HIPAA Compliance

Tools for HIPAA Compliance

A guide for implementing HIPAA compliance, as amended by ARRA/HITECH

Objectives

- Understand HIPAA Compliance Process and its requirements
  - Privacy Rule
  - Security Rule
- Learn about available resources to help you with HIPAA compliance

HIPAA Compliance

Covered Entity vs. Business Associate

- Covered Entity (CE)
  - Health Care Provider who transmits health information in an electronic form
  - Health Care Plan or
  - Health Care Clearinghouse
- Business Associate (BA)
  - An entity which receives PHI from a CE and performs a function on behalf of the CE, but is not part of the CE's workforce
  - Examples: vendor for HCPF's claims management system, provider's billing company, hospital's vendor for patient satisfaction survey

HIPAA Compliance

Covered Entity vs. Business Associate

- Covered Entities need to be in compliance with all of HIPAA
- Business Associates of a Covered Entity need to be in compliance with
  - Signed Business Associate Agreement
  - ARRA/HITECH provisions
    - You must report actual or suspected breaches to the Covered Entity
  - HIPAA's Security Rule

HIPAA Compliance

Business Associates' Requirements

- Understand what HIPAA is designed to do
- Train workforce members in HIPAA
- Use & Disclose PHI only as per the Agreement and per federal law
- Put in place SAFEGUARDS for the PHI you touch
- Report improper uses/disclosures to the CE (breaches)
- Assist CE in complying with Rights of Clients when necessary
- Allow the federal government to see your information when they are auditing the CE or you

PHI Review

- Protected Health Information (PHI)
  - Refers to *individually identifiable* health information maintained by a covered entity
  - Relates to the past, present, or future health condition, treatment, or payment of a client
  - Identifies the individual, or could be used to identify the individual
  - Can be transmitted or maintained in any form or medium
  - Is almost anything about a client!

HIPAA Compliance

HIPAA Review

- Enables clients to exercise rights regarding their health information
- Establishes how PHI may be used and/or disclosed by CEs and their BAs

- Sets <u>minimum amount of information necessary</u> to satisfy a request for PHI

HIPAA Compliance

HIPAA Compliance Process

- Identify where the PHI exists in your organization
- Do a security risk assessment
- Write policies and procedures to safeguard PHI
- Train your employees, volunteers, etc. on HIPAA, security awareness (i.e. viruses, etc.) and your policies and procedures
- Document everything

PRIVACY POLICIES

HIPAA Compliance

Privacy Rule Standards

- Standards outline basic requirements that must be covered to comply with Privacy Rule
  - How PHI will be used and disclosed in general
  - How PHI will be used and disclosed to carry out treatment, payment or health care operations (TPO)
  - When an authorization is required to use and disclose PHI
  - What opportunities the client has to agree or disagree with how their PHI is used or disclosed
  - Other requirements relating to uses and disclosures of PHI

HIPAA Compliance

Privacy Rule Standards

- Notice of Privacy Practices for PHI
- Patients' Rights
  - Request privacy protection for PHI
  - Access of individuals to PHI
  - Amendment of PHI
  - Accounting of disclosures of PHI
- Administrative requirements
  - Personnel designations, training, safeguards, sanctions, mitigation, refraining from intimidating or retaliatory acts, policies and procedures, documentation, group health plans

HIPAA Compliance

Suggested Privacy Policies

- Identifying PHI
- Verification of Client Identity
- Personal Representatives
- Notice of Privacy Practices
- General Safeguards
- Privacy/Security Officer(s)
- Documentation of Policies & Procedures
- Training
- Sanctions
- Non-Retaliation
- Incidents/Breaches
- Mitigation

HIPAA Compliance

Suggested Privacy Policies

- Uses and Disclosures
  - Minimum Necessary
  - Use and Disclosure of PHI for Treatment, Payment or Health Care Operations
  - Use and Disclosure of PHI – No Authorization Required
  - Use and Disclosure of PHI – Authorization Required
  - Disclosure of PHI for Research
  - Disclosure of PHI for Marketing
  - Business Associates
- Incidents/Breaches
  - Incident Response Reporting by employees
  - Potential Breach/Breach Response Plan

HIPAA Compliance

Notice of Privacy Practices

- Privacy policy that is communicated to your clients
- Informs clients what the CE/BA can do with client PHI
- Informs clients what CE/BA cannot do with client PHI
- If you don't have one, you're most likely working under some other entity's Notice

HIPAA Compliance

Rights of Clients Policies for Covered Entities

- Rights of Clients
  - Right to Access PHI
    - In electronic form if PHI exists currently in electronic form
  - Right to Request Amendment of PHI
  - Right to Request Privacy Protection for PHI
    - New requirement to restrict disclosures to health plan for payment or health care operations purposes if client pays for item/service in full at time of service

HIPAA Compliance

Rights of Clients Policies for Covered Entities, cont.

