Information Technology, Compliance and Human Resources Issues in Quality and Compliance

Melissa M. Zambri
Barclay Damon, LLP
mzambri@barclaydamon.com

BARCLAY DAMON LLP

Today's Agenda

- Everyone needs to get along.
- The players.
- The interactions.
- The personalities.
- Hot issues that require cooperation.

Personality Traits

- Extraverts (likes the outer world, energized by people, prefers talking)
- Introverts (internal focus, reflecting, prefer writing, likes quiet, likes time alone)
- Sensing – focuses on present, prefers tangible information, likes things orderly, practical, steady, orderly
- Thinking – logical consequences of decisions, weigh pros and cons, likes problem solving, likes to apply uniformity
- Judging – make decisions with information and as soon as possible, plan, likes closure

Your IT Department

- Handles high levels of job stress. Probably not a big department. With lots of users. With lots of different educational backgrounds and computer sophistication levels.
- Their systems play a key role, there is unrelenting demand that they work well and constant pressure for greater efficiency and faster turnaround – sometimes with no more money.
- They are required to continuously learn and evolve.
- They speak a unique language.

Your IT Department

- 90% of IT Directors reported that their health suffers as a result of their work – many citing impossible workload as a problem.
- Studies have shown that IT professionals tend to be much more introverted than extroverted – 25% of the general population is introverted; 67% of computer professionals are introverted.
- Then we require them to work on a team.

Your HR Department: Personality Traits

- Practical Expeditors
- ESTJ (extravert, sensing, thinking, judging)
- ESTJs thrive on order and continuity. Being extraverted, their focus involves organization of people, which translates into supervision. ESTJs are content to enforce "the rules," often dictated by tradition or handed down from a higher authority.

Your HR Department

- Stressors
  - They fire people . . . a lot.
  - They struggle to hire people . . . a lot.
  - They listen to everyone's complaints.
  - They deliver a lot of bad news.
  - They would prefer not to fire people; they would like to hire people; they would like to solve all of the complaints; and they would like to deliver good news, but that is not always in the cards and they do not control hardly any of it.
  - People are afraid of them.

Your Compliance Officer: Personality Traits

- Logical Assimilators
- ISTJ (introvert, sensing, thinking, judging)
- ISTJs are very responsible and reliable individuals who can be trusted to do their tasks well. As a result, they will usually excel in management where they are entrusted with responsibilities, expectations and objectives to meet.
- Also, they are able to work with huge amounts of data and are painstakingly accurate and methodical.

Your Compliance Officer

- Stressors
  - Why didn't we find that sooner?
  - Why didn't you know about that?
  - I thought we trained them?
  - That happened again?
  - When did that ADM come out?
  - Why did it come out yesterday but we were supposed to be following it two months ago?
  - Is it compliance, is it quality, is it an incident, is it all of the above?

Where Does Everyone Sit

- Is privacy with security under compliance?
- Is privacy with security under Information Technology?
- Is just security in information technology?

No completely common design.

The Intersection of HIPAA and HR

- HR Hires Employees
- Guess who causes almost all of your Medicaid compliance issues?
- Guess who causes the majority of breaches? Employees (and other workforce members) cause more breaches than technology
  - Most common issues
    - Impermissible use or disclosure (without authorization)
    - Lack of safeguards (mishandled)
    - Lack of access (refused access)
    - More than minimum necessary

The Intersection of HIPAA and HR

- The malicious insider - snooping
  - Neighbors
  - Family members
  - Friends
- Many people working in the industry do so because they are mission driven because of a family member or friend
- Personal factors
  - Your employees can be distracted, trusting, in a hurry, careless, which leads to tech support scams such as phishing
  - There is also anger/revenge, divided loyalty, adventure/thrill

The Intersection of HIPAA and HR

- Background checks – when are they done? Are they done in time?
- Hiring and the initiation of access to PHI
- Promotions/Demotions – changing access to PHI
- Firing – termination of access to PHI
- Performance Improvement Plans
- Training
- Application of Sanctions

All things employee-related touch on HR.

