HIPAA BASICS

KURT BRATTEN, ESQ.

O'CONNELL AND ARONOWITZ, P.C.

HIPAA Omnibus Final Rule
Implements HITECH Act - January 25, 2013

- Finalized the 2009 Interim Rules and 2010 HITECH Proposed Rule
- Final Rule was effective March 26, 2013; enforceable on September 23, 2013
- Extends HIPAA compliance directly to business associates
- Fundamentally alters the HIPAA breach notification standard
  - "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information"
  - Under the Omnibus Rule, a breach is presumed unless the Covered Entity can demonstrate a low probability the PHI was compromised

HIPAA Omnibus Final Rule
Implements HITECH Act - January 25, 2013

- Amends security rule and imposes new privacy rule requirements, such as:
  - Additional requirements for Notice of Privacy Practices
  - New standards for the Sale of PHI and its use in Marketing
  - Patients have enhanced rights to restrict the use and disclosure of their PHI
- Business Associates are now liable for HIPAA violations, including:
  - violations of Privacy and Security Rules
  - failing to meet reporting obligations to Covered Entity
- Business Associates are liable for subcontractors if they are agents
- Business Associate Agreement liability

HHS OFFICE FOR CIVIL RIGHTS GUIDANCE

- Reporting and Monitoring Cyber Threats
- Phishing
- Cyber Extortion
- Contingency Planning
- Guidance on Software Vulnerabilities and Patching
- Disposing of Electronic Devices and Media
- Workstation Security: Don’t Forget About Physical Security
- Risk Analyses vs. Gap Analyses

HHS OFFICE FOR CIVIL RIGHTS ENFORCEMENT ACTIVITY

- Oct. 2018 – Anthem agrees to pay $16 million fine to resolve the largest breach in U.S. history. Breach caused by a series of cyberattacks that exposed the ePHI of nearly 79 million people.
- Sept. 2018 - Boston Medical Center, Brigham and Women's Hospital, and Massachusetts General Hospital were fined $999,000 for the unauthorized disclosure of patients' Protected Health Information during ABC television filming.
- Court appointed receiver awarded $100,000 to OCR from defunct medical record storage and delivery provider, Filefax. Incident involved unauthorized person and leaving records containing PHI of 2,150 persons in an unlocked truck.

RISKS OF NON-COMPLIANCE

HIPAA Violations Can Be Criminal

If PHI is obtained or disclosed without authorization knowingly, under false pretenses or with intent to sell, transfer, or use PHI for commercial advantage, personal gain or malicious harm, this is a federal crime.

Covered Entities Must Self-Report Breaches

By law, Business Associates must report breaches to Covered Entities and Covered Entities must self-report HIPAA breaches of unsecured PHI to the individual affected, HHS, and, when the breach affects 500 or more individuals, to the media.

Civil Penalties Are Substantial and Mandatory for Willful Neglect

Office for Civil Rights is required to impose HIPAA penalties if the Covered Entity or Business Associate acted with willful neglect (i.e., with "conscious, intentional failure or reckless indifference to the obligation to comply" with HIPAA).

Additionally, HITECH allows State Attorneys General to bring civil actions for violations of the Privacy Rule and Security Rule (civil damages, attorneys fees and costs recoverable).

CIVIL PENALTIES UNDER HIPAA

CONDUCT OF COVERED ENTITY OR BUSINESS ASSOCIATE	PENALTIES
Did not know of violation and, by exercising reasonable diligence, would not have known	$100 to $50,000 per violation; Up to $1,500,000 per identical violation per year
Violation is due to reasonable cause and not willful neglect	$1,000 to $50,000 per violation; Up to $1,500,000 per identical violation per year
Violation is due to willful neglect but is corrected within 30 days after covered entity knew or should have known of violation	Mandatory fine of $10,000 to $50,000 per violation; Up to $1,500,000 per identical violation per year
Violation due to willful neglect and not corrected within 30 days after covered entity knew or should have known	Mandatory fine of at least $50,000 per violation; Up to $1,500,000 per identical violation per year

RECENT DEVELOPMENTS

CRIMINAL ATTACKS AND INSIDER THREATS PREDOMINATE:

- Over 5 million healthcare records were exposed or stolen in 2017
- In 2017 in NY, hacking accounted for over 44% of breaches and 94% of the total personal information exposed. Employee negligence (a combination of inadvertent exposure of records, insider wrongdoing, and lost devices or media) accounted for 25% of reported breaches. *Information Exposed: 2017 Data Breaches in New York State*, NYS Attorney General's Office.