- A List of all Disclosures of a Patient's PHI
  - Referred to as an "Accounting"
  - Currently not for TPO (treatment, payment & operations)
  - **Coming soon** – will include TPO if you have an electronic health record

- Right to Submit a Complaint
  - Complain to covered entity
  - Complain to federal government (Office of Civil Rights)

HIPAA Compliance

Suggested Privacy Forms

- Fax Cover Sheet
- Exercising Patient Rights (CE only)
- Designation of Personal Representative
- Authorization
- Notice of Privacy Practices (CE only)
- Business Associate Agreement

HIPAA Compliance

Example
General Safeguards Policy

- You may not sell PHI
  - (i.e. a list of all clients who have had hip replacements)
- If you contract with others who will have routine access to the PHI, you must
  - Enter into a Business Associate Agreement with your contractor
- Ensure client identity before giving out information over the phone by asking client to answer certain questions

HIPAA Compliance

Example Minimum Necessary Policy

- One of the most important HIPAA policies you can have!
- May be imbedded in another policy or policies
- Holds employees to only accessing, using or disclosing minimum amount of information necessary to do their job
- Example - firings in hospitals when VIP patient checks in and 12 hospital employees access the medical record even though they don't need to!
  - Octuplet mom (15 fired)
  - George Clooney (13 fired)
  - Brittney Spears (13 fired; 6 suspended)

HIPAA Compliance

Example Transmitting PHI Policy

- Paper PHI
  - Must always be <u>properly</u> shredded before discarding
  - Do not leave PHI in unattended or unsecured areas
  - Never put anything containing PHI in the trash!!

- Utilizing Fax to transmit PHI
  - Use approved cover sheet
  - Ensure correct fax number is entered before hitting send
  - Use pre-programmed fax address book whenever possible
  - Follow-up to ensure fax was received

Non-Retaliation Policy

- Policy is required under HIPAA
  - as well as under most federal laws
- Cannot retaliate in any way if
  - Client complains to you or Office of Civil Rights
  - Employee reports violation of HIPAA in good faith

HIPAA Compliance

Sanctions Policy

- Policy required under HIPAA
- Federal Health and Human Services noticed lack of enforcement under HIPAA
  - HITECH expects entities to sanction workforce members when they don't follow an organization's policies and procedures regarding HIPAA compliance
- Should be **flexible**, applied **equally**, and discussed in your HIPAA training

BREACHES AND MITIGATION

HIPAA Compliance

Breach/Data Breach Policy

- A breach is "unauthorized acquisition, access, use or disclosure of PHI…"
  - If you breach client data, you must notify
    - the individuals involved
    - the federal government, and
    - the media (breaches involving > 500 clients)

HIPAA Compliance

Breach/Data Breach Policy

- Policy – Breach Incident Response Plan
  - Who is involved in the investigation?
  - Who notifies the client? The feds? The media, if necessary?
  - Who is responsible for documenting all of this?

- Policy – Reporting of incidents/suspected breaches/actual breaches immediately to the Privacy Officer

HIPAA Compliance

Examples of Breaches

- Explanation of Medical Benefits (EOMB) sent to the incorrect client
- Unencrypted laptop containing client information is stolen from backseat of caseworker's car
- Real client information (instead of dummy information) used as part of training video available on the Internet
- Flash Drive (unencrypted) containing client PHI lost on public bus

Mitigation

- Covered entities have a responsibility to mitigate harmful effects due to uses or disclosures of protected health information
- Should be in your policies in multiple places
  - Breach Incident Response Policy
  - Training Policy
  - Incident Response Reporting (you can only mitigate what you know about)
  - Others?

