HIPAA: PROTECTING CLIENT INFORMATION POST-AFFORDABLE CARE ACT

Sponsor: Young Lawyers Division
CLE Credit: 1.0
Thursday, June 18, 2015
10:50 a.m. - 11:50 a.m.
Thoroughbred 4
Lexington Convention Center
Lexington, Kentucky
A NOTE CONCERNING THE PROGRAM MATERIALS

The materials included in this Kentucky Bar Association Continuing Legal Education handbook are intended to provide current and accurate information about the subject matter covered. No representation or warranty is made concerning the application of the legal or other principles discussed by the instructors to any specific fact situation, nor is any prediction made concerning how any particular judge or jury will interpret or apply such principles. The proper interpretation or application of the principles discussed is a matter for the considered judgment of the individual legal practitioner. The faculty and staff of this Kentucky Bar Association CLE program disclaim liability therefore. Attorneys using these materials, or information otherwise conveyed during the program, in dealing with a specific legal matter have a duty to research original and current sources of authority.

Printed by: Evolution Creative Solutions
7107 Shona Drive
Cincinnati, Ohio 45237

Kentucky Bar Association
# TABLE OF CONTENTS

The Presenter .......................................................................................................................... i

HIPAA – Protecting Client Information Post-Affordable Care Act ........................................ 1
  Introduction......................................................................................................................... 1
  HIPAA Basics .................................................................................................................... 1
  Today's Threats ................................................................................................................ 9

Why Should Lawyers Care about HIPAA/THITECH and the Regulations? ............................... 11

Protecting Client Data ........................................................................................................ 15

Where It Could Go Wrong .................................................................................................. 22

Points of Consideration ...................................................................................................... 24
LISA ENGLISH HINKLE is a member of McBrayer McGinnis Leslie & Kirkland in Lexington and practices in the area of health care law. She received her B.A. from the University of Kentucky and her J.D. from the University of Kentucky College of Law. Ms. Hinkle is a member of the Fayette County, Kentucky, and American Bar Associations, American Health Planning Association, The Fellows of the American Bar Foundation, and the American Health Lawyers Association.
I. INTRODUCTION

The Health Insurance Portability and Accountability Act ("HIPAA") imposes substantial duties on entities and their associates who come into contact with private health information. The Patient Protection and Affordable Care Act made some changes to HIPAA regulations and practices, but it wasn't until the Department of Health and Human Services issued the final HIPAA Omnibus Rule in 2013 that major changes to HIPAA took effect. These materials will address current duties of covered entities and business associations under HIPAA, addressing basic HIPAA provisions, current threats to protected health information, application of HIPAA to law firms/concerns for lawyers, protection of client data, potential penalties, and points to consider when dealing with HIPAA.

II. HIPAA BASICS

A. Glossary and Language

1. Office for Civil Rights (OCR): Tasked with overseeing and enforcing HIPAA.

2. Privacy Rule: 45 C.F.R. §164.500 et seq.


5. Covered Entity (CE): Health care provider, health plan (e.g., insurance), or health care clearinghouse.

   Examples: hospitals, nursing homes, surgery centers, physician offices, dentists, health insurance companies.

6. Protected Health Information (PHI): Any information relating to past, present, or future physical or mental health or condition of an individual.

   a. Medical records.

   b. Any information that identifies an individual as a patient.

   c. Correspondence.

   d. If in doubt, treat it as PHI.

7. Use (internal) vs. disclosure (external).
8. Business Associate (BA).

a. A person who creates, receives, maintains, or transmits PHI on behalf of a covered entity or organized health care arrangement for a function or activity regulated by HIPAA.