RECENT DEVELOPMENTS

CRIMINAL ATTACKS AND INSIDER THREATS PREDOMINATE:

- Malicious or criminal attacks continue to be the primary cause of data breaches. 52% of incidents involved a malicious or criminal attack, 24% of incidents were caused by negligent employees, and another 24% were caused by system glitches (including IT and business process failures). Malicious attacks are also the most costly type of breach. *2017 Cost of Data Breach Study: United States*, Ponemon Institute.

RECENT DEVELOPMENTS

THE RISE OF RANSOMWARE:

- Ransomware was the most prevalent form of malware in 2017. *2018 Data Breach Investigation Report*, Verizon.
- Worldwide, ransomware attacks rose 350% in 2017. *NTT Security 2018 Global Threat Intelligence Report*, Dimension Data.
- Numerous healthcare providers experienced ransomware attacks in 2017 and 2018.

RECENT DEVELOPMENTS

COSTS OF BREACHES ARE HIGHER IN THE HEALTHCARE INDUSTRY:

- Ponemon Institute estimates that the average cost of a breach in the United State is $7.91 million
- Ponemon's research show that the highest data breach resolution costs are for healthcare data breaches, which typically cost an average of $408 per record. The average cost is $148 per record.

SOURCE: Eighth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute (July 2018)

RECENT DEVELOPMENTS

MOST HEALTHCARE ENTITIES ARE UNPREPARED FOR A BREACH:

- 61% of respondents say their boards of directors are not informed and knowledgeable about their company's breach response plan.
- 56% of respondents say their board members want to know ASAP if a material data breach occurs, but only 45% of respondents say the C-suite would want to be informed about a data breach.
- Only 40% of respondents say the board understands the specific security threats facing their organization and only 15% believe the board is willing to successfully carry out its incident response plan.

SOURCE: Fifth Annual Study: Is Your Company Ready for a Big Data Breach?, Ponemon Institute (Feb. 2018)

RECENT DEVELOPMENTS

OCR'S PHASE II AUDIT RESULTS WERE DISAPPOINTING:

- Security Rule compliance was poor
  - 94% audited entities did not have a risk management plan
  - 83% of audited entities failed to conduct a risk analysis
- Privacy Rule compliance was marginally better
  - Most Notices of Privacy Practices were inadequate
  - Breach Notices were timely but content was lacking for most audited entities
  - 89% failed the patient rights component of the audit relating to individual access to their PHI

HIPAA and the HITECH Act Apply to:

- COVERED ENTITIES (CE):
  - Healthcare providers who engage in certain electronic transactions
  - Health care clearinghouses
  - Health plans
- BUSINESS ASSOCIATES (BA):
  - Entities that create, receive, maintain, or transmit protected health information (PHI) on behalf of a covered entity
  - Covered Entities can be Business Associates

What Is Protected Health Information?

- the PHI is defined as all "**individually identifiable health information**" held or transmitted by a CE or its BA, in any form or media, which includes demographic data that identifies the individual and that relates to:
  - the individual's past, present or future physical or mental health or condition,
  - the provision of health care to the individual, or
  - the past, present, or future payment for the provision of health care to the individual
- "**electronic protected health information**" or e-PHI, is PHI that is transmitted or maintained electronically

Who Are Covered Entities?

- Covered Entities include healthcare providers that transmit any health information electronically in connection with a transaction covered by the HIPAA Administrative Simplification Standards
  - Administrative Simplification Transaction Standards apply to any electronic transaction between two parties to carry out financial or administrative activities related to health care

Who Are Business Associates?

