Understanding Your Data Privacy & Security Vulnerabilities with the Electronic Health Record (EHR)

NAHC Annual Meeting
November 1, 2013
4:15 PM – 5:45 PM

PRESENTERS:
JOAN L. USHER, BS, RHIA, COS-C, ACE
JLU Health Record Systems, Pembroke, MA
Cherrylyn Simmons, BSN, RN
Homefront Health Care, Providence, RI

LEARNING OBJECTIVES:

This program is designed to further the attendees knowledge of Electronic Health Record requirements. At the conclusion of this program, the participant will be able to:

• Examine the latest requirements for privacy & data security

• Identify what policies & trainings are needed to protect and support the EHR

• Examine EHR vulnerabilities & common documentation errors
HIPAA Mega Rule

- Rule was released January 17, 2013
- Effective date March 26, 2013
- Compliance date Sept 23, 2013
- Modifications to HITECH also called Omnibus Rule
- Enhances patient privacy protections & provides patients with new rights to access health records

HIPAA Privacy & Security

- Modifies HIPAA privacy & security rule to add strength to the rules & enforcement
- Modifies the Breach Notification Rule from risk of harm to presumption of reportable breach
- Makes Business Associates directly liable for compliance with HIPAA
What is PHI?

- Protected Health Information (“PHI”):
  - Individually identifiable health information
  - Transmitted or maintained in any form or medium
- Held or transmitted by Covered Entities or their Business Associates
- Not PHI
  - De-identified information
  - Employment records
    - However is covered by state law

What is the “Record” under HIPAA?

- Designated record set includes the following information regarding care decisions:
  - Medical records
  - Billing records
  - Claims information
Breach Notification Rule

Updated

• Presumption of reportable breach, unless low probability the PHI has been compromised after risk assessment
• Description of what compromised means
  – “inappropriately viewed, re-identified, re-disclosed, or otherwise misused”

Now is the time to dust off the HIPAA Manual
HIPAA Self Audits
Risk Assessments

• Privacy Audit 45 CFR §164.530
• Security Audit 45 CFR §164.308
  1. Administrative Safeguards
  2. Physical Safeguards
  3. Technical Safeguards
• Document any risks
• Develop a compliance action plan

Administrative Safeguards

• Risk analysis and management of e-PHI related to workforce security, employee access to electronic info systems, employee training & awareness, protocols for incidents and emergencies, and contractual relationships with business associates
Administrative Safeguards

• Does the agency maintain an inventory of all of its computer hardware and software?
• Has the agency identified all locations in which ePHI is stored?
• Do the agency's disciplinary policies include sanctions for security violations?
• Are ePHI access rights promptly terminated for workforce members that leave the agency or when access is no longer required to perform their jobs?
• Does the agency provide security training to its workforce members?

Administrative Safeguards

• Are security incidents formally reported to anyone in the agency?
• Does the agency currently have an emergency operations plan in place?
• Does the agency have a disaster recovery plan in place?
• Are security measures evaluated when there are changes in agency operations or systems?
• Does the agency have agreements in place with all business associates as a result of its Privacy Rule compliance efforts?
Physical Safeguards

• Implement policies and procedures to limit physical access to electronic information systems and the facility in which they are housed, while ensuring that proper authorized access is permitted.

Physical Safeguards

• Does the agency have procedures in place addressing access to offices in emergency situations?
• Does more than one tenant/organization occupy the building in which the office is located?
• Are all entrances to agency offices secured?
• Is an alarm system installed?
• If the agency's clinician's utilize point of care devices, how are remote workstations secured?
• During the last year, has the agency disposed of any equipment on which ePHI was stored?
Technical Safeguards

• Implementation of technical policies for electronic information systems that contain e-PHI to allow access only to those persons or software programs that have been granted access rights

Technical Safeguards

• Is ePHI retained in files on location?
• Does the agency utilize software that is remotely hosted?
• What approach, if any, does the agency utilize to control access to ePHI? Does the agency have procedures in place to facilitate emergency access to its information systems by repair personnel and others not normally requiring access?
• Are user sessions automatically terminated after a specified period of inactivity?
Technical Safeguards

- Does the agency encrypt any of the ePHI stored on its servers or office workstations?
- Does the agency regularly capture and review network activity data?
- Does the agency review audit trails on a regular basis?
- Does the agency employ intrusion detection technology?
- How does the agency validate the identity of system users?
- Does the agency exchange ePHI with any outside organizations electronically?

