HIPAA – Are You As Compliant as You Think?

Jillian Harrington, MHA, CPC, CPC-I, CPC-P, CCS, CCS-P
Regulatory Specialist, HCPro, a division of BLR

Agenda

• Elements of HIPAA Regulations
• HIPAA Case Study Reviews
• Questions?
Elements of HIPAA Regulations

• Standards for Electronic Transactions and Code Sets
  – Compliance Date: October 16, 2003
  – Enforced by: Centers for Medicare and Medicaid (CMS)

• Standards for Privacy of Individually Identifiable Health Information
  – Compliance Date: April 14, 2003
  – Enforced by: Office of Civil Rights (OCR)

• Standards for Security of Electronic Protected Health Information
  – Compliance Date: April 20, 2005
  – Enforced by: Centers for Medicare and Medicaid (CMS)
HITECH Act

- Health Information Technology for Economic and Clinical Health Act
  - Various compliance dates for different sections
  - Major HIPAA-Related Elements of HITECH
    - Breach Notification
    - Access to Electronic Records by Patient
    - Business Associates/Agreements
    - Accountability
    - Marketing Restrictions
    - Enforcement
    - EHR

HIPAA Omnibus Rule

- January 2013
- Placed into regulation many of the elements addressed in the HITECH Act
- Omnibus final rule:
  - Business Associates will be directly liable for Privacy/Security violations
  - Additional limitations on marketing/fundraising – no sale of PHI
  - Access to electronic PHI by patients – restrict disclosure to health plans
  - Modification to Notice of Privacy Practices
  - Changes to research and decedent information release
  - Additional enhancements to enforcement rules and tiered civil monetary penalties
  - Replacement of Breach Notification ‘harm’ standard with more objective standard
  - Prohibition on health plans using or disclosing genetic information for underwriting purposes (GINA)
HIPAA Case Study Reviews

The ER Visit

• A ‘small town’ hospital emergency room was visited by a high profile sports figure. Hospital uses an electronic health record. The next morning, information was published in the local newspaper detailing much more than was released to the press

• What possibly occurred?
• How could it have been prevented?
The ER Visit

- Access to the EHR by an RN in another unit, who provided the information to her spouse who writes for the local newspaper
- Staff member was terminated
- Audit logs were run and MANY other inappropriate accesses of this patient’s record were found
- Regular audits of access to charts
  - High profile patients
  - Same name
  - Outside of unit
  - Employees
- Ongoing training

The Cafeteria Conversation

- A practice administrator and a student interning from the local college visit the cafeteria for lunch and to discuss the student’s progress in their internship.

  Practice Adm: “Jill, you’ve been performing quite well thus far in your work for us. I commend you on your treatment of Mr. Burns yesterday. He can be a very difficult patient to deal with at times. You showed him a great deal of respect and kindness, which we should always do”

  Student: “Thank you, he seemed like a very nice man and I enjoyed speaking with him. I am enjoying my work here at the clinic thus far.”

  Sitting at the table behind the student and the manager is Mr. Burns’ family that brought him in to the practice the day before, as Mr. Burns is there having ordered testing completed.

- What is wrong with this picture?
- How could it be avoided?
The Cafeteria Conversation

- The practice administrator should not have spoken directly about any patients in an open setting such as the cafeteria.
- This type of problem occurs regularly in cafeterias, elevators, outside of work
- Training, training, training
- Hold meetings in private locations
- Do 'walk around' audits – listen for violations

The IT Mixup

- Joe in IT is working on a problem involving access to a data submission system for the QA/QI department. Suzie really needs to get this data submitted to the state by the end of the day and is unable to submit it. Joe thinks that it is an issue with the organizations firewall. Suzie is really hounding him, saying that the hospital could incur a fine if the data is not submitted by COB today. Joe takes down the firewall and they are able to get the data submitted. Unfortunately, he has difficulty getting the hardware firewall to come back up, and it takes two days. During that timeframe their system is hacked and information from their Patient Financial System, including names, SSN’s, and addresses are stolen
- What is wrong with this picture?
- What could have been done differently?
The IT Mixup

- Although a physical firewall is not a HIPAA requirement, controlling access to your systems is (45 CFR 164.312 (a)(1)). Firewalls (both physical and software) can help to maintain the barrier between the outside world and the information within the organizations systems
- Joe took the easy way out by simply taking down the firewall, assuming he’d flip the switch and turn it right back on
- Access control was compromised for the time period, as was the standard of integrity (45 CFR 164.312 (c)(1))
- Breach notification & control processes must move forward in this case
- Don’t take the easy way out – maintain access control and integrity at all times
- Fine faced by QA/QI likely less than what could be costs for breach notification and control
- Work with staff to educate on HIPAA requirements
- In this case – what other options for submission of data? Tape? Disc?

