HIPAA and Electronic Information

Are you still acting like it's a paper world?

Rebecca Wahler, MS, CHPC, CHC

Compliance & Privacy Officer, NMHIC,

LCF Research, Albuquerque, NM

Overall Goal

- Develop basic understanding of the HIPAA and HITECH regulations related to electronic information
- Basic steps to be taken to improve compliance with the regulations

Credit Information

NMHIC and NM HITREC are programs administered by LCF Research, which is accredited by the New Mexico Medical Society to provide continuing education for physicians.

DISCLOSURE: The content of this lecture does not involve any ACCME-defined potential conflicts of interest. There is no commercial support for this educational activity. Everyone in a position to control the content of this lecture has disclosed all relevant financial relationships to LCF Research, and there are no relevant conflicts of interest to disclose.

Credit Information (continued)

- This activity may be acceptable for Nursing and Physicians Assistant CE credit if applicability to practice can be shown. Blank statements of credit are available to all attendees who complete a pre-test and post-test/ evaluation form.
- To obtain a certificate, **please complete the pre-test and post-test/evaluation form** and exchange it for your blank statement of credit when you leave.
- Personalized *AMA PRA Category 1 Credit*™ certificates will be e-mailed to physician (MD/DO) participants within 2-4 weeks to the address provided on your evaluation/ participation form.

Objectives

- Areas that will be reviewed include:
  - HIPAA, and HITECH Regulations quick review
  - Compliance Assessment
  - Security Risk Assessment
  - Remediation Tasks

HIPAA Regulations

HIPAA, HITECH and the Security Rule

45 CFR Part 160, 162 and 164

For more information refer to handout.

NM Confidentiality Laws

- NMSA 1978 §24-1-9.4; Sexually Transmitted diseases; confidentiality
- NMSA 1978 § 24-1-9.5; Sexually transmitted disease; disclosure statement
- NMSA 1978 § 24-1-9.7; penalty
- NMSA 1978 § 24-2B-6; HIV confidentiality
- NMSA 1978 §NMSA 24-2B-7; disclosure statement
- NMSA 1978 § 24-2B-9; penalty
- NMSA 1978 §24-2E-2 and 24-2E-3; viral hepatitis Recently repealed. http://www.nmlegis.gov/Sessions/13%20Regular/final/SB0310.pdf
- NMSA 1978 § 28-10A-1; HIV related test; limitation
- NMSA 1978 § 24-21-1; Genetic information privacy
- NMSA 1978 § 32A-6A-24; children's mental health and developmental disabilities privacy
- NMSA 1978 § 43-1-19; mental health and developmental disabilities
- 42 CFR Part 2; Substance Abuse treatment confidentiality of records

Compliance Assessment

45 CFR 164.308 (a)(8)

- *A covered entity must perform a technical and non-technical compliance assessment.*

A HIPAA compliance assessment and a security risk assessment are <u>not</u> the same thing.

Compliance Assessment Tools

A good tool for determining compliance with the regulations is the Audit Protocol at the Office of Civil Rights or at HIPAA Collaborative of Wisconsin (hipaacow.org).

- Both are great non-technical HIPAA compliance tools.
- Non-technical is looking for documentation and policies.

Security Risk Assessment

45 CFR 164.308 (a)(1)(i)

- *A Risk Analysis is a required task.*

- A Security Risk Assessment is a tool to help you determine the threats, vulnerabilities and likelihood of events to your electronic system.

Security Risk Assessment Tools

- The government has provided a Security Risk Assessment tool.
- A version can be found at hipaacow.org as well.
- Both can help determine threats, vulnerabilities, likelihood and impact

Remediation Steps

After completing the compliance and security assessment your office will find missing items and things that need to be improved or changed

Common Deficiencies

1. No risk assessment completed or done in years
2. No HIPAA polices or outdated policies
3. No evidence of annual HIPAA training of workforce
4. Missing Business Associate Agreements and Management of BAs
5. Monitoring audit logs and systems logs

Policies and Procedures

45 CFR 164.316 Policies and procedures and documentation requirements

- Policies and Procedures are required
- Must be able to show workforce has been trained on the policies

Policies and Procedures

- Policies explain the “why” and Procedures are the “how” you are doing something
- Policies don’t need to be super complex. Basic and easy to read information is best
- Plenty of HIPAA templates are available for a fee

Business Associate Regulations

HIPAA §164.308 (b) (1) Administrative safeguards

- A Business Associate (BA) is any entity that creates, receives, transmits or maintains your PHI
- Need a written BA Agreement (not the same thing as the service agreement)
- BAs should have a BAA in place with their subcontractors

What is a Business Associate?