For example, claims processors or administrators; data analysts, processors or administrators; utilization reviewers; quality assurance agents; patient safety organizers; billers; benefit managers; practice managers; re-pricers.

b. A person who provides any of the following services to or for a covered entity or organized health care arrangement where the provision of the service involves the disclosure of protected health information from the covered entity or the organized health care arrangement or from another Business Associate: For example, legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; financial.

c. A subcontractor (Sub-K) that creates, receives, maintains, or transmits protected health information on behalf of the Business Associate.

d. BA status is "definitional":

   i. If it does what a BA does, it's a BA.
   ii. Knowledge or intent of CE or BA are irrelevant.
   iii. Presence or absence of a contract is irrelevant.

e. Key BA obligations.

   i. Exposed to potential federal criminal penalties for violation of HIPAA.
   ii. Subject to regulatory jurisdiction of OCR and state attorneys general.
   iii. Required to cooperate with OCR investigations of CE and BAs.
   iv. Exposed to potential civil monetary penalties for violation of HIPAA.
   v. Can be exposed to private tort actions by individuals harmed by BA failure to comply with HIPAA.
Example:

Walgreens Indiana Verdict: $1.44 million – Pharmacist's husband had fathered a child with a customer. The pharmacist then allegedly looked up the customer's prescription information and shared it with her husband, who then used it to pressure the customer into not asking for child support.

vi. Examples of scenarios that may trigger BA obligations.

a) Physician contacts you to defend her in a medical malpractice action where you will need to review her records.

b) Hospital contacts you to provide advice regarding an unpaid patient bill.

c) Nursing home asks you to interview residents regarding an adverse incident.

d) Billing company calls with a regulatory question and asks you to review claims.

e) Healthcare provider wants you to pursue collection of unpaid claims.

vii. Examples of scenarios that probably don't trigger BA obligations.

a) Pharmacy asks you to review its policies and procedures (No PHI).

b) Employer asks you to help determine whether an employee is entitled to family medical leave.

c) A life insurance company or workers' comp plan asks you to defend it in a suit brought by an insured.

d) An individual injured in an automobile accident asks you to file a lawsuit.

e) An estate planning client asks you to draft a health care power of attorney (No PHI).

---

f. General rule: A Covered Entity may disclose PHI to a Business Associate in accordance with a Business Associate Agreement (BAA).

i. CE is required to have a BAA with the Business Associate.

ii. Things a BAA must address:

   a) Establish the permitted and required uses and disclosures of PHI by BA.

   b) Provide that BA will not use or further disclose the information other than as permitted or required by the contract or as required by law.

   c) Require the BA to implement appropriate safeguards to prevent unauthorized use or disclosure of the PHI, including compliance with the Security Rule for PHI.

   d) Require reporting to CE any improper use or disclosure, including breaches.

   e) Require BA to make PHI available for access and amendment, and require information for accounting.

   f) Require Privacy Rule compliance, to the extent applicable.

   g) Require BA to make books and records available to HHS – Don’t forget about the attorney/client privilege!

   h) Require return or destruction of PHI at termination, if feasible.

   i) Require the BA to ensure that subcontractors agree to the same restrictions and conditions.

   j) Authorize termination of the contract by CE if the BA violates a material term.

iii. BAA AGREEMENTS INVOLVE SERIOUS ETHICAL CONSIDERATIONS FOR LAWYERS.

g. BA requirements for response and reporting of security incidents.
i. A "security incident" includes "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

ii. BA must "[r]eport to the covered entity any security incident of which it becomes aware."

iii. The BA must identify and respond to suspected or known security incidents and document the security incidents and their outcomes.

iv. The BA must report security incidents to the covered entity (including those reported to it by its subcontractors).

v. The BA must mitigate, to the extent practicable, harmful effects of security incidents that are known to the business associate.

vi. The BA must conduct a risk assessment to determine the probability that the information was compromised in view of the security incident.

vii. Not all security incidents rise to the level of a breach, but you may be able to prevent a breach by blocking unsuccessful attempts to infiltrate your systems or exfiltrate your data.


a. A "breach" is generally defined as an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E [the Privacy Rule].

b. Under the HIPAA Omnibus Rule, the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E [the Privacy Rule] is generally presumed to be a breach unless the CE or BA, as applicable, demonstrates that there is a low probability that the PHI has been compromised.

c. Exclusions from "breach."

i. Good faith: "The acquisition, access, or use by a workforce member or person acting under the authority of a . . . BA was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part."
ii. Inadvertent disclosure: "Any inadvertent disclosure by a person who is authorized to access protected health information at a CE or BA to another person authorized to access protected health information at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part."

iii. Good faith belief not reasonably able to retain: A disclosure of protected health information where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

iv. Factors for assessing risk – the risk must be assessed using at least the following four factors:
   a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   b) The unauthorized person who used the PHI or to whom the disclosure was made;
   c) Whether the PHI was actually acquired or viewed; and
   d) The extent to which the risk to the PHI has been mitigated.

