Privacy & Security: What You Need to Know
Vicki Bokar RN
• Sr. Director Corporate Compliance, Cleveland Clinic

John DiMaggio
• Chief Executive Officer, Blue Orange Compliance
Objectives

Discuss recent changes to federal patient privacy and security legislation

Provide real-life scenarios of patient privacy and security breaches and why nurses may be at risk

Review common challenges to HIPAA compliance and some practical tips for overcoming those challenges
Privacy and Security – Is it Important?

• Patients, family members, business partners etc. trust you with information
• Comply with state and federal laws and regulations
• Protect important electronic and non-electronic information
• Meaningful Use Requirement
• Enforcement
Privacy and Security – What can go wrong?

• Breaches are prevalent, frequent and widely reported
  • Intentional
  • Accidental
• Audit
  • Reactive - required by HITECH & in response to complaints or breaches
  • Proactive – HHS next wave of HITECH audits OR Meaningful Use audits
• Implications
  • Reputation at stake
  • Forced, time-based remediation
  • Fines, penalties, civil suits
• How can you prepare?
  • Prevent it from happening
  • Demonstrate compliance with regulations
  • Demonstrate best practice controls & prevention
Privacy and Security – What do you have to do?

• Minimum – HIPAA
• State laws if more strict
• Any additional company policies of more strict
Ohio – State Laws

- **General**
  - **Ohio Revised Code § 3721.13(10).** All residents have the right to confidential treatment of personal and medical records.

- **Access**
  - **Ohio Revised Code § 3721.13(8).** Residents have the right to access all information in the resident’s medical record. If the attending physician determines it is not medically advisable, then the information must be given to the resident’s sponsor if the sponsor is authorized to receive such information.

- **Restrictions**
  - **Ohio Revised Code § 3721.13(10).** Residents have the right to approve or refuse the release of medical records outside of the facility, unless certain exceptions (release in connection with transfer to another provider or as required by law, rule or third party payment contract).

- **Breach**
  - **Ohio Revised Code § 1349.19.** Any person or entity that conducts business in Ohio and owns or licenses computerized data that contains personal information (defined as an individual’s name when linked to certain data elements, including social security number, driver’s license number or any account number) must disclose any unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of such personal information. Notice must be made within 45 days to the individual whose data was compromised and, if involving more than 1,000 individuals, to consumer reporting agencies.

  **NOTE:** there are separate provisions for mental health, HIV, minors, substance abuse
HIPAA Background

• What is HIPAA? Health Insurance Portability and Accountability Act
• Why HIPAA?
• Privacy and Security in Title II (of V)
  – Administrative Simplification Part 164
    • Subpart C – Security
    • Subpart D – Breach
    • Subpart E - Privacy
HIPAA Privacy/Security Timeline

- 2003: HIPAA Privacy
- 2005: HIPAA Security Rule
- 2010: HITECH
- 2013: Omnibus
- 2012: Test Audits
- 2015: Audits Resume
HIPAA – Who needs to comply?

- **Covered Entity (CE):**
  - Health Plans
  - Health Care Providers: Any provider who electronically transmits health information in connection with standardized transactions regulated by HIPAA (e.g., claims transactions, benefit eligibility inquires, etc.).
  - Health Care Clearinghouses: Entities that process nonstandard information they receive from one entity into a standard format (or vice versa).

- **Business Associate (BA):**
  - A person or organization (other than a member of the CE’s workforce) that performs certain functions or activities on behalf of the CE that involves the use or disclosure of protected information. – Create, Receive, Maintain, Transmit
HIPAA – What is protected?

- Individually Identifiable Health Information (IIHI)
  - Name, Social Security Number, diagnosis, telephone number, the fact that a person is a resident
- Anything that can identify the resident and/or health conditions
- IIHI protected under HIPAA is PHI
- PHI in electronic form is EPHI
HIPAA – What has changed? - Omnibus

- Business Associates
  - Liability
  - Subcontractors
  - Compliance Dates
- Breach
  - Guilty until proven innocent
  - Analyze by Risk Assessment
- Sale of PHI
- Uses/Disclosures for Marketing, Fundraising Purposes
- Individuals may restrict disclosure to health plan if paid out of pocket
- CE’s must provide electronic record to individuals if requested
- Notice of Privacy Practices – disclose new rules
HIPAA – Uses and Disclosures

• Required Disclosures:
  • To individuals requesting access to their own PHI or an accounting of disclosures.
  • To HHS to investigate possible violations

• Permitted Uses and Disclosures
  • Treatment
  • Health Care Operations
  • Payment
  • Public Policy Exceptions
  • Deceased Persons (Revised)
  • Fundraising (Revised)
HIPAA – What is Security?

