Risks, Breaches, and Penalties

Tom Dumez, CHP, CSCS

Agenda

- Risks and/or potential risks
- Recent breaches
- Recent penalties

Common Risks

- Lack of a thorough risk assessment
- Driver error or record center employee error
- Data vault employee error
- Delivery errors
- Lack of good and sound (and practical) policies and procedures
- “The Fear of the Unknown” of owners
- Facility deficiencies
- “We have always done it that way” mentality
- Methods of delivery of scanned images
Risks...

- Employees: do they really know both the professional and personal implications of a breach?
- Are they aware of the damage that bad publicity can bring?
- Is there a ‘security’ culture?
- Are policies and procedures updated regularly, with privacy and security in mind?
- Does management convey a message that privacy and security do matter?
- Are any recent fines and penalties ever discussed, or do you avoid talking about these?
- Is your database really secure and does your RMS provider assume liability if their employee goes rogue?

Recent breaches (since May 2016)

- LinkedIn: exposed in May 2016
  - 117,000,000 emails, passwords and account numbers stolen by hackers in 2012
  - The information ended up being published online
  - LinkedIn responded by requesting passwords be changed and now offer 2-step verification

Democratic National Convention (June 2016)

- Thought to be of Russian origin
- Hackers were able to read all email and chat traffic
- Had access for about a year
- DNC Chairwoman lost her job over the scandal
- Officials suspect that employees were targeted with “spear phishing” emails
- Donors social security numbers and other personal information was hacked
- The DNC created a Cybersecurity Advisory Board—too little, too late
Others...

- Radiology Regional Center in PA: Reported a breach of 483,063 patients’ PHI. The breach did not involve a hacker in this instance, instead the data exposure occurred when patient files fell from a vehicle that was transporting the files to be incinerated.
- Ohio: Community Mercy Health Partners also reported a breach of more than 100,000 patient records. Files containing the protected health information of 113,528 patients were discovered in a recycling bin in Springfield, Ohio.
- The theft or loss of paper copies of patients PHI or devices containing ePHI accounted for 17.2% of breaches in June.

Data tape breaches

- TD Bank “lost or misplaced” unencrypted data tapes resulting in 265,000 PII records being breached.
- TRICARE “lost” unencrypted tapes and 4.9 million military clinic and hospital patients records were breached.
- McLean Hospital, a Harvard Medical School affiliate, “lost track” of 4 unencrypted backup tapes and 12,600 patient records were breached.
- Why do storage companies continue to accept unencrypted data tapes, or any other unencrypted media?
- Do we really believe that a contractual “opt out” will cover our behinds?

2016 Data Protection Benchmark Study

- The main purpose of this study was Data Loss Prevention and DLP solutions/programs
- Average cost of a breached medical record is now $355, compared to $322 since 2011
- 24% of increased data loss incidents are “employees’ use of social media”
- 14% of respondents do not provide security awareness training
- 12% of respondents do not know how to associate value to the data that they process or touch or see.
Recent Fines and Penalties

- North Memorial Health Care of MN:
  - Unencrypted laptop stolen from a BA (Accretive Health) employee’s car contained 9,497 patient records
  - No updated BAA
  - No current risk assessment or vetting of the BA
  - Fine: $1.55 million

- Catholic Health Care Services of the Archdiocese of Philadelphia:
  - Just 412 patient records
  - Caused by the theft of a CHCS-issued employee iPhone (unencrypted and not password protected)
  - Had no policies regarding mobile devices, no risk assessment, nor what to do in the event of a security incident
  - Fine: $650,000

- Care New England Health Systems (BA): provides centralized corporate support for its subsidiary affiliated covered entities, which include a number of hospitals and health care providers in Massachusetts and Rhode Island.
  - Women’s and Infants Hospital, a client (CE), lost unencrypted backup tapes containing the ultrasound studies of approximately 14,000 individuals that CNE loaded onto the tapes
  - Part of the C.A.P was to update BAA’s. Between 9/2014 until 8/2015, no updated BAA was in place.
  - Fines: CNE paid $400,000 and WIH paid $150,000
  - Updated C.A.P. with threats of even higher fines if more violations occur

- Raleigh Orthopaedic Clinic (NC) a BA: released the x-ray films and related PHI of 17,300 patients to an entity that promised to transfer the images to electronic media in exchange for harvesting the silver from the x-ray films. Raleigh Orthopedic failed to execute a business associate agreement with this entity prior to turning over the x-rays (and PHI).
  - CAP: revise its policies and procedures to: establish a process for assessing whether entities are business associates; designate a responsible individual to ensure business associate agreements are in place prior to disclosing PHI to a business associate; create a standard template business associate agreement; establish a standard process for maintaining documentation of a business associate agreements for at least six (6) years beyond the date of termination of a business associate relationship; and limit disclosures of PHI to any business associate to the minimum necessary to accomplish the purpose for which the business associate was hired.
  - Fine: $750,000
Advocate Health Care (AHC)

- Its subsidiary, Advocate Medical Group, a BA, had 4 unencrypted laptops stolen
- AMG sent AHC 3 breach notifications in 4 months
- The security lapses affected approximately 4 million AHC patients.
- OCR found that AHC failed to accurately assess potential risks to its IT systems and they also failed to ensure that its' BA's had adequate protections in place.
- CAP: AHC must conduct a full risk assessment (this alone implies that it did not previously do so) and create HHS-approved plans to secure its IT systems handling protected patient health information.
- Fine: $5.5 million

So, what do you do?

- Provide sound BAA's to your customers in an effort to lower liability
- Levels of liability should be the same in a BAA as what's in your storage and service agreement or contract
- Perform an accurate and totally objective risk assessment
- Provide relevant training to your staff and management
- Remember that you play an integral part in keeping data both private and secure and there are penalties for failure
- Privacy and security are not the same thing: you can have data privacy without having data security, but you can't have data security without data privacy

Questions?

Tom Dumez
President, Prime Compliance
Grand Rapids, MI
616.893.8243
tdumez@thehipaaman.com