Entities that create, receive, maintain, transmit PHI on behalf of a Covered Entity:

- In connection with HIPAA functions (healthcare operations, payment, covered entity functions)
- Provision of certain services (e.g., legal, accounting, billing or claims management, consulting)
- Data transmission providers, health information organizations and e-prescribing gateways
- Data storage or hosting companies (e.g., cloud or off-site storage providers) even if they do not access PHI
- Subcontractors of Business Associates that have access to PHI

Business Associates Are Not:

- Members of Covered Entity's workforce
- Those whose duties do not require access to or handling PHI (e.g., janitor)
- Entities receiving PHI to conduct activities on their own behalf (e.g., banks, third party payors)
- Health care providers while providing treatment
- Members of an Organized Healthcare Arrangement (care coordination)

Business Associates Must:

- Sign and comply with Business Associate Agreements with Covered Entities
- Report to Covered Entity any breaches of unsecured PHI
- Comply with the Security Rule (subject to audit):
  - perform a risk analysis
  - appoint security officer
  - implement appropriate administrative, technical and physical safeguards
  - have Business Associate Agreements with subcontractors that are at least as stringent as those Business Associate executed
  - create written policies and procedures
  - train personnel

Overview of HIPAA and HITECH Act Requirements

- PRIVACY RULE
  - Must maintain privacy of PHI
  - Meet a growing list of obligations to patients
  - Several readily apparent mandates: minimum necessary, Notice of Privacy Practices
- SECURITY RULE
  - Must conduct risk analysis
  - Must implement required physical, administrative and technical safeguards to secure e-PHI and appropriate systems
  - Manage Business Associate and subcontractor relationships
- BREACH NOTIFICATION RULE

PRIVACY RULE
Uses, Disclosures and Requirements

- Permitted uses and disclosures of PHI include:
  - to the individual
  - for healthcare operations, payment and treatment
  - for other reasons, if patient or personal representative does not object:
    - provider directory
    - those (spouse, family members, friends, or other persons identified by patient) directly involved in patient care or payment for care
  - for certain public safety or government actions
  - if "incident to" another permitted use or disclosure
  - public interest and benefit activities (required by law, public health)
- Minimum necessary standard

PRIVACY RULE
Administrative Requirements

- Appoint privacy officer
- Implement privacy policies, including:
  - uses and disclosures of PHI
  - sanctions policy for employees responsible for violations
  - processes for handling security incidents and breaches
  - the “minimum necessary” standard
- Train personnel
- Mitigate and report breaches of unsecured PHI
- Document ongoing compliance activities, disclosures, incidents, risk assessments

PRIVACY RULE
Patient Rights

Patients may exercise various rights, some of which are not mandatory, including:

- Requesting restrictions on use or disclosure for treatment, payment or healthcare operations
- Seeking communications by alternative means or at alternative location
- Access to PHI
- Requesting amendment of PHI
- Right to an accounting of PHI disclosures
- Notice of privacy practices

PRIVACY RULE COMPLIANCE
How am I supposed to communicate PHI?

- CE providers can share PHI for treatment purposes without patient authorization, as long as they use reasonable safeguards when doing so. These communications can be made orally or in writing, by phone, fax, e-mail, or otherwise.
  - A provider may fax a patient's record, test results or health care instructions to another provider to which the patient is being transferred.
  - A doctor may discuss a patient's condition over the phone with another provider who is treating the patient.
  - When a patient initiates communications with a provider using e-mail, the provider can assume that e-mail is acceptable, unless otherwise stated.
- Reasonable safeguards vary based on the circumstances and the mode of communication used.

PRIVACY RULE COMPLIANCE
Accounting of Disclosures of PHI

- CE must be able to provide patients with an accounting of certain disclosures of their PHI, upon request. The accounting must include:
  - date of disclosure
  - name of entity or person who received the PHI
  - brief description of PHI disclosed
  - brief statement of purpose of the disclosure
- Patients have the right to a written accounting of disclosures for the 6 year period preceding the request.
- Disclosure need not be documented in each patient record.
  - Example: Health Oversight Agency

SECURITY RULE

- Appoint security officer
- Report to Covered Entity any breaches of unsecured PHI
- Documentation obligations (subject to audit):
  - perform a **risk analysis**
  - implement appropriate **administrative, technical and physical safeguards**
  - sign and comply with Business Associate Agreements with Covered Entities and subcontractors
  - create written policies and procedures
  - Personnel training
- Technical yet flexible

SECURITY RULE COMPLIANCE
How Important is the Risk Analysis?

- A risk analysis is essential to HIPAA compliance and security. A strong risk analysis determines which security measures are reasonable and appropriate and how the Security Rule safeguard requirements will be addressed.
- The risk analysis process must include, at least, the following considerations:
  - assessment of potential risks and vulnerabilities to the entity's e-PHI
  - reasonably anticipated threats or hazards to the security or integrity of e-PHI
  - the probability and criticality of the potential risks to e-PHI
  - the appropriate security measures to address the risks identified
- This process should be ongoing, as entities should review the effectiveness of security measures, risks to e-PHI, access to e-PHI and security incidents.