OIG: Corporate Compliance

- Focus of OIG for Work Plan & updated HIPAA Regulations
- Existence of an active corporate compliance plan
- Incorporation of compliance plans into their day-to-day operations and determine whether the plans contain elements identified in OIG’s compliance program guidance
Tips for Revisiting HIPAA

✓ Update your Privacy Program
✓ Retrain Workforce
✓ Perform Administrative, Physical & Technical Review for Security
  • Analyze areas of vulnerabilities and mitigate
✓ Review Corporate Compliance Program
✓ Review all policies related to HIPAA & CC
✓ Be serious about sanctions for violations
✓ Focus on compliance activities

Who Is a Business Associate (BA)?

• New definition of business associate
  – Creates, receives, maintains, or transmits protected health information
BA Agreements

- Need to include the following
  - HIPAA Compliance
  - Safeguards: physical, administrative, technical
  - Training: all employees
  - Notification of Breach
  - Indemnification
  - Subcontractor extensions

Liability of Business Associates

- Impermissible uses and disclosures
- Breach notification to covered entity
- Ability to provide e-copy of ePHI as specified in the business associate contract
- Ability to disclose PHI to HHS for HIPAA investigation
- Ability to provide an accounting of disclosures
- Failure to comply with the applicable requirements of the Security Rule
Business Associate Contracts

- Must specify compliance with Breach Notification Rule
- Should specify to whom BA provides electronic access
- If CE delegates HIPAA responsibility, must specify that BA will comply with HIPAA
- If on 1/25/13 a valid BAA is in place, parties have an extra year to comply
- Sample notice available

Changes to Notice of Privacy Practices

- Prohibition on sale of PHI
- Duty to notify affected individuals of a breach of unsecured PHI
- Right to opt out of fundraising (if applicable)
- Right to restrict disclosure of PHI when paid out of pocket
- Limit use of genetic information (certain health plans only)
- Deleted appointment reminders
Action Items

- Begin process of updating BA agreements
  - Consider who is BA
  - What safeguards does the BA have in place?
- Amend Notice of Privacy Practices
- Train staff
  - on HIPAA changes
  - What is a breach

Electronic Copy of PHI

- Form and format requested, if readily producible
  - If not readily producible and maintained in paper, then readable hard copy
  - May charge for labor and electronic media
Electronic Copy of PHI

• Individual may designate third party to receive copy
  – Must be in writing
  – Clearly identify the designated person
  – Clearly identify where to send the copy

Restriction for Out-of-Pocket Payments

• Covered entity must agree to individual’s request to restrict disclosure to health plan
  – For payment or health care operations
  – Unless required by law
  – Individual or person on individual’s behalf pays for item or service out of pocket in full
Increased Enforcement

- Willful neglect: Conscious, intentional failure or reckless indifference
- OCR will investigate all cases of possible willful neglect
- OCR will impose penalty on all violations due to willful neglect
- Greater OCR discretion to proceed directly to penalty without seeking information resolution

Action Items

- Policies:
  - Release of Information Policy
  - Notice of Privacy Practice
  - Device & Media Destruction
  - Reporting a Potential Breach of PHI
    - State & Federal Requirements
    - Procedure for investigating, steps taken
    - Risk Analysis
  - Information Access Management
  - Integrity of Electronic PHI
  - Protection against loss, tampering or unauthorized use
  - Laptop, Notebook, Other Equipment Use & Security
  - Workstation Use & Security
  - HIPAA Privacy & Security Policies
HIPAA Climate