The Intersection of HIPAA and HR

- Is your initial training for employees on HIPAA good enough?
- Is it specific enough?
- Is it documented?
- Experian report from 2016
  - 2 out of 3 admit employees are weakest link
  - #1 security risk is employee carelessness or negligence
    - Unleashing malware, succumbing to phishing attacks
    - Using unapproved devices, e-mails, etc. to send sensitive information

The Intersection of HIPAA and HR

- Hiring and Access Procedure Controls
  - Workforce Clearance (background checks and credentials)
  - Job Descriptions with Assigned Security Responsibility
  - Minimum Necessary Access Based on Functional Role Responsibilities
  - Access Not Initiated Until Training Complete
  - Access Termination Procedures when Employee Leaves or Changes Jobs
  - Subcontractor Access Approval and Notice of Change in Contract Terms

The Intersection of HIPAA and HR

- Behavior Indicators of Insider Threats
  - Takes proprietary or other material home
  - Interest in matters outside of their duties
  - Unnecessary copying/printing
  - Remote access at odd times
  - Disregard of policy
  - Works off hours without authorization
  - Inappropriately seeks information
  - Unusual interest in personal lives of coworkers
  - Suspicious activities
  - Career disappointments
  - Concern over investigation

Who is Penalizing Who?

- HR involved in sanction decisions?
- Compliance involved in sanction decisions?
- How do you know discipline is consistent?

What is Compliance and Who Should Be Responsible?

- Should the endless variety of compliance challenges be housed together?
- But what happens if they remain in silos? What happens if they report to different supervisors?
- How many roles can you put in one person realistically?
- Do the missions ever conflict?

HR Challenges that Involve Compliance and IT

- Hiring good people
- Cyber breach concerns
- Alternative work arrangements
- Employee handbooks
- Credentialing
- Training

IT Challenges that Involve Compliance and HR

- Termination of Account Access
- Changes in Account Access Because of Role Based Change
- EMR – what it captures?
- EMR – how are people making mistakes?
- All things HIPAA Security, including Cyber Security

Compliance Challenges that Involve IT and HR

- HIPAA
- Training
- Documentation
- Discipline
- Disclosures

HIPAA Hot Topics

- Failure to perform privacy/security risk analysis
- Records on the road
- Laptops, thumb drives and encryption
- Knowing you have an issue and not fixing it
- Failure to report breaches timely
- Malware and ransomware
- Shared log ins
- Disposal of information
- Hybrid entities

Breach Notice

- ***NYS Attorney General Announces Settlement With Healthcare Services Company That Deferred Notice of Breach Of More Than 220,000 Patient Records*** - In October 2015, an unauthorized person gained access to confidential patient reimbursement data through the entity's website and downloaded records of 221,178 patients. The FBI opened an investigation. In January 2017, more than a year after the breach, the company provided notice to those affected in New York. The company claimed the delay was due to the investigation by the FBI, but the FBI never stated that a consumer notification would compromise its investigation.

HIV Information

- Hospital agreed to pay $387,200 for allegedly disclosing two patients' medical records to their employers without consent.
- Faxed the patient's PHI to his employer rather than sending it to the requested personal post office box.

HIV Information

August 2017 - Thousands of people with HIV received mailed letters from Aetna that may have disclosed their HIV status on the envelope. The letters, which Aetna said were sent to approximately 12,000 people, were meant to relay a change in pharmacy benefits. Text visible through a small window on the envelopes listed the patients' names and suggested a change in how they would fill the prescription for their treatment for the virus. Several of the affected individuals filed complaints with the Health and Human Services Office of Civil Rights or other state authorities.

Sole Failure of Timely Notification After Breach - $475,000 Penalty

- 45 days late notifying 836 patients.
- Lost 2013 surgery scheduling sheets.
- This was not the first time the provider was late with notices.
- Best practice – how long do you look for something?