- Confidentiality
- Integrity
- Availability
HIPAA – Security Threat Examples

- Malicious Outsider
  - Hackers
  - Phishers
- Malicious Insider
  - Disgruntled employees
  - Employees leaving
- Human Error
  - Lost laptop
  - Didn’t secure firewall properly
  - Inadvertent email or fax
- Environmental
  - Fire, Flood
  - Loss of power
  - Loss of connectivity

- Confidentiality
- Integrity
- Availability
Protecting Information – Security Safeguards

- Access Control
- Security Awareness
- Contingency Planning
- Personnel Security
- Risk Assessment
- Media Protection
- Physical and Environmental
- Transmission Integrity
- Audit and Accountability
- System Integrity
- System Maintenance

Types of Safeguards
- Physical
- Administrative
- Technical

HIMSS
transforming health through IT

NURSING INFORMATICS INSTITUTE
HIPAA – Some Controls in Place Around You

- Administrative
  - Risk Assessment, Security Plan
  - Training
  - Policies and Procedures
  - Documentation
  - Contingency Planning
- Technical
  - Antivirus
  - Firewall
  - Encryption
  - Account Lockout, Screensaver
  - Username/Passwords – complexity, change regularly
- Physical
  - Keys/KeyCard Restricted access
  - Monitors positioned
Breach

• An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected information.
• Presumed a breach unless proven otherwise – Risk Analysis
• A breach is discovered on the first day it is known to the Covered Entity or the Business Associate
• Exceptions:
  – Unintentional
  – Inadvertent
  – Unauthorized person was unable to retain information
• If you think there is any possibility a breach has occurred, contact your Privacy Officer
Recent Breaches and Causes

• Community Health Systems
• HHS “Wall of Shame” – Breaches affecting 500 or more individuals
FBI LIAISON ALERT SYSTEM
#A-000039-TT

The following information was obtained through FBI investigation and is provided in conjunction with the FBI’s statutory requirement to conduct victim notification as outlined in 42 USC § 10607.

SUMMARY

The FBI is providing the following information with HIGH confidence. The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII). These actors have also been seen targeting multiple companies in the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data.

TECHNICAL DETAILS

The FBI has received the following information pertaining to a recent intrusion into a health care system that resulted in data exfiltration. Though the initial intrusion vector is unknown, we believe that a spear phish email message was used to deliver the initial malware. Typically, these actors use Information Technology themed spear-phishing messages which contain a malicious link that may connect to a new VPN site/service/client or a new Webmail site/software. Once access is obtained, the actors may collect and use legitimate account credentials to connect to the targeted system, usually through VPN.
We’re Not in Kansas Anymore!

- Armed robbery: Boston Massachusetts 9/24/14
- Physician’s laptop and cell phone were stolen
- The assailants were armed with a gun and a knife
- The physician, was reportedly tied to a tree and forced to disclose passwords for both devices
- Protected Health Information belonging to 999 individuals was compromised
HIPAA Violations: Consequences

• Loss of patient trust, disciplinary action (including termination), adverse licensure action by state boards, private tort & class action litigation

• *Individual workers* have been prosecuted for violating HIPAA

• 2004 - Richard Gibson, phlebotomist, stole demographic info from a cancer patient and opened 4 credit cards. Sentenced to 16 months jail and 9k restitution (per plea Agreement)

• 2010 – Huping Zhou, a UCLA researcher, was sentenced to 4 months in federal prison for snooping. UCLA agreed to pay an $865,000 fine

• 2014 - Joshua Hippler, East Texas hospital employee, indicted on charges of Wrongful Disclosure of PHI. If convicted, he faces up to 10 years in prison
Private Tort Litigation

Hinchy v. Walgreen Co. et al

• A Walgreen pharmacist was informed by her husband of past sexual conduct with Hinchy & possibility of a sexually transmitted disease

• The pharmacist intentionally accessed Hinchy’s prescription information while at work

• The pharmacist’s husband sent a text message to Hinchy, causing her to suspect that her information was impermissibly accessed.

• In July 2013, jury awarded $1.44 M to Hinchy
Then There’s the Untrained Employee

_Penn State Hershey Medical Center_ – Data breach affecting 1801 individuals

- Lab Tech authorized to work with PHI after hours from home
- Transported PHI on unencrypted flash drive
- Entered PHI into a test log using personal devices and systems that weren’t secure
- Used his personal email account to send the updated test log to two Penn State doctors
Why is HIPAA Compliance So Challenging?