- 77,190+ HIPAA Complaints
- 18,559+ Covered Entities Affected

New HIPAA Audits

- The first of 150 HIPAA audits began in December 2011
- OCR is randomly selecting organizations for the first HIPAA privacy and security audits mandated under the HITECH Act
- OCR’s focus is on auditing a variety of covered entities’ functions in the initial round, with Business Associates (BA) being included in future audits
- Another 130 organizations were be audited by the end of 2012
- The contract was awarded to KPMG, LLP
  http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
OCR Audit Findings

Privacy Issues
- Review process for denials of patient access to records
- Failure to provide appropriate patient access to records
- Policies & procedures
- Uses & Disclosures of decedent information
- Business associate contracts

Security Issues
- Conduct Risk Assessment
- Grant, modify user access
- Incident response
- Contingency planning
- Media reuse & destruction
- Encryption
- Use activity monitoring
- Authentication
- Physical access controls

BREACH
Common Data Breach Scenarios

• Unintended Breaches
  – Improper disposal
  – Lost laptops
• Employee/Ex-Employee
• Hackers & Thieves / Organized Crime
• Competitive Espionage

Top 5 Security Risks/Potential Breach

1. Portable Devices
2. Theft
3. Transfer and Disposal
4. System Security
5. Business Associates
## Security Risks

### Portable Devices
- Includes: Laptops, flash drives, smartphones
- Need encryption
- No BYOD

### Theft
- Know the steps to follow if Portable Media stolen
- Largest number of breaches

## Transfer & Disposal Risk

- South Shore Hospital, MA has agreed to pay $750,000 to resolve allegations that it failed to protect the personal and confidential health information of more than 800,000 consumers. In February 2010, South Shore Hospital shipped three boxes containing 473 unencrypted back-up computer tapes with 800,000 individuals’ personal information and protected health information off-site to be erased. The hospital contracted with Archive Data Solutions to erase the back-up tapes and resell them.
- The hospital did not inform Archive Data, however, that personal information and protected health information was on the back-up computer tapes nor did South Shore Hospital determine whether Archive Data had sufficient safeguards in place to protect this sensitive information.
In the News... Breach less than 500

- HHS announces first HIPAA breach settlement involving less than 500 patients - Hospice of North Idaho settles HIPAA security case for $50,000
- The HHS Office for Civil Rights (OCR) began an investigation after HONI reported to HHS that an unencrypted laptop computer containing the electronic protected health information (ePHI) of 441 patients had been stolen in June 2010.
- Over the course of the investigation, OCR discovered that HONI had not conducted a risk analysis to safeguard ePHI and did not have in place policies or procedures to address mobile device security as required by the HIPAA Security Rule.

Timeline for Breach

Idaho reported breach February 2011

January 2013 Fine $50K & Resolution Agreement

June 2012
OCR Began investigation
Breaches

- Reminder to submit breaches less than 500 to OCR by February 28, 2014 for calendar year 2013.
- A new educational initiative, *Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information*, has been launched by OCR and the HHS Office of the National Coordinator for Health Information Technology (ONC)
- Offers HC providers practical tips on ways to protect PHI when using mobile devices such as laptops, tablets, and smartphones. www.HealthIT.gov/mobiledevices

Breach Checklist for Covered Entities

1. Has there been an impermissible use or disclosure of PHI?
2. Perform risk assessment – determine and document whether the impermissible use or disclosure compromised the security or privacy of PHI and whether any financial, reputational, or other harm to the individual resulted
3. Determine if the incident falls under any of the exceptions to the definition of breach
4. Was the PHI unsecured?
Breach Risk Assessment Factors

1. Nature and extent of PHI involved
2. The unauthorized person who used the PHI or to whom the disclosure was made
3. Whether the PHI actually was acquired or viewed
4. The extent to which the risk to the PHI has been mitigated

Notification of Data Breach

- When an entity experiences a data breach it must give notice of the breach to the States Attorney General, Office of Civil Rights, affected consumers
- Notice required when:
  a) A breach of security; or
  b) PHI/Personal information compromised
- State Attorneys General authorized to bring civil lawsuits for HIPAA violations
Enforcement

• When a government agency learns of a breach it will examine several factors including:
  – Was Proper Notification Made?
  – Did the owner of the data make false or misleading representations concerning the security of data?
  – Was the data stored or maintained in a manner so that it was not reasonably protected and therefore susceptible to a breach?
  – Did the owner of the data have either no policies or inadequate policies in place with respect to protection of PHI?
  – If reasonable policies were in place were they followed?