B. HIPAA Privacy Rule

1. General rule: A CE (or BA) may not use or disclose an individual's PHI without that individual's authorization, except as permitted by HIPAA.
   a. Establishes rules on how CEs (and their BAs) may use and disclose PHI.
   b. Grants patients certain rights with regard to their own PHI.
   c. Imposes requirements on CEs to safeguard the privacy of PHI.

2. Exceptions.
   a. Disclosures to the Individual & HHS.
b. Disclosures for Treatment, Payment, & Health Care Operations (TPO Disclosures).

c. Disclosures to Personal Representatives.

d. **New Rule in the Omnibus Rule – CE must comply with HIPAA for a deceased individual for fifty years after the individual's death.**

e. Disclosures Requiring an Authorization.

f. Disclosures for Facility Directories & Family.

g. Disclosures for Public Health, Oversight, Legal.

3. Administrative requirements.

a. Personnel designations.

b. Training.

c. Safeguards.

d. Handling individual complaints.

e. Sanctions.

f. Mitigation of violations.

g. Refraining from intimidating or retaliatory acts.

h. Prohibition on waiver of rights to complain to HHS.

i. Policies and procedures; documentation.

C. HIPAA Security Rule

1. Requires CEs/BAs to protect the storage and transmission of electronic PHI.

2. Requires CEs/BAs to implement *administrative, technical and physical safeguards* to protect electronic PHI.


   a. When is it electronic?

   b. Print electronic material.
5. HIPAA security basics.
   b. Physical safeguards (45 C.F.R. §164.310) – Four standards.
   d. Documentation (45 C.F.R. §164.316).

D. When Does HIPAA Apply?
   1. Usually applies to:
      a. Patient information from a hospital.
      b. Medical files from a physician.
      c. Enrollee’s information from a health plan.
      d. Nursing home resident's records.
      e. Claims records from a health care billing company.
      f. Employment records???
   2. Usually doesn't apply to:
      a. OSHA records.
      b. Life insurance.
      c. An individual client's personal medical data (e.g. medical malpractice plaintiffs or estate planning clients).
      d. Education/FERPA records.
      e. De-identified information.
      f. Employment/personnel records???
III. TODAY'S THREATS

A. Medical Identity Theft
   1. "Use of individual's name and personal identity to fraudulently receive medical service, prescription drugs and goods, including attempts to commit fraudulent billing."
   2. Increased prescription drug fraud.

B. Identity Fraud
   1. One in four chance of being a victim of identity fraud as a result of a data breach.
   2. Consequences for victim range from loss of income to loss of life.
   3. It is difficult to correct errors due to identity fraud.

C. PHI Black Market
   1. Personal Health Information ("PHI") can be monetized twenty to fifty times more easily than personal financial information ("PFI").
   2. Value of PHI is up to fifty times greater than the value of a SSN.
   3. Value ranged from $500 to $1,500 per harvested PHI.

D. "Advanced Persistent Threat" ("APT")
   1. Targeted attack to gain an inside foothold.
      a. EHR systems.
   2. Entry tactics include:
      a. Targeted emails or "spear phishing."
      b. Mobile devices.
      c. Network devices that are not properly secured.
   3. Healthcare information is more vulnerable than other types of information.
      a. Lack of situational awareness.
      b. Not understanding entry tactics.
c. Time and resources needed to secure PHI.

d. Changes in technology.

E. You!!

1. Authorized user lack of awareness, for example:
   a. Unencrypted CD containing mental health records handed to consultant.
   b. Paper records placed in a dumpster.
   c. Leaving boxes of medical records "unattended and accessible."
   d. Unauthorized employees looking at medical records.

