Lessons Learned: HIPAA Violations and Office of Civil Rights Enforcement

Lindsey Wiley, MHA, CHTS-IM, CHTS-TS
HIT Manager, OFMQ
An Important Reminder

For audio, you **must** use your phone:

**Step 1:** Call (866) 906-0123.

**Step 2:** Enter code 2071585#.

**Step 3:** Mute your phone!!!

= AUDIO
Mission of OFMQ

OFMQ is a not-for-profit, consulting company dedicated to advancing healthcare quality. Since 1972, we’ve been a trusted resource through collaborative partnerships and hands-on support to healthcare communities.
OFMQ Areas of Expertise

• Analytics
• Case Review
• Education
• HIPAA
• IT Consulting
• Health Information Technology
• National Quality Measures
• Quality Improvement
HIT Service Lines

- HIPAA/Meaningful Use Security Risk Assessment - Level 1, 2, and 3
- Meaningful Use Assistance
- Meaningful Use Audit Support
- Risk Management Consulting and Development
- Staff HIPAA Security Training
- Website Development & Secure Email
- IT Consulting
Lindsey Wiley, MHA, CHTS-IM, CHTS-TS

Lindsey works with healthcare providers and hospitals to advance the use of electronic health records (EHR) to improve patient care and health outcomes. She consults with physician practices and hospitals to successfully implement and meaningfully use EHRs, including assistance associated with vendor products, hardware, software and system configuration and troubleshooting, staffing considerations, workflow analysis, EHR utilization, security and privacy, and quality data reporting from EHR systems.
OFMQ’s Role in Health IT

• Bridging the gap between Technology and Quality Improvement
• Participating in multiple Healthcare Initiatives within the State
• Spreading awareness of HIPAA Requirements
What is HIPAA?

• Health Insurance Portability & Accountability Act of 1996
• HIPAA Protects Individually Identifiable Health Information
• Protected Health Information (PHI)
What Is HIPAA?

• Began as a program to protect health insurance coverage for workers and families when changing/losing jobs and added administrative simplifications for healthcare transactions
• HIPAA applies to all organizations and individuals that deal with health information (Covered Entities)
• Defines minimum necessary criteria for PHI
• Privacy rules were added to protect the privacy of individuals’ health information
• Security rules were added to protect electronic health information
• Omnibus Rule was added to refine HIPAA applicability to Business Associates and to add stiffer penalties for violations
HIPAA Importance

- Meaningful Use requirements
- Required by law
- Required to report breaches
- OCR actively enforces law and issues fines
- PHI/PII is worth millions
- Breaches can result in significant losses for you and your patients
- Impact of breaches is felt for years
Protected Health Information (PHI)

• Individually identifiable health information that is:
  – Created or received by a health care provider, health plan, employer, or health care clearinghouse that relates to:
    • Past, present, or future physical or mental health or condition of an individual
    • Provision of health care to an individual
    • Past, present, or future payment for the provision of health care to an individual
  – Combination of 2 or more identifiers such as...
Examples of PHI

- Encounters/Visit Documentation
- Appointment Dates/Times
- Radiology Films and Reports
- Names (Including Initials)
- Postal Addresses
- Medical Record Numbers
- Social Security Numbers
- Account Numbers
- License/Certification Numbers
- Vehicle Identifiers/Serial Numbers/License Plate Numbers
- Internet Protocol Addresses

- Lab Results
- Invoices
- History and Physicals
- Health Plan Numbers
- Full Face Photographic Images and any Comparable Images
- Web Universal Resource Locators (URLs)
- Telephone Numbers
- Fax Numbers
- Email Addresses
- Biometric Identifiers, including Finger and Voice Prints
- Any Dates Related to Any Individual (DOB, Admission Date, Discharge Date)
- Any other unique identifying number, characteristic or code
Personally Identifiable Information (PII)

- DHS defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.

**EXAMPLES OF PII**

- Names (Including Initials)
- Social Security Number
- Date and Place of Birth
- Email Addresses
- Mother’s Maiden Name
- Account Numbers
- Driver’s License Numbers
- Passport Numbers
- Vehicle Identifier Numbers
- License Plate Numbers
- Device Identifiers or Serial Numbers
- Internet Protocol Addresses
- Biometric Identifiers
- Educational Information
- Financial Account Information
- Medical Information
- Criminal or Employment Information
- Citizenship Status
Who is Enforces HIPAA?