Report...Report...Report

• Report Immediately
  – Type of breach and # of individual affected
  – Better to report than have media report

• Begin internal investigation
  – Need to include IT, MR and forensic review
An ounce of prevention is worth a pound of cure. – Benjamin Franklin

EHR Vulnerabilities
Legal Medical Record

• The record contains the information needed to support the patient’s diagnosis and condition
  – Evidence of what occurred in the care of the patient and justifies treatment & services provided
• Legible
• Appropriate Authentication (Signed & Dated)
• Clear & concise language

Electronic Health Record (EHR)

If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately is considered an “original”.

Federal Rules of Evidence
Federal Rules of Evidence (803) (6)

• Establishes Admissibility
• Federal Rules of Civil Procedure
• Uniform Business and Public Records Act
• Exception Hearsay Rule
  1. Documented in a normal course of business
  2. Kept in the regular course of business
  3. Made near or at the time of the matter recorded
  4. Made by a person within the business with knowledge of the acts, events, conditions, opinions, or diagnoses appearing on it

Electronic Audit Trails

• Definition
  – *Is a business record of all transactions and activities, including access, associated with medical record*

• Purpose
  – To establish integrity of EHR
• Critical legal functionality
• Do not allow “back door” access by system administrator to makes corrections without an audit trail
Auditing of the EMR

- Facilitated by running queries to identify specific records meeting defined parameters
- Running reports on key metrics associated with defined protocols
- Specific to patient
- Specific to staff/labor

Other E-Policies Needed
Checklist e-Policies

✓ Contents of the Legal Record
✓ Procedures for creation & maintenance of reliable records
✓ Authentication of entries in medical record (e-signature)
✓ Information Access Management
✓ Printing the Legal EHR
✓ Amendments, Corrections, Deletions
✓ Authorization to release information electronically

Checklist e-Policies

✓ Use of Abbreviations (Do not use)
✓ Copy & Paste Functionality (Carry forward)
✓ Importing/Scanning photographs
✓ Back up Procedures
✓ Downtime Procedure Documentation
✓ Protection from malicious software
Current Efficiencies of EHR

• Point of Care documentation
• Generation of orders
• Ease of access to information for same & other disciplines
• Ability to tract 485, CTI, Physician orders
• Matching of visits to frequency of orders
• Scheduling capabilities
• Collection of data for case conferences, IDT
• Ability to provide reminders, prompts & alerts
• Clinician Work lists
• Audit capabilities for clinical record review
• Automatic creation of payroll data
• Flow through of information to billing system
• QA, PI, IC data collection

Current Vulnerabilities EHR

• Protection of patient information
• Increased access to information
• Audit trials
• Cut & Paste Functionality
• Ease in documentation
• Flow through of information to billing system
**E PHI Vulnerability Sources**

- Current staff
- Per Diem Staff
- Receive e-mail from patient with PHI listed
- Portable Storage Devices
  - Without Encryption

**Encryption**

- Encrypted PHI is not subject to the breach rule – encrypt where possible

- “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” *Federal definition*

- **Encrypted**, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.
Standards for Encryption

- Consistent with National Institute of Standards and Technology (NIST) Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices
- Valid encryption processes for data moving through a network, including wireless, which comply with requirements of Federal Information Processing Standard 140-2

Timely Documentation

- Documentation should be completed at or as close to Point of Care as possible
  - In the Home
  - In the Car
- **Tip**: *Completing the documentation in the patient’s home allows for the most comprehensive note that encompasses what was seen, heard and done for the visit*
Documentation Errors

- Addendums
  - New documentation is used to add information to the original entry
- Amendments
  - Documentation meant to clarify information within the record
- Corrections
  - A change in information meant to clarify inaccuracies after the original document is complete
- Deletions/Retractions
  - The action of eliminating information from previously closed documentation without substituting new information
- Entry wrong patient record
- Entry wrong admission
- Late entry
  - Documentation entered after the point of care