2. PHI can be inappropriately removed, transferred or sent out.
   a. Postal main.
   b. Email.
   c. Instant messaging.
   d. File transfers through Drop Box, etc…

3. Lost and misplaced devices are the leading cause of concern.
   a. Thumb drives.
   b. CDs.
   c. Any device that has access to the firm's network or your work email.
      i. Laptop.
      ii. iPad.
      iii. Cell phone.

4. Insecure or improper destruction of PHI.
IV. WHY SHOULD LAWYERS CARE ABOUT HIPAA/HITECH AND THE REGULATIONS?

A. Lawyers Representing Clients Often Must Have Protected Health Information to Perform Their Jobs

B. Lawyers Qualify as BAs when a Client Discloses/Authorizes Use of Protected Health Information

1. Creating, receiving, maintaining or transmitting protected health information on behalf of a "covered entity" client.

2. Providing services to a client that is a BA of other covered entities can also trigger HIPAA obligations (software vendors, accountants, consultants, third party administrators).

3. Receiving a client's medical records from a covered entity.

C. The Omnibus Final Rule Makes BAs Directly Liable for:

1. Impermissible uses and disclosures of PHI.

2. Failure to notify CE when PHI is lost or inappropriately accessed.

3. Failure to provide electronic PHI when requested.

4. Failure to disclose PHI when requested by CMS to investigate BA's compliance.

5. Failure to provide accounting of disclosures.

6. Failure to comply with the Security Rule.

D. What HIPAA Requires of Law Firm BAs

1. Post Omnibus Rule: direct regulatory obligations from all BAA.

   a. Full compliance with the Security Rule.

   b. Use and disclose PHI only as permitted by the upstream BAA.

   c. Comply with the Minimum Necessary Rule.

   d. Notify the CE in case of a security breach.

   e. Provide access to a copy of the electronic PHI in their possession to the CE or individual, as specified in their upstream BAA.
f. Provide the information needed for an accounting of disclosures.

g. Provide access to their records to OCI to investigate the BA’s compliance.

h. Requirement for “assurances” from any Service Provider.

i. Requirement for BAA with any Subcontractor.

j. Requirement for BA with CE of Upstream BA (as applicable). Many BAA requirements are redundant to regulatory requirements.

2. Checklist for lawyers as BAs.

a. Appoint a HIPAA Security Officer.

b. Identify clients to whom the firm is a BA.

c. Determine whether firm receives, transmits, or maintains PHI.

d. Conduct a risk analysis/assessment.

e. Draft and implement policies, procedures, and other documentation/practices required by the Security Rule.

f. Draft policies and procedures relating to BA obligations.

   i. Reporting breaches of unsecured PHI.

   ii. Reporting unauthorized uses and disclosures.

   iii. Responding to requests for access/accounting.

   iv. Identifying PHI.

   v. Determining when BAA and subcontractor agreements may be required.

   g. Revise/draft BAA and subcontractor agreement templates to reflect HITECH/Omnibus Rule changes.

   h. Keep PHI secure (limit off-site uses, keep in files instead of out in the open, don’t talk about PHI in public, address encryption).

   i. Disclose PHI only to those who need to know in order to perform their job function.
j. Train law firm personnel on your HIPAA policies and procedures.

k. Provide periodic security reminders.

l. Ensure that third parties to whom you disclose PHI have executed a BAA subcontractor agreement (if necessary).


E. HITECH Drastically Changed the Enforcement and Auditing Authority of Office of Civil Rights ("OCR")

1. HIPAA Omnibus Rule formalized HITECH Act requirements and underscores the need for strengthening HIPAA compliance.

2. Numerous $100k+, even million-dollar penalties.

3. Not limited to big institutions – also includes smaller groups.

4. Strengthening audit program.

5. Criminal penalties exist.

6. State Attorneys General can bring civil action.

7. No private right of action for HIPAA damages, but may be state tort liability.

8. As of February 28, 2014:

   a. Complaints filed = 92,975.

   b. Cases investigated = 32,227.

   c. Cases with corrective action = 22,222.

   d. CMPs and resolution agreements = >$16 million.

   e. Increased authority to issue CMP’s directly against BAs.

