HIPAA/HITECH Privacy Training

HCA Healthcare℠

Objectives

- Provide an overview of HIPAA and HITECH privacy key definitions and principles
- Describe how HIPAA and HITECH affect job duties
- Give tips and guidance for applying privacy requirements

Facility Privacy Official (FPO)

- Each facility has a designated FPO
- Every workforce member should be familiar with the facility's FPO
- This is the "go-to" person for:
  - Potential patient privacy issues
  - Questions on patient privacy matters
  - Patient privacy complaints

HIPAA Definition and Purpose

- What is HIPAA?
  - Health Insurance Portability and Accountability Act of 1996
  - Title II- Administrative Simplification
  - Federal Law

- What is the purpose of the law?
  - Guarantee privacy and security of health information
  - Protecting health insurance coverage, improving access to health care
  - Reducing fraud, abuse and health care costs

HITECH Definition and Purpose

- What is HITECH?
  - Health Information Technology for Economic and Clinical Health Act
  - Subtitle D of the American Recovery and Reinvestment Act of 2009 (ARRA)
  - Federal Law

- What is the purpose of the law?
  - Made massive changes to existing privacy and security laws
  - Creates a nationwide electronic health record
  - Increased penalties for privacy and security violations

HITECH Changes

- Examples of changes due to HITECH
  - Criminal provisions
  - Office of Civil Rights audits
  - Breach notification requirements
  - Changes to the patients' right to access

Breach Notification

- Certain breaches of protected health information resulting in risk that the information was compromised require notification to:
  - The patient
  - The Department of Health and Human Services
  - In some situations, the media

Civil Money Penalties for Non-Compliance

Violation Categories	Minimum penalty/violation	Maximum penalty/violation	Annual limit
No Knowledge	**$100**	**$50,000**	**$25,000**
Reasonable Cause	**$1,000**	**$50,000**	**$100,000**
Willful Neglect			
Corrected	$10,000	$50,000	$250,000
Not Corrected	$50,000	$50,000	$1,500,000

Criminal Penalties for Non-Compliance

- Applies to health plans, providers, clearinghouses and business associates that knowingly and improperly disclose information or obtain information under false pretenses.
- **Apply to any "person"**
  - Up to $50,000 and one year in prison for obtaining or disclosing protected health information (PHI)
  - Up to $100,000 and up to five years in prison for obtaining PHI under "false pretenses"
  - Up to $250,000 and up to 10 years in prison for obtaining or disclosing PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm

Protected Health Information (PHI)

- Name
- Address including street, county, zip code and equivalent geocodes
- Names of relatives
- Name of Employers
- All elements of dates except year (*e.g.,* DOB, admission /discharge, expiration, etc.)
- Telephone numbers
- Fax numbers
- Email addresses
- Social security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Any vehicle or other device serial number
- Web universal resource locator (URL)
- Internet protocol address (IP)
- Finger or voice prints
- Photographic images
- Any other unique identifying number, characteristic or code

Covered Entity

- An entity subject to HIPAA and HITECH
- Health plans, healthcare clearing houses, and healthcare providers that transmit electronically for billing
  - Hospitals
  - Physician Practices
  - Insurance Companies
  - Home Health Agencies
  - Hospice

Business Associate (BA)

- A person, company, corporation, or any other legal entity that creates, receives, maintains or transmits PHI to perform a function or activity on behalf of the facility or to perform certain professional services for the facility
  - Billing
  - Legal
  - Quality Assurance
  - Claims Processing

- Services covered by a Business Associate Agreement (BAA)

Affiliated Covered Entity (ACE)

- Legally separate affiliated CEs designated as a single CE for HIPAA purposes
- Typically facilities within the same Meditech market or division

Organized health Care Arrangement (OHCA)

- Clinically integrated care setting in which individuals typically receive healthcare from more than one healthcare provider
- Most commonly found in the hospital setting

Designated Record Set (DRS)

- Group of records maintained by or for facility
  - Medical and billing records
  - Information, in whole or in part, used by facility to make healthcare decisions about the individual

Minimum Necessary

- Only workforce members with a legitimate “need to know” may access, use or disclose PHI
  - Regardless of the extent of the access provided
- Only the minimum amount of PHI necessary may be used to accomplish the intended purpose of the access, use or disclosure
- Workforce members may not access his/her own record
  - Contact HIM/medical records to request

Notice of Privacy Practices (NOPP)

- Patients' privacy rights are outlined in the NOPP
  - Breach Notification
  - Right to Access
  - Right to Amend
  - Confidential Communication
  - Right to Restrict
  - Right to Opt Out of the Directory
  - Right to Request an Accounting of Disclosure
  - Fundraising and the Right to Opt Out
- Patient receives NOPP at each registration

Right to Access

- Patient (or legal representative) may inspect and/or obtain a copy of PHI contained in the DRS
- Some limited exceptions
  - Psychotherapy notes, and information compiled for use in civil/criminal/administrative actions
- Direct patients to your facility's designated department (e.g., HIM)
- Individuals have the right to obtain information in an electronic format
- Individuals (except medical staff physicians) may not access their own record in any system

Right to Amend

- Patients have the right to request an amendment to records in the DRS
- Request must be made in writing to the FPO
- Cannot change or omit documentation already in the medical record

Confidential Communications

- Patients have the right to request to be contacted at alternate locations or by alternate means
- All reasonable requests must be accommodated
- A form must be completed by the patient or patient's legal representative

Right to Restrict

- Patients have the right to request restrictions of uses and disclosures of PHI
- The request must be made in writing to the FPO or the FPO's designee
- Do not agree to any request – refer the individual to the FPO