- A Business Associate is an entity providing services to health care providers, health insurers and other HIPAA-covered entities
- Expanded definition includes any entity that “creates, receives, maintains, or transmits” PHI on behalf of a covered entity
- Business Associates of covered entities must follow the same regulations and face similar penalties for non-compliance

Business Associates

- Subcontractors are now included in the “must comply group” with HIPAA and Security Rule regulations
- BAs are required to complete Risk Assessments
- Directly liable for impermissible uses/disclosures of PHI

Government provided BAA template:

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Business Associate Contracts

- BAs are required to follow the minimum necessary requirement.
- Covered entities are required to get written assurance from their BA that all PHI will be appropriately safeguarded.
- Violations of the Privacy Rule mean potential civil and criminal penalties for the BA.
- BA are required to notify the covered entity of a breach of unsecured PHI.

Business Associate Management

- Must make an effort to show due diligence in selecting and managing your Business Associates
- The greater amount and depth of PHI the BAA has access to the more effort the medical provider should put forth in managing that vendor

Business Associate Management

Some suggestions:

1. Ask for a copy of their annual Risk Assessment or attestation.
2. Ask if they have a complete set of HIPAA policies and can prove workforce training on those policies.
3. Ask if they monitor audit logs and IT system logs.
4. Ask if they are using sub-contractors.
5. Ask how many people are accessing or working with your PHI.
6. Ask if any of the user accounts are shared or individual.

A good presentation from HRSA on what questions to ask your vendors is available.

Workforce Management

- Policy training
- HIPAA training
- Workforce/HR policies
- Access
- Audit logs
- IT System logs

Policy Training

- Documentation on workforce training on HIPAA policies
- Focus on certain policies:

  Breach prevention, unique user IDs, password management, minimum necessary, patient rights, audit logs, IT system activity review

HIPAA training

- Complete annual HIPAA training
- New employees should receive some training on HIPAA and your policies before access to systems that contain PHI is granted
- Document all training

Workforce & HR Policies

HIPAA §164.308 (a) (1) (ii) (C) Administrative safeguards.

Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

HIPAA §164.308 (a)(5) (i) Standard: Security awareness and training.

Implement a security awareness and training program for all members of its workforce (including management).

Workforce and HR Policies

- Job descriptions should outline what systems that employee has access to and what level of access
- Background checks
- Sanction Policy
- Documented training on HIPAA policies

Access, Modification, Deletion

HIPAA §164.308 (a) (3) Administrative safeguards

- Have policies defining appropriate workforce access to PHI
- Policies on how you authorize that access
- Policies on how you supervise workforce access
- Policies on how you determine the access is appropriate
- Policies on modifying or termination of access to PHI

Access, Modification, Deletion

HIPAA §164.308 (a) (4) Administrative safeguards

- Policy on information system access and management of those systems
- Policy and procedure on access authorization
- Policy on access establishment and modification

Workforce Access

HIPAA §164.312 (a)(1) Technical safeguards.

(a) (1) **Standard: Access control.** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

Access, Modification, Deletion

- Apply the role-based feature in your EHR
- Apply the “minimum necessary” rule when granting employee or contractor access to your EHR
- Control who sets up new computer accounts and/or modifies those accounts
- Remove access to the EHR systems when no longer needed

Audit Logs

HIPAA §164.312 (b) Technical safeguards.

(b) **Standard: Audit controls.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Audit Logs

- Turn on your auditing capabilities in all electronic health information systems, if possible (EHR, Practice Management, Billing and Coding Software, Scheduling Software)
- Review audit logs at a minimum of monthly or more frequently if needed
- Review user activity
- Spot check user access with patient scheduling
- Save the audit logs with any additional documentation pertaining to them (6 years)

IT System Logs

HIPAA §164.308 (a) (1) (ii) (D) Administrative safeguards.

Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

IT System Activity Review

- Regular review of IT System activity is important
- Document all reviews and any actions taken
- A good summary of what types of IT Security actions should be considered can be found on the HIPAA Education Resources sheet (#8).

IT Security Review

IT reports that are useful for further review:

- Patching and update reports on all Operating, Applications and Network Equipment
- Remote access user activity
- Review of user account creation, modification or deletion
- Authentication activity (failures)
- Password failures
- Anti-virus/malware patching
- Encryption management

Additional Resources

- http://www.hhs.gov/ocr/privacy/index.html
- http://www.ahima.org/
- http://www.himss.org/
- http://hipaacow.org/

Questions?

www.nmhic.org

(505) 938-9900