Records Release

- Mrs. Jones is in for a visit with Dr. Bob on Monday, and requests a copy of her records as she is going next week to see a physician in a distant city. Your practice requires a form for records release, even for treatment purposes. Mrs. Jones would like to hand carry the records to be sure that they arrive to the visit with her. She fills out the form and signs it, stating she will be back in later that week to pick up the records. On Friday, a person not known to the practice comes in to pick up Mrs. Jones’ medical record on her behalf. The front desk staff person releases the record.
- What was wrong here?
- What could have been done differently?
**Records Release**

- Information can be released to a third party in an emergency circumstance or in the case of the individual being incapacitated.
- In these cases, the organization would need to determine if it was in the best interest to release the information and disclose only what is relevant to the situation. (45 CFR 164.510(b)(3))
- No attempt to call Mrs. Jones was made – no signature was required
- Was this an emergency situation? Did these rules apply?
- Include this situation in your release of information policy
- Provide training to ALL staff involved in these processes – explain the consequences
- Also, be sure of state requirements for release
- Information on form for alternative person to pick up?

**Laptop Troubles**

- Tina, a biller in your practice, is getting slammed due to adding a new physician and two new mid-levels. She regularly works late hours, finishing up her work. She decides that she’ll take her laptop over to Starbucks and work there for a while. While at Starbucks, she runs quickly to the restroom, leaving the laptop on the table she was sitting at. Upon returning, the laptop is gone. Although access to the EHR and patient financial systems is online, this laptop contained numerous files with PHI on the hard drive, none of which were encrypted.
- Is this a problem for the practice?
- How could this have been prevented?
Laptop Troubles

• Although encryption isn’t a required safeguard, entities will be held accountable for safeguarding PHI

• By having unprotected PHI on this machine, there was no access control, and the person that stole it could access the information

• Address the Access Control standards (45 CFR 164.312(a)(1) based on the use of information within your organization

• Have policies in place regarding movement of laptops, mobile devices, etc out of the office

• Have policies in place regarding use of the hard drive to save files with PHI

Sign-In and Call Back Troubles

• Jillian comes into her OB/GYN’s office for her 2nd prenatal visit. She has not told anyone about her pregnancy, and due to other health issues likely won’t say anything to friends or family until she is quite far along. She signs the sign-in sheet. A friend of Jillian’s, Amy, comes in shortly after and signs in to see a different physician.
Sign-In and Call Back Troubles

• Jillian and Amy greeted each other, although Jillian was nervous seeing Amy there, worried she would find out about her pregnancy. The MOA comes out to bring Jillian back to the exam rooms.

  MOA: Ms. Harrington? Dr. Ruggiero will be a few minutes for your visit, but we'll start with your regular prenatal testing

• Amy makes a phone call to another friend. “Did you know that Jillian was pregnant?? I thought Dr. Ruggiero only saw pregnant patients on Tuesdays, and I was right! She’s here seeing him today, and the nurse confirmed it.”

• What is wrong with this scenario?
• What could be done to prevent it?

Sign-In and Call Back Troubles

• Generally using a patient’s name with a sign-in sheet or calling them back to an exam room is considered an incidental disclosure.

• OCR states that the information disclosed must be “appropriately limited” (FAQ 199 – OCR website)

• Both sign-in sheet and staff could have disclosed info here

• Only use patient name and time when signing in, if doctor could give away additional information – or use other sign in mechanism (eg labels)

• When staff call patients back to exam rooms, call name only – do not give other information in range of other patients

• Have policies and procedures, provide training, and define consequences
Fax Machine Debacle

• A practice administrator notices that the fax machine that has been in use by the practice for the past several years is simply getting old and out of date. After exploring many options, he decides to move forward with an online fax service and sell the existing fax machine. The new owner of the fax machine finds a massive amount of PHI stored in the memory of the fax machine and not knowing what to do contacts the local Health Department, who in turn contacts the Office of Civil Rights

• Has the initial practice done something improper?
• What could have been done differently?

Fax Machine Debacle

• Fax machines, like computers and copiers have a 'hard drive' that stores information.

• Per the physical safeguards section of the Security Regs, prior to any re-use or disposal, electronic PHI must be removed from these devices (45 CFR 164.310(b)(2)

• In this instance, they did not wipe the fax machine clean prior to sale – they violated this section

• Be aware of all media in place that store information (fax, copiers, external hard drives, thumb drives, mobile devices, tablets, laptops, etc)

• Have policy and procedure in place to assure cleaning and proper disposal or re-use of these devices

• Track this procedure
Domestic Abuse Situation

• Judy was seen in the emergency room for a crush injury to her hand in the morning. She said that she accidentally closed her hand in the car door. Later in the day the local police arrived and wanted to speak with the physician and wanted copies of the medical record information. They received a report of the woman’s husband purposefully slamming her hand in the car door. The physician shared the information with the police officer, and they printed the medical record information for them. They did not have a subpoena or court order for this information, and there is no state law that requires disclosure of information in domestic abuse cases in this state.

• Is there an issue in this situation?