Opt Out of the Directory

- Patients have the right to opt out of the facility directory
- Cannot acknowledge the patient is in the hospital or the condition of the patient except for treatment, payment or health care operations purposes
  - Clergy will not have access
  - No floral or other deliveries
- In the hospital setting, the confidential flag is set in Meditech

Accounting of Disclosures (AOD)

- Patients have the right to request a written accounting of disclosures of PHI to authorized individuals a facility has made during the six years prior to the date the report is requested

- Every facility must have a process in place to log AOD entries (e.g., MEDITECH MRI Correspondence Module, spreadsheet)

Patient Privacy Complaints

- Route all patient privacy complaints to the FPO
- FPO must acknowledge the complaint
- Complaint log maintained by the FPO in accordance with the facility's policy
- No retaliatory actions can be made
- Disposition of the complaint must be consistent with the facility's sanctions policy

HIPAA Authorizations

- Form signed by the patient or patient's personal representative authorizing the release of PHI to a third party or individual
  - Not required for treatment, payment, or health care operations disclosures (unless otherwise required by State law)

- Certain required elements in order to be "HIPAA Compliant"
  - Always use the facility's form, when possible

Sanctions

- Every facility must have a sanctions policy to address privacy and information security violations
- Workforce members may be sanctioned (e.g., written warning, termination) for privacy and security violations
- Contact your FPO for a copy of your facility's policy

Uses and Disclosures Required by law

- PHI may be disclosed about an individual the facility believes to be a victim of abuse, neglect, or domestic violence to a government authority authorized by law to receive it
- PHI may be disclosed in the course of any judicial or administrative proceeding
- PHI may be disclosed to law enforcement in certain scenarios:
  - If required by law, including reporting certain types of wounds or injuries
  - In response to law enforcement official's request for PHI for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person; or if the individual is, or is suspected to be, a victim of a crime
  - To alert law enforcement of death resulting from criminal conduct
  - If the facility believes in good faith that a crime has occurred on the premises

Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is Not Required

- Disclosures for Public Health Activities
- Certain Disclosures of Immunizations
- Health Oversight Activities
- Certain Disclosures about Decedents
- Disclosures to avert a Serious Threat to Health or Safety
- Disclosures for Specialized Government Functions
- Disclosures for Workers' Compensation

Uses and Disclosures to Other Covered Entities

PHI may be disclosed to other covered entities without the patient's HIPAA complaint authorization

- For treatment activities of a health care provider
- For the payment activities of the entity that receives the PHI
- For limited health care operations activities, if each entity either has or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship
  - For limited health care operations
  - For the purpose of health care fraud and abuse detection or compliance
- To other members of the OHCA for health care operations

Uses & Disclosures of PHI for Involvement in the Patient's Care and Notification Purposes

- To notify a family member, personal representative, or another person responsible for the care of the patient of the patient’s location, general condition, or death
- To an entity authorized to assist in disaster relief efforts, for the purposes of coordinating the permitted uses and disclosures
  - Patient agreed
  - Patient was provided opportunity to object and did not
  - Inferred based on professional judgement that patient did not object
- Relevant PHI may be disclosed to any person to whom the patient has given his or her passcode

Verification of External Requestors

- Must verify the identity of any person or entity that is unknown to the workforce member and is requesting PHI
- Exceptions
  - Facility directory
  - Disaster relief purposes
  - Disclosures for the involvement in the individual's care and notification purposes

Incidental Use and Disclosures

- Disclosure that cannot be reasonably prevented, limited in nature, and occurs as a by-product of a permitted use or disclosure of PHI
- Must have appropriate safeguards in place
- Examples:
  - Discussions overheard at the nurses' station
  - Physician speaking with a patient in a semi-private room
  - Telephone conversation overheard at the registration desk

Safeguarding Oral PHI

- Do not discuss PHI in public areas or with anyone without a need to know – even if you don’t use the patient’s name
- Use lowered voices or step away from others
- Verify recipients of PHI prior to disclosure
- Ask permission to speak in front of visitors
- Only leave messages containing PHI on answering machines in accordance with facility policy

Safeguarding Paper PHI

- Properly dispose of PHI (e.g., shredding bin)
- Do not leave PHI in public view
  - Example: Charts left unattended on the counter of the nursing station
- Secure PHI after hours
- Verify recipients of PHI prior to disclosure
  - Example: Hand discharge paperwork belonging to another patient to the wrong patient
- Never remove PHI from the facility unless relevant to your job function and approved in advance by your manager

Safeguarding Electronic PHI

- Log off work stations when not in use and never share passwords
- Use screen savers/privacy screens
- Position screens out of the general public view
- Adhere to all Information Security Policies and Standards

Safeguarding Faxed PHI

- Use fax cover sheets
- Use pre-programmed fax numbers when applicable
  - Have a standard process for periodically reviewing programmed numbers for changes
  - Test programmed numbers prior to initial use
- Double-check fax numbers prior to hitting “send”
- Verify intended recipient got the fax

Key Takeaways

- Protecting PHI is required by law
- Safeguarding PHI is everyone's responsibility
- HIPAA gives patients privacy rights
- Work with your FPO for patient privacy questions, complaints and concerns
- PHI may only be accessed by those with a legitimate need to know

Next Steps

- Your FPO and/or management team will provide you with job-specific and facility-specific patient privacy training as applicable to your specific role and job function

Resources

- Patient Privacy Atlas Site (Keyword: HIPAA)
- IPS@HCAHealthcare.com
- HCA FPO Listing on Atlas