- Office for Civil Right’s (OCR)
- Responsible for:
  - Administering and enforcing the HIPAA Privacy and Security Rules
  - Conducts complaint investigations
  - Compliance reviews
  - Audits
- OCR works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA
Increased Enforcement
2016 HIPAA Audits

What and Why?

• This is the 2\textsuperscript{nd} round of audits, 1\textsuperscript{st} in 2013
• OCR can gain feedback on aspects of HIPAA that are causing covered entities problems
• Help develop new guidance to ensure safeguards are in place to protect PHI
• Ensure covered entities are following HIPAA rules (fines if not)
2016 HIPAA Audits

• Focusing on key areas based on round 1 findings
• Most will be desk audits not onsite audits
• Focus points include: encryption & decryption, facility access control, breach notification & complaints
• OCR is not interested in penalizing every organization that suffers a data breach, but they do expect those organizations to have safeguards in place
• In order to avoid financial penalties, covered entity MUST have conducted a risk assessment
Selection of Phase 2 Audits

- OCR has randomly selected 550-800 covered entities' through surveys recently issued asking for organization and contact information.
- Based on the survey information, OCR will select approximately 350 covered entities' for the phase 2 audits (232 health care providers, 109 health plans, 9 health clearinghouses).
- Selected covered entities will be sent data requests asking for contact information for their business associates (BA), from this they will select the BA’s that will participate in the audits.
Dear XXXX:

This is an automated communication from the Office for Civil Rights (OCR).

According to our records, you are the primary contact OCR should use to reach NAME OF FACILITY regarding its potential inclusion in the HIPAA Privacy, Security, and Breach Notification Rules Audit Program. We are attempting to verify this email address.

Please respond within five (5) days as instructed below to either confirm your identity and email address or instead provide updated primary and secondary contact information.

If you ARE the primary contact for this organization, please select the following link YES. Once the link is selected, a browser window will open and your response will be recorded.

If you ARE NOT the primary contact for this organization, please select the following link NO. Once the link is selected, a browser window will open and your response will be recorded.

Thank you for your cooperation. If we do not receive a response from you we will use this email address for future communications with this entity. Failure to respond will not shield your organization from selection.

If you have questions or comments regarding this message, you may contact us at OSOCRAudit@hhs.gov.

Sincerely,

Jocelyn Samuels
Director
Office for Civil Rights

Department of Health and Human Services

http://www.hhs.gov/ocr
Audit Process

OCR will audit:

• 150 out of the 350 selected covered entities and 50 business associates for compliance with the Security Standards
• 100 covered entities will be audited for compliance with the Privacy Standards
• 100 covered entities will be audited for compliance with the Breach Notification Standards
Audit Process

- Covered entities and business associates will have two weeks to respond to OCR’s request
- They will be asked to provide content and file organization, file names and any other document submission requirements
- It is critical that the organizations provide the specific documentation requested by the OCR, the auditors will not be contacting them for clarifications or request additional information
- Failure to respond to the request could result in a referral to the OCR Regional Office for compliance review
Don’t Let this be You!
Hackers hold California Hospital’s Network Hostage

• Attackers asking $3.6 million to decrypt the system and files.
• Hospital is unsure how far widespread, what kind of ransomware, or how infected in first place.
• Believed to be caused by staff member clicking a malicious link or attachment to spread malware through the network.
• Disruption in business as they are now depending on fax machines, landline phones, and paper medical records.
• Patients transferred out to other facilities
Case Studies

• 2012 Impairment Resources LLC forced to file Chapter 7 bankruptcy when nighttime burglary resulted in breach of approximately 14,000 electronic patient records – rather than face HIPAA violation penalties and civil suits, the company closed its doors forever.

• March 2012 Blue Cross Blue Shield of Tennessee – 57 unencrypted computer hard drives stolen from leased facility that contained PHI for over 1 million individuals, lack of administrative and physical controls at site resulted in $1.5 million in penalties

• October 2011 Sutter Health – unencrypted, password protected desktop computer with PHI for 4.2 million patients stolen from administrative offices, resulted in class action lawsuit for $1 Billion (suit was eventually dismissed, but not until 2 ½ years later)
Case Studies

- **2012 Medical Center in Boston** – Physician’s Laptop with PHI and PII Stolen from his Desk, Resulted in $100,000 Settlement
- Pharmacy chain maintained pseudoephedrine log books containing PHI in a manner so that individual PHI was visible to the public at the pharmacy counter; **OCR’s corrective action plan** for compliance required implementation of policies and procedures to safeguard the log books
- January 2016 – Premier Healthcare notified 200,000 patients after **laptop with PHI was stolen** from the billing department in the administrative office
- August 2011 – **Laptop that accompanied portable CT scanner stolen** from unlocked treatment room during overnight hours, laptop hard drive contained PHI of 599 patients – resulted in $850,000 in fines
What Would You Do?