Domestic Abuse Situation

• This is a tricky situation
• Law enforcement can only have information in certain instances (partial list)
  – Subpoena, warrant, summons
  – Limited info to identify an individual
  – In cases when a patient is a victim of a crime and is incapacitated (under specific circumstances)
  – Of inmates under certain circumstances
  – Reporting required by law (state or otherwise)
  – Reporting related to specific criminal conduct on hospital premises
• In this case
  – Patient didn’t consent to disclosure
  – No state law requiring reporting
  – No subpoena or authorization from the patient allowing access to the information
  – Was the husband a possible serious threat to health and safety of wife?

• Training for all staff on release of information to law enforcement personnel
• No ROI from departments directly – go through ROI coordinator, Medical Records, HIM
• Review your state laws on situations of abuse. Some states do allow/require release of information in these situations
Dr. Bob at XYZ Medical Associates has a great small answering service that he’s been using for several years, and he’s been very happy with his service from them. They recently upgraded their phone system to an online system which allows the XYZ staff to access the information immediately online, and he can even check out the information from home online to see the calls coming into the practice. Unfortunately, their system wasn’t as well protected as they had thought, and all of XYZ Medical Associates (and their other clients) information ended up accessible via Google and other search engines online. It was discovered by a patient simply searching their name on Google. Dr. Bob says ‘This isn’t my problem, it’s the answering services problem. It says so in my contract with them. We don’t even have to have a Business Associate agreement with them because it’s not like that’s really medical record information.’

Is Dr. Bob right?

No, Dr. Bob is sadly wrong

They are violating HIPAA by not having a Business Associate agreement with their vendor with which they share PHI

They can also both be held liable for any civil monetary penalties resulting from the breach at the answering service

Review any situations where you share PHI with vendors on a regular basis
• Transcription
• Document storage/destruction
• Medical billing/repricing
• Utilization Review
• Health Information Exchanges
• Patient safety/Accreditation
• Many, many others

Be sure your BAA’s are up to date after the Omnibus rule, which altered the definition of BA and adjusted the requirements
**Training?**

• Tim is a nurse at the General Hospital Emergency Department. All staff at the hospital receive training on HIPAA Privacy and Security upon hire, or received training upon HIPAA implementation. Tim has worked there for many years, so received his training during the HIPAA rollout periods for privacy and security. There was a privacy breach at the hospital, and an external auditor was brought in to do a comprehensive risk assessment. As part of this assessment, the audit staff was simply walking around, talking to staff about various element of HIPAA.

  Auditor: Can I ask you about your HIPAA Training you’ve received?
  Tim: Sure, but it’s been some time
  Auditor: How long has it been since you received HIPAA Training in privacy or security?
  Tim: Gosh, that must have been like 10 years ago, when Suzie still worked in the Education Department
  Auditor: You haven’t received any of the educational bulletins since?
  Tim: Oh I get the e-mails, but we get so many e-mails I delete those. I don’t have time to read them

• Are there problems in this scenario?

**Training**

• HIPAA privacy and security each have requirements for training
  – Privacy – Train all new staff within a reasonable period after hire, train applicable staff on changes in the policies as affected
  – Security – Put in place a security awareness and training program, including periodic security updates
• By the ‘letter of the law’ they are likely not out of compliance, as long as they are training all of their staff upon hire, and those e-mails include security updates
• But is it effective??

• Examine your training plan and see where any holes may be
• Don’t just e-blast everyone or hang posters because it is easy. They become ignored easily
• Try to piggyback on other trainings – Nursing Ed, other annual mandatorics, etc – Get our there and share the HIPAA message, live if possible
Cell Phones

• Steve’s dad is in the hospital, so he and a buddy stop to see him before they go out for the big game. When they arrive, they find Dad has a roommate, and this roommate has a complex external fixation device on his leg, which Steve and his buddy are quite amused with. After sitting with Dad for a while, they decide to take off – but the roommate is sleeping so Steve’s buddy decides to grab a picture of the device and post it on Facebook. Little does he know that this picture is seen on FB by a family member, who becomes quite upset and threatens to sue for a HIPAA violation.

• Is this a HIPAA violation?

Cell Phones

• Actually, no – this is not a HIPAA Violation
• If a staff member took a photo and shared it, it could potentially be a HIPAA violation – in this case, the person taking and sharing the photo is not a ‘covered entity’
• However, can the hospital be held liable? Is anyone liable?
• HIPAA expects covered entities to implement reasonable measures to protect patient privacy

• Post signage indicating no cell phone use, especially in the ED
• Suggest staff be vigilant with regard to looking for this type of thing
• Be sure to include this in training, as staff use of cell phone/tablet cameras could be highly detrimental to the organization
Keys to Maintaining HIPAA Compliance

• Stick to your plan!
• Train, train, train
• Auditing and monitoring
• Watch the violations – they are telling
• Be open and helpful to staff – they are in the trenches

Questions??
Thank you for your time!!

Jillian Harrington
jharrington@hcpro.com
Regulatory Specialist
HCPro, Inc