Employee Access to ePHI

- HIPAA Violation: Memorial Healthcare System (MHS) reported to OCR that employees impermissibly accessed and disclosed to affiliated physician office staff the PHI of 115,143 individuals. It was discovered that the login information of a former employee of an affiliated physician's office was used from April 2011 to April 2012, without detection. This affected 80,000 individuals, despite the existence of workforce access polices and procedures.
- OCR Investigation Indicated MHS Failed To:
  - Implement procedures for reviewing, modifying and/or terminating a user's right of access.
  - Review records of information system activity by workforce users and users at affiliated physician practices even though previous risk analyses showed risk in these areas.
- Penalty: Settled potential HIPAA violations for $5.5 Million.
  - Implement a corrective action plan.
  - Agreed to complete a risk analysis and risk management plan.
  - Revise Polices and Procedures.

Disclosing PHI in Press Release

- HIPAA Violation: Memorial Hermann Health System (MHHS), a not-for-profit health system, disclosed PHI without patient authorization in a press release.
  - MHHS disclosed a patient's name in the title of a press release related to an incident involving a fraudulent identification card.
  - OCR initiated a compliance review after media reports of this incident.
  - It was found that MHHS also failed to timely document the sanctions against its workforce members related to the disclosure.
- Penalty:
  - Adopt a corrective action plan.
  - Settle potential violations: $2,400,000.

Board Responsibilities for HIPAA

- Former OCR Director Leon Rodriquez stated: “[s]enior leadership helps define the culture of an organization and is responsible for knowing and complying with the HIPAA privacy and security requirements to ensure patients’ rights are fully protected.”

Board Issues with Cyber Security

- **Wyndham** - (dismissed in October 2014), plaintiffs alleged that Wyndham's directors had breached their fiduciary duties with respect to Wyndham's data security and the associated risks. Points made in dismissing lawsuit - security policies, and proposed security enhancements were discussed in 14 board meetings; in at least 16 audit committee meetings; and that Wyndham hired a security consultant and began to implement the consultant's recommendations.
- In the **Target** case (dismissed in July 2016), the plaintiffs alleged that Target's directors and officers breached fiduciary duties by, among other things, failing to implement a system of internal controls to protect customers' personal and financial information, and failing to monitor internal control system. Favorable decision based upon the data security measures in place pre-breach, the changes enacted post-breach and management's reports to the board's audit committee and corporate responsibility committee covering the company's data security measures.
- In the **Home Depot** case (dismissed in November 2016), plaintiffs alleged that certain of Home Depot's directors and officers, including general counsel, breached their duties of care and loyalty, wasted corporate assets, and violated federal securities laws by, among other things failing to adequately oversee cybersecurity. In dismissing the case, the court observed "numerous instances where the Audit Committee received regular reports from management on the state of Home Depot's data security, and the Board in turn received briefings from both management and the Audit Committee."

Social Media: It is Everywhere and So Are Your Ex-Employees

Social Media HIPAA Violations

- Posting verbal “gossip” about a person served to unauthorized individuals, even if the name is not disclosed.
- Sharing of photographs, or any form of PHI without written consent from a patient.
- A mistaken belief that posts are private or have been deleted when they are still visible to the public.
- Sharing of seemingly innocent comments or pictures, such as a workplace lunch which happens to have visible files of those served underneath.

E-Mail Tips

Must you reply all?	Beware of groups	Before forwarding, CHECK WHAT IS AT THE BOTTOM OF THE CHAIN!
Write for publication	Should that be in writing?	Don’t forward privileged communication too far

Best Practice Policies

What do your employees agree to? Does it extend beyond their employment?	Social Media?	Device policy?
Bringing PHI out of office?	Using home computer?	Staff understand what they can and cannot discuss with ex-employees?

Best Practice Policies

Policies and procedures stale?	Minimum Necessary – Significant violators? Auditing? Training?	Is your training stale?
Board informed? Trained?	Photos? Development Office Trained?	Policies for HIV? Required to be updated annually in New York.

Conclusion and Questions

Thank you for your time.