9. OCR Phase 2 of HIPAA Audit Program.

   a. 2014 – OCR announced that it is gearing up for second round of audits by starting with a survey of 1200 organizations including 400 BAs.

      Survey: "gather information about the respondents to enable OCR to assess the size, complexity and fitness of a respondent for an audit."
b. Audits started taking place in October 2014 and will continue through June 2015.

c. Unlike Phase 1, which focused on covered entities, Phase 2 will focus on both covered entities and business associates.

d. OCR will notify and send data request to 350 covered entities this fall. The data request will ask the covered entities to identify and provide contact information for their BAs. The OCR will select the BAs for participation in the Phase 2 audits from this pool.

e. Penalty rubric:

i. Tier 1.

a) BA's culpability level – Did not know and could not have known of the HIPAA violation.

b) Penalty per incident: $100-$50,000.

ii. Tier 2.

a) BA's culpability level – Knew, or would have known through reasonable due diligence that an act or omission violates HIPAA, but did not act with willful neglect.

b) Penalty per incident: $1,000 - $50,000.

iii. Tier 3.

a) BA's culpability level – Acted with willful neglect, but corrected the violation within thirty days.

b) Penalty per incident: $10,000 - $50,000.

iv. Tier 4.

a) BA's culpability level – Acted with willful neglect and took no corrective actions within thirty days.

b) Penalty per incident: $50,000.

v. Timely corrective action is an affirmative defense to Tier 1 and Tier 2 violations.
V. PROTECTING CLIENT DATA

A. Safeguards for Client Data

1. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

2. Security encompasses all of the administrative, physical, and technical safeguards for an information system through the use of people, processes, and technology.

a. Administrative safeguards for client data.

   i. Implement policies and procedures to prevent, detect, contain, and correct security violations: risk analysis, risk management, sanction policy, and information system activity review

   Risk analysis – "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information . . . ." and manage the risks as reasonable and appropriate for your organization.

   a) Identify all systems that create, receive, maintain, or transmit ePHI.

   b) Identify and document potential threats and vulnerabilities.

   c) Assess current security measures.

   d) Determine the likelihood of a threat occurrence.

   e) Determine the potential impact of a threat occurrence.

   f) Determine the level of risk.

   g) Finalize documentation.

   h) Periodically review and update the Risk Analysis.

   i) Typical areas addressed in a law firm's Risk Analysis.
1) End points: laptops, desktops, and mobile devices.

2) Fax machines.
   A) Internal hard drives.
   B) Are the faxes digitized (and how/where does the data flow)?

3) Copy services: BAA necessary?

4) Copiers.
   A) Internal hard drives.
   B) Are the copies digitized (and how/where does the data flow)? PDF/fax capabilities (same question)?

5) Email providers.
   A) Security.
   B) Used for transmitting PHI (probably even if you don't want to, clients will send)?
   C) Is BAA in place?
   D) Encryption/secure portal solution?

6) Dictation machines.

7) Website intake forms: potential clients who send PHI.

8) USB, DVD, hard disks, other portable media: allow, use and/or encrypt?

9) Shredding companies: BAA in place?

10) Cloud storage (Dropbox, others) and document management.
    A) Security?
B) BAA in place?
C) Encryption in transit/at rest?

11) Video recordings.
12) Experts.
13) Court reporters.
14) Expert reports.
15) Practice management software.
16) Third party IT company: BAA in place?
17) Paper files.
   A) How are they handled onsite?
   B) Offsite storage and BAA?
   C) Overall facility physical security.
18) WiFi access.
19) Internal servers.
   A) Firewalls/security/monitoring.
   B) Physical controls (locked server room).
   C) Outside access capabilities (VPN, other tunnels).
20) Voicemail provider.
21) How clients send PHI to you?
22) How you send it out?
23) Personnel risks (and training).
   A) User account removals (could be multiple types of access – mobile, server, email, cloud).
B) Apply appropriate sanctions against workforce members regarding violations of organization's policies and procedures.