HIPAA Compliance

Privacy Rule Resources

- Privacy Resources
  - HCPF website for forms, etc.
    - www.colorado.gov/cs/Satellite/HCPF/HCPF/1214386664393
  - CDHS website for sample policies
    - www.colorado.gov/cs/Satellite/CDHSOps/CBON/1251591540090
  - University of Miami Miller School of Medicine
    - privacy.med.miami.edu/glossary/index_hipaa.htm

SECURITY RULE COMPLIANCE

HIPAA Compliance

Security Rule Review

- Protects PHI in electronic form "ePHI"
  - Requires protecting the confidentiality, integrity, and availability of the information
- Requires safeguards to ensure PHI is protected from inappropriate access, modification, dissemination and destruction

Security Rule Standards

- Similar to Privacy Rule Standards
- 3 Categories:
  - Administrative
  - Physical
  - Technical

HIPAA Compliance

"Required" vs. "Addressable" Standards

- Required
  - Mandatory if you are a covered entity or business associate

- Addressable
  - *Is it a reasonable and appropriate safeguard for your environment?*

If yes, implement it

If no:

1. Document why it is not
2. <u>Implement an alternative safeguard</u>

Note: Cost cannot be used as a valid reason for not implementing a standard!

HIPAA Compliance

Requirements

- You should
  - Designate someone to be in charge of security for your organization
  - Perform a Risk Assessment (RA)
  - Secure systems containing ePHI based on results of your RA
  - Have policies & procedures in place to protect ePHI
  - Train employees
  - Document everything

HIPAA Compliance

Safeguards

Administrative

Physical

Technical

HIPAA Compliance

Administrative Safeguards

- Security Management Process
  - Risk Management
  - Risk Analysis
  - Sanctions
- Assigned Security Responsibility
  - Security Officer, security contact, etc.
- Workforce Security
- Information Access Management
- Security *Awareness* & Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts

Physical Safeguards

- Facility Access Controls
  - Contingency operations
  - Security plan
  - Access control & validation
- Workstation Use
- Workstation Security
- Device & Media Controls
  - Disposal of PHI
  - Media re-use
  - Accountability
  - Data backup and storage

Technical Safeguards

- Access Controls
- Audit Controls
  - You must maintain a log and keep an audit trail of activity for each system
- Integrity
- Person or Entity Authentication
- Transmission Security

HIPAA Compliance

Security Risk Assessment

- Look at your systems containing ePHI
  - Conduct an accurate assessment of potential risks and vulnerabilities to confidentiality, integrity and availability of ePHI held by the Covered Entity
- Fix what is broken or not protected enough
  - Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level

HIPAA Compliance

Security Risk Assessment

- Document It
  - Actions taken must be in written form (electronic counts)
- Review periodically to see if it is working

HIPAA Compliance

Examples of Security Policies

- Workstation use
  - Passwords
  - Screensaver time-outs
  - Access only to those who need it
  - Audits of system access
- Computer security
  - Firewalls
  - Anti-virus
  - Backups of data
- Facility security
  - Locks
  - Badges
  - Etc.
- Incident Response
  - Know what an incident or potential breach is
  - Report incidents ASAP
- Encryption
  - Laptops, Computers, Emails

Encryption of Email

- Encryption of PHI sent via email is not required by the Security Rule – but ***is expected by the federal government*** when enforcing the Security Rule?
  - As the cost of technology decreases and ease of its use/functionality increases, the "standard" in the industry becomes encryption
  - Technically, there is no other equivalent safeguard to encryption that you could implement – so you have to encrypt, or send by mail or fax

Security Resources

- Security Rule Series
  - Security 101 for Covered Entities, Safeguards, Policies and Procedures, etc.
  - www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf
- Risk Analysis Guidance
  - www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

NIST Guidance

- National Institutes for Standards and Technology (NIST) - www.nist.gov
  - Federal agency that sets computer security standards for the federal government and publishes reports on topics related to IT security
  - Mandatory for federal agencies; excellent guide for all other entities

NIST Guidance

- Most applicable:
  - 800-66: An Introductory Resource Guide for Implementing the HIPAA Security Rule
- Others:
  - NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems
  - NIST Special Publication 800-66: An Introductory Resource Guide for Implementing the HIPAA Security Rule
  - NIST Special Publication 800-88: Computer Security
  - NIST Special Publication 800-111: Guide to Storage Encryption Technologies for End User Devices

HIPAA Compliance

Remember

- The Privacy Rule is Good Business
- The Security Rule is designed to be flexible and scalable for organizations
- All of us are integral to protecting the privacy and security of clients' information

Questions?

Erika Bol

Privacy Officer

Department of Health Care Policy and Financing

303-866-2958

erika.bol@state.co.us