Correction of Clinical Records

- State Operations Manual
- The HHA is encouraged to create policies and procedures that govern correction of clinical records.
  - When a comprehensive assessment is corrected, the HHA must maintain the original assessment record as well as all subsequent corrected assessments in the patient’s clinical record for five years, or longer, in accordance with the clinical record requirements at 42 CFR 484.48.
  - It is acceptable to have multiple corrected assessments for an OASIS assessment, as long as the OASIS and the clinical record are documented in accordance with the requirements at 42 CFR 484.48, Clinical records.
  - Some agencies use a manual corrections form for one or more OASIS items that can be acceptable after confirming the correction with the original clinician or as described in the agency’s policies and procedures
New England Journal Medicine

• “Many times, physicians have clearly cut and pasted large blocks of text, or even complete notes, from other physicians; we have seen portions of our own notes inserted verbatim into another doctor’s note. This is, in essence, a form of clinical plagiarism with potentially deleterious consequences for the patient.”

• Pamela Hartzband, MD, and Jerome Groopman, MD, Beth Israel Deaconess Medical Center

Cut & Paste Functionality

• For organizations that allow carrying forward clinical documentation, auditing its use is a key part of ensuring document integrity. AHIMA

• Copying forward clinical documentation is the process of copying existing text in the record and pasting it in a new destination

• Also called cloning
Cloned Documentation

• Providers need to be aware that EHR can inadvertently cause documentation pitfalls
  — such as making the documentation appear cloned.
  — Cloned documentation could cause payment to be denied in the event of a medical review audit of records.
• Documentation is considered cloned when it is worded exactly like or similar to previous entries.
  — Also when the documentation is exactly the same from patient to patient
  — Individualized patient notes for each patient visit are required.
  — Documentation must reflect the patient’s condition necessitating treatment, the treatment rendered and the overall progress of the patient to demonstrate medical necessity.

Standardized Records

• Standardized MR entries can create problems when used improperly.
  — Standardized entries are statements that describe usually routine care.
• Clinicians may select a standardized entry from a menu in an EHR software program.
• Paper documents use check off boxes.
• Use of these entries saves time but if clinician selects the wrong entry or does not confirm the language of the entry is appropriate for the patient, an inaccurate or incomplete record may result.
Drop Down Menus

• Condition: Client condition is_______
  – Unchanged
• POC: Client is____________________
  – Partially participating in POC
  – Up as tolerated, no activity restrictions
• Homebound:
  – Max assist; Adult Day Health
• Teach: Topic #  Who - How - Response
  – Medications Pt Verbal Verbalized understanding

Tips for Clinicians

• Document clearly...
  – Spelling Counts
• Do not assume a drop down menu does not require a narrative
• Checking off homebound alone does not prove homebound status
  – Document rationale for homebound
• Be aware of any documentation inconsistencies among clinicians in same patient record
Secure your E-PHI
Decrease your Vulnerabilities

- Stay current with HIPAA changes
- Ensure policies are in place for compliance
- Begin reviewing audit trails
- Revisit HIPAA Security

Helpful Websites

- Federal Breach Notification
- HIPAA Privacy
  - [http://www.hhs.gov/ocr/privacy/](http://www.hhs.gov/ocr/privacy/)
- HIPAA Security
- AHIMA EHR Issues
Questions?????

It's QUESTION TIME!!

About the Speakers

Joan L. Usher, BS, RHIA, COS-C, ACE
Joan is President & CEO of JLU Health Record Systems, Pembroke MA, a consulting firm specializing in record management including EHR, OASIS, and Coding. She has a degree in Health Information Management and is OASIS certified. She is member of the Board of Directors for Home Care Alliance of MA and Hospice & Palliative Care Federation of MA.

Cherryllyn Simmons, BSN, RN
Cherryllyn is Director of Clinical Services for Homefront Health Care in Providence, RI. She was instrumental in the agency's start-up, Joint Commission Accreditation and conversion to EHR. She has over 30 years experience in nursing.