C) Information system activity review (e.g., audit logs, access reports, and security incident tracking reports).

ii. Implement ongoing monitoring and evaluation plans (Are the policies, procedures, and plans adequate?) Should such plans and procedures be revised based upon experience?

iii. Have written contracts (or other written arrangements) with downstream subcontractors, as applicable.

iv. Secure the human element: have controls in place prior to employment, during employment, and after termination or other change in employment).

a) Acceptable use policy which sets forth what authorized users can and cannot do with IT assets, mobile devices, etc.

b) Security awareness and training for new users and continuing users regarding policies and procedures.

v. Have appropriate sanctions and other measures in place in the event of a violation of policies and procedures. Know what is going on in real-time (be proactive).

vi. Inventory who has access to your data.

b. Physical safeguards for client data.

Be concerned not only with unauthorized access by outsiders, but also with insiders. The insider is someone we have given legitimate access to information, systems, and resources.

The insider may be an employee, intern, volunteer, security guard, janitor, contractor, consultant, etc. – essentially, anyone with inside (and authorized) access.
c. Technical safeguards for client data.

i. Access control for electronic information systems. Implement technical policies and procedures for information systems with regard to authorized users and software programs.

ii. Keep user and transaction logs and analyze these logs. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems.

iii. Maintain data integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

iv. Authentication: Implement procedures to verify that a person or entity seeking access is the one claimed.

v. Transmission security: Implement technical security measures to guard against unauthorized access to information that is being transmitted over a network.

vi. Practical tips.

a) Make sure network infrastructure is secure (e.g., wireless networks, routers, firewalls, etc.).

b) Disable, as appropriate, automatic "joining" of networks (e.g., evil twin).

c) Wired communications are generally more secure than wireless communications.

d) Consider restricting access to websites and installation/use of certain applications (e.g., peer to peer sharing sites, etc.).

e) Encrypt whenever possible data at rest, data in motion, and archived data.

f) Ensure secure remote access from home or on the road and mobile device security too.

g) Ensure that the users accessing your resources are who they say they are.
h) Use unique user IDs (or other means of user identity proofing) for each user.

i) Use complex passwords or an appropriate alternative for authentication.

j) Protect documents and storage media (including flash drives, backup tapes, mobile devices, and cloud) from unauthorized disclosure, modification, removal, and destruction.

k) Ensure that all information systems and storage media are appropriately disposed of.

This may even include photocopiers, mobile devices, and other information systems which are used either on premises or off premises (e.g., laptop computer used for work from home).

B. Failure to Secure Client Data

1. The data security breaches at Anthem, Sony, Home Depot, Target, and Premera Blue Cross serve as stark reminders that all organizations, even the ones with most secure networks, face significant cybersecurity threats and challenges that could cause substantial financial costs and reputational damage.

   a. Anthem: On February 4, 2015, the second largest healthcare insurance company in the U.S., Anthem Inc., reported a data security breach affecting 78.8 million customers.

      i. In January, hackers sent phishing emails to employees that allowed the hackers to steal at least five employees’ network credentials, usernames, and passwords. These hackers even obtained the information belonging to the system administrator account. The system administrator did not notice the breach until someone used his access codes and information and was inside the system.

      ii. Although the final report on the Anthem data breach has not yet been issued, the fact that the hackers obtained five sets of access keys or credentials (log in and passwords) from authorized users indicates how dangerous an innocent mistake, such as opening a phishing email, can be to an entire data system.
b. Target: During the 2013 holiday shopping season, Target suffered a substantial security breach of its credit and debit card system that impacted 70 million customers.

i. The hackers obtained access to customer information through hacking Fazio Mechanical, a refrigeration contractor of Target. An employee of Fazio Mechanical opened a malicious phishing email that installed a piece of malware, which recorded login credentials and gave the hackers access to a portal into Target's internal systems. The hackers used the portal access to gain control of Target's servers. Thus, the hackers gained access to Target's system by hacking into the system of an outside contractor and using that contractor's access information to get into Target's system.

ii. The Target breach indicates that CEs must closely monitor the security breaches of their contractors, because those outside security breaches can give hackers an indirect access point or back door into the CE's system.

c. Premera Blue Cross: An attack on the health insurer's systems began on May 29, 2014, but wasn't discovered until January 29, 2015. Up to 11 million customers, with digitized records going back to 2002, may be affected.

i. Unlike with Anthem or Target, potential ePHI, such as claims and clinical information, may have been breached as well.

ii. Malware got into the system's computers, but they still aren't sure how.