- A door leading to the parking lot that is normally locked is propped open with a box. What would you do?

  1. Move the box and close the door.
  2. Wait around to see who is going in and out.
  3. Close the door and contact security officer.
  4. See what is in the box.
What Would You Do?

A co-worker that has been on vacation for several weeks arrives at work only to realize they forgot the alarm code for the building. They text you and ask you for your alarm code. What is your response?

1. Text the alarm code.
2. Text the alarm code and tell your security officer you need a new code.
3. Tell them to contact the security officer.
4. Ignore the text message.
What Would You Do?

• You print and need to dispose of a large amount of documents containing PHI. The destruction bin is on the other side of the office complex. What would you do?

1. Put in my regular trash can temporarily and dispose of in destruction bin at end of day.

2. Use a crosscut shredder at my desk as an alternative.

3. Place in a cardboard box next to my desk and dispose of in a destruction bin at end of day.

4. Leave paper on my desk and turn upside down.
Case Studies

• 2015 St. Elizabeth’s Medical Center fined $218,000 for HIPAA breaches, one of which involved unencrypted ePHI stored on a former hospital workforce member’s personal laptop and USB flash drive, affecting 595 individuals

• April 2010 Affinity Health Plan, Inc. — impermissibly disclosed PHI of 340,000 individuals when it returned multiple photocopiers to leasing agent without erasing the data contained on the copier hard drives, resulted in $1.2 million fine

• December 2015 – University of Washington Medicine (UWM) reports data breach affecting 90,000 individuals when ePHI was accessed after employee downloaded an email attachment that contained malicious malware, resulted in $750,000 settlement

• March 2014 – Franciscan Health System experienced data breach affecting 8,300 patients as a result of phishing scam; employees replied to emails from entity masquerading as parent company
What Would You Do?

- Your friend tells you to check out this news article about your neighbor. You go to the site and get a window that says yours computer has been infected with a virus – Click OK to remove the virus.

1. You click OK
2. You click OK and contact your security officer
3. You reboot your computer
4. Contact your security officer/IT and wait for further instruction
What Would You Do?

• You receive an email from your supervisor asking you to send them a list of all patients seen in the past month. The email states you need to have their full name, address, phone, and social security number. What would you do?

1. Run the list and send to your supervisor.
2. Encrypt the list and send to your supervisor.
3. Call your supervisor to verify the request and provide the information via an approved secured mechanism.
4. Contact your security officer.
What Would You Do?

• While at work you decide to check out Facebook on your computer. Your friend posts a personality quiz about what color of cat you would be. What would you do?

1. Take the quiz, I love those things.
2. Take the quiz but do not post the results. That would be embarrassing.
3. Skip this quiz but take the one where I get the $20 gift card for coffee.
4. Close Facebook. I really should not be accessing social media at work.
I am Scared,
What Should
I do
Your To-Do List

• Don’t be in denial – willful neglect will cost you
• Ignorance is no longer an excuse or option
• Perform a **COMPLIANT** Risk Assessment- Make corrections based on results
• **TRAIN** your staff, **EVERYONE** must be trained
• Review your policies and procedures per rules
• Don’t use generic policy – customize!
• DOCUMENT
• Conduct drills in audit and breach response
• Always have a plan for moving forward, AND FOLLOW IT
We Are Here To Help!

Email: ofmqhit@ofmq.com
       lwiley@ofmq.com
Call: (877) 963-6744
Visit: www.OFMQ.com

Questions?
Register Now at QualTechConference.com

QualTech 2016

Early Bird Price Ends May 10th: $129
Regular Price: $149

OFMQ’s 1st Annual HIT Conference

“Bridging the Gap Between Quality & Health Information Technology”

Join other professionals from hospitals, long-term care, ambulatory clinics, home health, hospice, and behavioral health care settings in learning how to eliminate the barriers of care coordination and better utilize HIT to advance healthcare.

Expert speakers to address hot topics such as Quality Improvement, HIPAA, Value-Based Purchasing, HIT.
Upcoming WebEx Events

Monthly HIT Educational WebEx | Wed, May 11 | 12:15pm
“Population Health Management”

Register at www.ofmq.com/event-month
Thank you!