Cyber Security Round Up

CTHIMA Workshop
November 9, 2018

Presentation by Jennifer L. Cox, J.D.
Cox & Osowiecki, LLC
Hartford, Connecticut

Today's Program Agenda
Discussion of Security Issues and HIPAA

- HIPAA Security compliance goes beyond technology or technical tools and solutions
- Five key security and cyber awareness areas
- Cloud and co-location considerations for HIPAA compliance
- Social media and digital presence
- Necessary data protections versus information blocking

Security Is Not All Technical

- Ensure that HIPAA Security Compliance is not "just an IT/IS" function
- The HIPAA Privacy Rule still contains a "mini-security rule" that should not be overlooked or forgotten
- Of the three HIPAA Security Rule safeguards, the administrative safeguards section has the most content, by far, with scores of:
  - Policy, procedure, implementation and documentation requirements

Administrative Safeguards

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

-HIPAA 45 CFR 164.304

Cyber and Security Awareness

Five Awareness Areas That Deserve An Internal Compliance Check

- Workforce awareness and training
- Connecticut laws on monitoring workforce
- Leadership and governance awareness
- Bring Your Own Device policies
- Processing Security Incidents (versus breach)

Workforce Awareness and Training

- Studies indicate that over 80% of breaches include **human error**
- HIPAA requires specific training for security awareness:
- “Implement a security awareness and training program for all members of its workforce (including management).”
  - Security Rule 45 CFR 164.308(a)(5)

Workforce Awareness and Training

- How clear (and practical) is the training?
- Is specific instruction given on being vigilant about reporting anomalies or problems?
- Consider security **social engineering** testing
- How does your “help desk” handle reports
  - Do staff feel comfortable making reports?

Workforce Awareness and Training

- In addition to training, there is a requirement for deploying or sharing **Security Reminders**
  - Security Rule 45 CFR 164.308(a)(5)(ii)(A)
- Document security reminders (*e.g.*, include the type of reminder, its message, and the date it was implemented)
- Include HR as part of any Security policy review, training, and planning
  - Ensure policies and notices meet Connecticut law requirements for electronic surveillance of workforce
  - Termination of access credentials must be up-to-date

Electronic Monitoring of Workforce

Connecticut law C.G.S. section 31-48d includes:

- "Electronic monitoring" means the collection of information on an employer's premises concerning employees' activities or communications by any means other than direct observation, including the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic or photo-optical systems, but not including the collection of information (A) for security purposes in common areas of the employer's premises which are held out for use by the public, or (B) which is prohibited under state or federal law.

Electronic Monitoring of Workforce (cont.)

- (b) (1) …each employer who engages in any type of electronic monitoring shall give prior written notice to all employees who may be affected, **informing them of the types of monitoring which may occur.** Each employer shall post, in a conspicuous place which is readily available for viewing by its employees, a notice concerning the types of electronic monitoring which the employer may engage in. Such posting shall constitute such prior written notice.

Leadership Awareness

- Security needs to be an enterprise-wide practice and investment, expressly including leadership and governing body
- Do the Privacy and Security Officials have a direct line of communication to upper management?

Leadership Awareness

HIPAA Security Series Administrative Safeguards sample question:

Is executive leadership and/or management involved in risk management and mitigation decisions?

Leadership Awareness

- Vulnerabilities need to be identified and addressed on an ongoing basis
- Who is involved in risk assessment and mitigation planning?
- Do you have a gap analysis with unfilled gaps?
  - Is leadership aware?