2. Lessons learned.

a. Train employees to detect scams and report possible scam emails.

b. Test employees' ability to recognize scams.

c. Monitor employee access to identify stolen access info.

d. Limit third party and contractor's employees' access to system.

e. Monitor breaches of contractors to avoid back door entry.
f. Require that contractors assess and closely monitor security risks.

g. Require immediate notification of any security breach of a contractor’s system.

VI. WHERE IT COULD GO WRONG

A. Civil Monetary Penalties

"A complaint alleged that a law firm working on behalf of a pharmacy chain in an administrative proceeding impermissibly disclosed the PHI of a customer of the pharmacy chain. OCR . . . found no evidence that the law firm had impermissibly disclosed the customer's PHI. However, the investigation revealed that the pharmacy chain and the law firm had not entered into a Business Associate Agreement . . . Without a properly executed agreement, a covered entity may not disclose PHI to its law firm. To resolve the matter, OCR required the pharmacy chain and the law firm to enter into a Business Associate Agreement."

– Pharmacy Chain Enters into Business Associate Agreement with Law Firm, hhs.gov Health Information Privacy website

Key concepts:

1. May be imposed upon CEs (your client) and BAs (you), and upon both if both are found at fault.

2. Calculated at one violation per failure to comply with any "requirement" (positive or negative obligation) of the Privacy or Security Rule.

3. One failure can violate more than one requirement.

4. "Continuing violation:" Any requirement whose failure "continues" from the time at which the violation first began. Counted at one violation per day, for each day it "continues."

5. Foundational violation: Any failure to comply with a requirement which causes failures to comply with other requirements.

6. Potential CMP amounts.

a. Violation not known (despite due diligence): $100/violation to $25,000 calendar year maximum.

b. Violation due to "reasonable cause:" $1,000/violation to $100,000 calendar year maximum.

c. Violation due to "willful neglect:" Increased to $500,000/violation to $1.5 million calendar year maximum.
B. Major Client Financial and Reputational Harm

**M.O. v. Internal Medicine Associates, Inc.** (Monroe County Circuit Court, Indiana 2013).

1. Healthcare provider retained attorney to collect patient debt.

2. Attorney's public court filings included patient name, contact information, Social Security number and positive HIV status, unsealed for six months. No evidence information was ever viewed.

3. Medical review board concluded health care provider violated the standard of care for patient privacy.

4. Jury awarded patient $1.25 million for emotional distress, embarrassment based on negligence claim.

C. Enforcement and Penalties

1. HHS Office of Civil Rights (OCR) may investigate compliance.
   a. Based on complaint by anyone – whistle blower, adversary, etc.
   b. On OCR's own initiative; "Audit Program" contemplates audit of 1,200 CEs and BAs.
   c. Every notification of breach affecting 500 or more individuals is reviewed for potential investigation.
   d. Notification of breach affecting fewer than 500 individuals may also trigger investigation.

2. Scope of OCR investigation.
   a. Essentially unlimited as relevant to HIPAA/HITECH compliance.
      i. Privacy and security policies and procedures, security analyses, responses to individual requests and complaints, incident responses and breach assessments, etc.
      ii. Documentary records, interviews with appropriate personnel, etc.
b. CEs and BAs have regulatory obligations to maintain documentation, cooperate with investigations.

Cignet Health: Failure to cooperate with OCR investigation grounds for $3 million civil monetary penalty.

VII. POINTS OF CONSIDERATION

A. A Firm's Most Critical Asset Is Information and Data

B. The HIPAA Security Rule was Designed to Align with the HIPAA Privacy Rule

1. Neither can be viewed in a vacuum.


C. Do Not Neglect the Three Parts of the Security Triad (CIA)

1. Confidentiality → protection of the patient's medical record.

2. Integrity → the authenticity, accuracy, and completeness of the patient record.

3. Availability → access to the patient record.