of PHI

- Name
- Address
- Phone / fax
- Dates
  - Birth
  - Death
  - Admission
  - Discharge
- Social Security #
- Email addresses/URL
- Account #s
- Device identifiers
- Any unique identifying #, code, or characteristic

Violations at SJGH

- Report of violation received
- Reviewed to determine if actual violation occurred
- Logged and investigation begins
  - Interviews
  - Documentation gathering
  - Level of breach determined

Levels of Breach

- Level I – unintentional, acting in good faith.
- Level II – intentional, knowingly or willfully (Curiosity or Concern)
- Level III – intentional, knowingly or willfully. (Malicious Intent, Financial Gain, Entertainment)

Level I

- Cause or motivation
  - Lack of training
  - Inexperience
  - Unintentional
  - Accidental
  - No harm, no foul
- Examples:
  - Left PHI on copier
  - Email address error
  - Patient with similar name
  - Conversation overheard
  - Computer left unattended
  - Documents not put in shredder
  - Desk left unsecured

Level II

- Cause or motivation
  - Curiosity
  - Concern
  - Carelessness
  - Compassion
- Examples:
  - Checking on a patient
  - Copying information as a favor
  - Accessing test results
  - Experimenting with the computer
  - Installing software
  - Using someone else's password
  - Deleting information from the network

Level III

- Cause or motivation
  - Malicious intent
  - Financial gain
  - Entertainment
- Examples:
  - Selling patient addresses
  - E-broadcasting patient PHI
  - Intentionally altering information
  - Providing information to an attorney
  - Identity theft

Violations are happening more often than you think

- In 2021, 607 violations affecting nearly 45 million individuals were submitted to the OCR and are now visible on the Wall of Shame (a 20% increase in breaches compared to 2019, only two years prior)
- Breaches have increased 84% in the last 5 years, with 329 reported in 2016
- The average cost per record breached hit $499 in 2020 on an upward trend, totaling $13.2 billion for the year
- Unauthorized access/disclosure accounts for 34% of violations every year, up 162% over the past three years
- Hospitals typically account for 30% of all large data breaches

Facing the Consequences

- Most often, the OCR resolves cases through voluntary compliance or by accepting a covered entity's plan to address the breach and adjust policies and procedures to void future violations. For severe cases, the Enforcement Final Rule of 2006 allows the OCR to issue financial penalties to covered entities that fail to comply with HIPAA Rules. There are currently four main tiers of such violations.

Facing the Consequences

- Tier 1, $100 - $50,000 per breach: A violation that the covered entity was unaware of and could not have reasonably avoided.
- Tier 2, $1,000 - $50,000 per breach: A violation that the covered entity should have been aware of but could not have been avoided.
- Tier 3, $10,000 - $50,000 per breach: This violation is considered to be the result of willful neglect in instances where corrective measures were taken within a reasonable timeframe.
- Tier 4, $50,000 per breach: This violation is considered to be the result of willful neglect in instances where no corrective measures were taken to resolve the breach

AB 211, SB 541, HITECH

- Must report to the State (CDPH) when we discover unlawful or unauthorized disclosure of PHI within 5 business days
- State will investigate and will fine if safeguards are not adequate
- Fines can be up to $250,000 per occurrence
- Organizations and individuals can be fined
- HITECH is similar but on a Federal Level

Breach Activities

- Report to the State
- Federal Government reporting and activities
- Send a letter to each patient involved in the breach
- Send appropriate communication to recipient of PHI
- Ensure employee counseling/disciplining as appropriate

Reportable Breaches Here

- Form stickered with wrong pt's sticker
- PHI sent to wrong email – "SJGH secure" not in subject line
- PHI faxed to wrong place
- Phone with PHI lost
- Employee taking PHI home
- PHI left unsecured
- Electronic PHI sent unsecured

Your Role

- Report immediately to Privacy Officer, your supervisor, electronically
- Provide a detailed description of what was disclosed for the Privacy Officer's investigation
- The original PHI or a copy must be provided to the Privacy Officer
- Try to retrieve PHI or get an assurance that the recipient destroyed it
- Provide as many details as possible to help the investigation
- Don't fear the Privacy Officer!

What is Security Awareness?

- Recognizing what types of security issues and incidents may arise
- Knowing what to do in the event of a security breach

Risks

- Electronic – Phishing, Malicious Code, Viruses, Trojan Horse, Worms, Spyware, Adware, Peer to Peer Connections and Downloading content, Spam, Chain letters, hoaxes
- Social Engineering – Impersonation, Important User, Third-party authorization, Technical support

Recognize the Signs of Social Engineering

- Refuse to give contact information
- Rushing
- Name-dropping
- Intimidation
- Small mistakes
- Request confidential information
- Request you to do something improper

What can *you* do?

Ask Questions!

- Correct spelling of the person's name?
- Number where you can return the call?
- Contact information?
- Why the information is needed.
- Who authorized the request. Verify the authorization

- AND DO IT!!!

Passwords and Badges

We share offices, equipment and ideas, but…

Do not share your password or your badge with anyone, anytime!

Email and the Internet

- All email messages should be considered public.
- No PHI or any confidential information should be emailed outside of our local intranet.
- Your electronic footprint can be tracked.

Other Safety Measures

- Log off when not using your computer.
- Lock your workstation (Ctrl+Alt+Del and Lock).
- Automatic Screen Savers.
- Do not leave sensitive information on the copier or remote printers.
- Check your printer to ensure printing to the right one
- Confirm fax numbers before sending. Dial 9 for an outside line

Questions ?