Bring Your Own Device

- There is no specific standard or specification requiring a policy for BYOD
- But, not having a BYOD policy makes it difficult (perhaps impossible) to remain Security Rule compliant
- If your policy is “Never…[bring your own device]” – how are you auditing that?
  - Operational tip: “Never” (and “always”) should generally be avoided in policy writing

Bring Your Own Device

- Workforce members have a tendency for self-help and/or misunderstand technical requirements
  - Example: password protection on a cell phone does not necessarily equal encrypted device
- If your HIPAA policies affect more than employees, how does BYOD work, and what are the means of communication and oversight for non-employees who have to follow your policies?
  - Example: use of personal devices by attending physicians, medical staff

Security Incidents

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

-45 CFR 164.304

Processing Security Incidents

- Security Incidents will be far more common than breach
  - Business associate agreements should address both breach and Security Incidents, with clarity on what needs to be reported to the covered entity
  - Security Incidents do not require external notification to patients or reports to OCR
- A Security Incident may or may not be a breach
- If the Security Incident might also be a breach, be sure that the Privacy Official is aware and engaged

Security Incident ≠ Breach

Cloud Computing and HIPAA Security

- A Cloud Service Provider (CSP) is the business associate of the covered entity (or business associate) for whom it is providing services
- The ability to view or access PHI is not the trigger or key element
- OCR issued extensive guidance on CSPs and HIPAA compliance:
  - https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

Cloud Computing and HIPAA Security

- CSPs generally offer online access to shared computing resources with varying levels of functionality depending on the users' requirements, ranging from mere data storage to complete software solutions (*e.g.*, an electronic medical record system), platforms to simplify the ability of application developers to create new products, and entire computing infrastructure for software programmers to deploy and test programs. Common cloud services are on-demand internet access to computing (*e.g.*, networks, servers, storage, applications) services.

Cloud Computing and HIPAA Security

Q: If a CSP stores only encrypted ePHI and does not have a decryption key, is it a HIPAA business associate?

A: Yes, because the CSP receives and maintains (*e.g.*, to process and/or store) electronic protected health information (ePHI) for a covered entity or another business associate. Lacking an encryption key for the encrypted data it receives and maintains does not exempt a CSP from business associate status and associated obligations under the HIPAA Rules. **An entity that maintains ePHI on behalf of a covered entity (or another business associate) is a business associate, even if the entity cannot actually view the ePHI**

Physical Co-location *May* Differ From Cloud Service

- A CSP must be a BA (with a BAA in place)
- But the application of BA rules for "pure" physical co-location (without CSP functionality or features) is an unanswered question
- HIPAA lawyers disagree about this and OCR has yet to clearly declare one way or the other
- Argument that it is NOT a BA situation:
  - It's more like leased office space, where your landlord is not your BA

Co-location

- Non-cloud co-location that *might* not be a BA:
  - Your owned server
  - No shared servers
  - No cyber access by third parties
  - No physical access by third parties
  - Encrypted data

Co-location

- Best practice: the co-location site is a BA (with a BAA in place)
  - There is at least a shared responsibility for physical safeguards
  - The purpose of the relationship is rented space for servers
  - Consistent with OCR approach to paper record storage

Social Media Considerations

- Social Media needs to be monitored and moderated
- Not easy to have blanket rules for patients, visitors or employees
- Policies for media, social media, marketing and general communications should be part of routine internal discussion and review

Reminder About Labor Laws And Social Media Restrictions

NLRB ruling and confirming case law clarify: Employers must be cautious about restrictions on employee activities, including:

- You may not have a blanket rule, policy, or handbook, that prohibits references or negative posts about work or workplace on social media
- You must be careful if you choose to discipline workers because of comments – it is important to assess whether the remarks fall under "protected concerted activity" per NLRA (even if the remarks are hostile, vulgar, seen by clients/patients)

HR-Related Social Media Reminder

- It does not matter if you are union or non-union
- It isn't dispositive that the posts used offensive language or made personal attacks
- This includes not disciplining people who support the remarks – *e.g.*, with a "like"
- Similar issue: If you prohibit photos (for example to maintain patient privacy), you need to be very careful how that is worded, and how it is enforced…a worker who is gathering evidence of a crime or improper employer behavior might be protected

HR and Labor and Employment Compliance Specifics

- It may be a good time to have your handbook or policies reviewed
- You may wish to speak with an attorney or consultant who is trained, experienced and versed in labor and employment/HR specifically (not just any lawyer)
- Most general lawyers, and most healthcare lawyers, are aware of, but not particularly well-versed in, this area of law and compliance