SECURITY RULE COMPLIANCE
Is Encryption of e-PHI Required?

- A mechanism to encrypt e-PHI is an **Addressable** safeguard requirement.
- Entities must implement encryption if it determines that this is a reasonable and appropriate safeguard for its e-PHI. If the entity decides that encryption (or any other addressable specification) is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure or not implement at all.
- Entities must document the decision and rationale if encryption is not implemented.
    - Assessment and determination should be based on organization's environment, security framework and needs, risk analysis, risk mitigation strategy and the cost of implementation.

BREACH NOTIFICATION RULE

WHAT IS A BREACH UNDER HIPAA:

- A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information (PHI).
- Breaches involve ”unsecured protected health information”

LIMITED EXCEPTIONS:

1. unintentional workforce access,
2. inadvertent disclosure to authorized person, and
3. “good faith” belief that unauthorized person could not retain data disclosed

BREACH NOTIFICATION RULE

An impermissible use or disclosure of PHI is **presumed to be a breach** unless the CE or BA demonstrates that there is a **low probability that the PHI has been compromised** based on a risk assessment including at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom it was disclosed;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

Hollywood Presbyterian Attack

Feb. ‘16: Hackers broke into and took over Hollywood Presbyterian’s servers, encrypting patient files and demanding $ for decryption key

- Hollywood Presbyterian (HPMC): 434-bed private hospital in LA
- Systems locked for about 10 days
  - No access to digital health records; staff used pen and paper
  - Fax lines jammed, email unavailable; some emergency patients routed to other hospitals
  - Ability to provide health services limited
- “Locky” **ransomware** used in attack is reliant on human error
  - Email with attached file that includes garbled text
  - Users instructed to activate macros to make text readable
  - Once activated, malware encrypts files; timer starts on ransom

Hollywood Presbyterian Attack

- Reported incident to law enforcement authorities
- HPMC pays $17,000 ransom (40 Bitcoins) and publicly acknowledges attack
  - Initial attack: Feb. 5
  - Press release: Feb. 17
- “The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this.” – HPMC President and CEO Allen Stefanek
- Per HPMC, no evidence patients’ health records were accessed
- Electronic medical records fully restored on Feb. 15
- Systems tested, cleared of malware

BREACH NOTIFICATION RULE

IN THE EVENT OF A BREACH, NOTICE MUST BE GIVEN TO:

- All affected individuals:
  - Notification must be provided without unreasonable delay and in no case later than 60 days following discovery of a breach
  - Notice should be written, but other means available (electronic, telephonic or by substitute notice)
  - The notice should include brief descriptions (i) of the breach, (ii) data involved, (iii) steps affected persons should take to protect themselves from harm, (iv) what the CE is doing to investigate the breach, mitigate the harm, and prevent further breaches, and (v) contact information for the CE (or BA)

BREACH NOTIFICATION RULE

IN THE EVENT OF A BREACH, NOTICE MUST BE GIVEN TO:

Prominent media outlets must be notified if > 500 residents of a State/jurisdiction affected

- Without unreasonable delay and no later than 60 days

The Secretary of HHS must be notified, through OCR

- CEs must notify the Secretary by completing the online HHS form
- If a breach affects 500 or more individuals, CE must notify the Secretary without unreasonable delay and no later than 60 days
- If a breach affects fewer than 500 individuals, CE may notify the Secretary on an annual basis, within 60 days of the end of the calendar year in which the breaches are discovered

HHS OFFICE FOR CIVIL RIGHTS (OCR) ENFORCEMENT ACTIVITY

Administrative decision in *MD Anderson* proceeding bolstered OCR's enforcement authority

- ALJ granted summary judgment to OCR on all issues, upholding its enforcement authority and finding a $4,348,000 penalty to be reasonable
- Involved three breach reports regarding a stolen laptop and 2 lost USB drives (unremedied pattern)
- Risk analyses found device level encryption a high risk but no action taken for 5 years

Thank You

Kurt E. Bratten

kbratten@oalaw.com
www.oalaw.com