- People want to reduce HIPAA to a list of do’s and don’ts (it doesn’t work that way)!
- Unique nomenclature differs from that used in the industry
- Typically need to apply both the Privacy Rule and Security Rule to any given situation!
- Each Rule consists of numerous standards and implementation specifications
- Which standards apply will depend on the underlying facts
- Change one fact, the answer could be completely different
The Good News!

• Most of HIPAA aligns with old fashioned common sense

• HIPAA respects - and often defers to - professional judgment

• The word “reasonable” appears 51 times in the Security Rule – it’s truly not meant to impede the provision of healthcare

• The Risk Analysis is your compliance “north star”
Some Risk Analysis Considerations

• Though it seems to get the most media attention, EMR “Snooping” is not the only risk to ePHI!

• Need to think beyond the EMR and mainstream billing systems:
  – Clinical photography - security of camera and stored images
  – Operational Registries, databases (even Excel spreadsheets)
  – Networked medical devices (e.g. smart pumps, etc.)
  – Laptops connected to diagnostic equipment

• Patient safety **MUST** be factored into your risk analysis and risk management process – always involve personnel from clinical, administrative and financial operations
Designated Record Set(s)

• Is not limited to information maintained in the electronic medical record
• Is broader than the “Legal Medical Record”
• A Designated Record Set is:
  – the medical records and billing records about individuals maintained by or for a covered health care provider;
  – the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or,
  – used, in whole or in part, by or for the covered entity to make decisions about individuals.
• With some exceptions, the individual’s Right to Access applies to PHI maintained in the covered entity’s designated record set(s)
Smart Computers; Dumb Users

- All employees (including students/volunteers) need to understand:
  - Social media policies
  - De-identification requires more than just “stripping 18 identifiers”
  - Posting any work-related information can land them in hot water with HIPAA and beyond
  - HIPAA applies not just to PHI of patients, but to all *individuals*, including colleagues and co-workers who are patients of the employer
  - How to avoid disclosing PHI via prayer chains and other well-intentioned support mechanisms (e.g. caringbridge etc.)
Achieving the Right Balance
PHI is the New Currency of Healthcare
Data Integrity

• Doesn’t get enough attention, but is just as important as privacy/security
• Health reform has prompted numerous initiatives involving the collection, analysis, use or disclosure of PHI
• Everyone needs to be singing from the same hymnbook (Silos are risky)
• Example: eliminating a data field for security purposes
• The pressure of cost-containment can also lead to unintended risks (e.g. shortcuts, unsecure work-arounds etc.)
Some Practical Take-Aways

• Policies/procedures alone are not enough – they need to be communicated and understood

• Your weakest link is the employee you hired yesterday – training is not a “one-time-only” deal

• Business Associate Agreements and Confidentiality Statements are not enough. What happens when the ink dries? Are the contractual terms communicated to those with day-to-day responsibility?

• Compliance must be monitored and consistently enforced

• Nursing Informatics & IT Security professionals have the opportunity to translate, educate & develop core competencies for all workers
Practice What You Preach!

• Never send PHI to a personal email address (yours or someone else’s)
• If patient insists you transmit PHI via regular email, be sure to explain risks
• Do not use Auto-Forwarding for email
• Avoid saving/downloading PHI. If you must save, only save to secure network drive or encrypted flash/USB drive
• Only use mobile devices that are encrypted
• Never upload or scan PHI in online tools (read terms & conditions)
• Never use apps that are not officially approved by IT Security
• Report privacy & security incidents promptly
Practice What You Preach

• Do NOT disable anti-virus software or install unapproved software. Never introduce new hardware or media without approval from your organization’s IT Security personnel
• Be suspicious of any email that you didn’t expect to receive (and never click on a link or attachment)
• Beware of phishing emails
• Keep up with Security Awareness training
Additional Resources

• Office for Civil Rights [http://www.hhs.gov/ocr/privacy/index.html](http://www.hhs.gov/ocr/privacy/index.html)
• Office of the National Coordinator for Health Information Technology (ONC) [http://www.healthit.gov/](http://www.healthit.gov/)

- Logo - NURSING INFORMATICS INSTITUTE - transforming health through IT - Logo
Objectives (Review)

Discuss recent changes to federal patient privacy and security legislation

Provide real-life scenarios of patient privacy and security breaches and why nurses may be at risk

Review common challenges to HIPAA compliance and some practical tips for overcoming those challenges
Vicki Bokar RN
• Sr. Director Corporate Compliance, Cleveland Clinic
  bokarv@ccf.org
  216 445 8274

John DiMaggio
• Chief Executive Officer, Blue Orange Compliance
  John.dimaggio@blueorangepolicy.com
  614 567 4109