Filming and Promotions

- General rules:
  - You **may not film patients** without their **PRIOR** permission
  - You may not use a patient's identity in your promotional materials without consent
  - You may not post photos or identifying information about patients on your social media sites/pages without their consent
- Work to control what is within your control
  - You are not required to stop all friends and family from their personal Facebook use
    - Suggestion: **Do not tackle visitors to get their phone**
    - Suggestion: Try de-escalation techniques when visitor policies are not being followed
  - You should remove inappropriate posts on your own social media pages

Data Protections Versus Information Blocking

- The obligation to protect data and keep data safe from unauthorized access naturally is the cornerstone of an entity's culture and design for privacy and security
- A provider has the legal discretion in many cases to determine whether to disclose (and it is often easier, and feels more secure, to deny access to third parties)
- But failing to allow access to another provider or a carrier could be interpreted as improper "information blocking" – even if security was the genuine goal

Connecticut Law On Information Blocking

To the fullest extent practicable, **a hospital** must use its EHR system to enable the secure two-way exchange of patient electronic health records with other licensed providers who (1) have a system that can exchange these records and (2) provide health care services to a patient whose records are being exchanged….Upon the request of a patient or the patient's health care provider, as long as:

- the transfer or receipt would be secure, not violate any state or federal law or regulation, and not constitute an identifiable and legitimate security or privacy risk, and
- for requests from a provider, the patient **consents to <u>and</u> has authorized** the exchange.

Under the act, if the hospital has reason to believe that such a record transfer would be illegal or present an identifiable and legitimate risk to security or privacy, it must promptly notify the requesting party.

See C.G.S. sections 19a-904c; 19a-904d

Federal Rules on Information Blocking: 21st Century Cures Act

- 21st Century Cures Act defines "information blocking" broadly as a "practice that . . . is likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information" if that practice is known by a developer, exchange, network, or **provider** as being likely to "interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information."

42 U.S.C. §300jj-52(a).

- **We await regulations to implement this.**

Federal Rules Information Blocking

- We have a preview of where these regulations will land from the Promoting Interoperability programs (Meaningful Use and MACRA/MIPS)
  - Prepare for impact
- Both MU and MACRA/MIPS programs include obligations for providers to attest that they are not information blocking
- The “Prevention of Information Blocking Attestation” is elaborate, and has three statements, each of which has accompanying guidance and definitions

Statement #1

- Statement 1: A health care provider must attest that they did not knowingly and willfully take action (such as to disable functionality) to limit or restrict the compatibility or interoperability of CEHRT.

Statement #2 (parts 1 and 2)

- Statement 2: A health care provider must attest that they implemented technologies, standards, policies, practices, and agreements reasonably calculated to ensure, **to the greatest extent practicable and permitted by law**, that the CEHRT was, at all relevant times:
  1. Connected in accordance with applicable law;
  2. Compliant with all standards applicable to the exchange of information, including the standards, implementation specifications, and certification criteria adopted at 45 CFR Part 170…

Statement #2 (parts 3 and 4)

…[**to the greatest extent practicable and permitted by law**, that the CEHRT was, at all relevant times]:

3. Implemented in a manner that allowed for timely access by patients to their electronic health information (including the ability to view, download, and transmit this information); and
4. Implemented in a manner that allowed for the timely, secure, and trusted bidirectional exchange of structured electronic health information with other health care providers (as defined by 42 U.S.C. 300jj(3)), including unaffiliated providers, and with disparate CEHRT and health IT vendors.

Statement #3

Statement 3: A health care provider must attest that they responded in good faith and in a timely manner to requests to retrieve or exchange electronic health information, including from patients, health care providers (as defined by 42 U.S.C. 300jj(3)), and other persons, regardless of the requestor's affiliation or technology vendor.

Shift Caused By Information Blocking Focus

- HIPAA created a dichotomy between disclosures that are mandatory (*e.g.*, patient access under 45 CFR 164.524; "required by law") versus others that are ***permitted*** but not required (*e.g.*, for the healthcare operations of the other provider)

Information blocking rules will transform many *permitted* disclosures into "likely required" disclosures.

Q & A