Confidentiality Update
September 12, 2018

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

BARCLAY DAMON LLP

Today's Privacy Agenda

- HIPAA Privacy
- Auditing and OCR
- Recent Developments
- Privacy Best Practices

HIPAA General Background

What is HIPAA?

- *Health Insurance Portability and Accountability Act*
- HIPAA is a Federal Law

HIPAA Health Information Regulations:

1. Transactions and Code Set Standards
2. Privacy
3. Security
   - These regulations apply to "covered entities"
   - **Covered Entities** = Include most health care providers, health plans and health care clearinghouses.

Overview of HIPAA Privacy

- Uses & Disclosures of PHI Restricted
- Requires the Safeguarding of PHI
- Requires Those Covered by the Rule to Implement Certain Administrative Measures
- Grants Individuals Certain Rights Regarding Their PHI
- Privacy Officer

Covered Entities vs. Business Associates

- **Covered Entities must comply** with the United States Department of Health and Human Services Privacy and Security rules.
- **"Business Associates"** are persons or entities that perform certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provide services to, a Covered Entity.

Business Associates; Subcontractors

Business Associate Requirements:

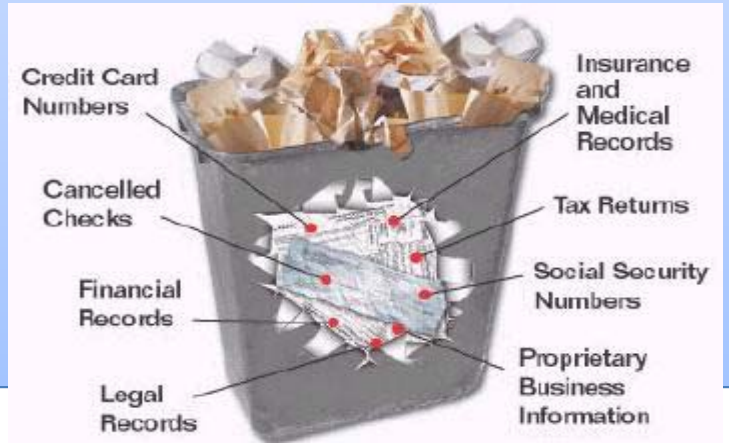
- Only use or disclose PHI to service or support a covered entity
- Safeguard the PHI
- Report to the covered entity any improper use or disclosure of which it becomes aware
  - Today: Business Associates can be penalized for non-compliance

Business Associates; Subcontractors

Ensure that your agents and subcontractors that create, receive, maintain or transmit PHI agree to the same conditions and restrictions
Make available requested information if needed for patient access, amendment or an accounting of disclosures
Upon request, make available information to the Secretary of Health and Human Services
Comply with the rules and regulations that apply to covered entities if carrying out a covered entity's obligations

Business Associates; Subcontractors

- Return or destroy PHI at termination of a contract
- Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI
- Report to the covered entity any security incident of which you become aware
- Comply with the Breach Notification Provisions



Business Associates; Other Considerations

- Auditing rights
- Cooperation
- Indemnity
- Insurance

Business Associate Agreements

- HIPAA Violation: A workforce member of a business associate of North Memorial Health Care of Minnesota (North Memorial) had their unencrypted, password-protected laptop, containing electronic protected health information (ePHI), stolen from a locked vehicle. The business associate was a major contractor for North Memorial and performed payment and health care operation activities on behalf of North Memorial.
  - Breach affected up to 9,947 individuals.
  - OCR received a breach report from North Memorial.
- OCR Investigation Indicated North Memorial:
  - Failed to have a business associate agreement in place with a major contractor.
  - Provided this business associate access to stored electronic and non-electronic protected health information (ePHI) of 289,904 patients.
  - Failed to complete a risk analysis to address all of the potential risks and vulnerabilities to ePHI in its IT infrastructure.
- Penalty: Settled potential HIPAA violations: $1,550,000.

No Business Associate Agreement

- HIPAA Violation: Center for Children's Digestive Health (CCDH) and their business associate were unable to produce a signed Business Associate Agreement to the OCR. The business associate was responsible for storing records with PHI for CCDH.
  - After an investigation was initiated against the business associate, the OCR conducted a compliance review of CCDH.
  - Neither CCDH nor the business associate could produce the Business Associate Agreement.

- Penalty:
  - Implemented a corrective action plan.
  - Settled potential violations: $31,000.

OCR and Auditing

- Enforcement is up.
- But auditing is not.

Large penalties and many of them, but word on the street is auditing has been suspended. OCR is still taking complaints and is required to investigate those.

State Laws

Stronger State Laws Continue to Apply:

HIPAA privacy rules set a floor of privacy standards, but states, such as New York, are free to require additional protections

– HIV, Mental Health, Alcohol and Substance Use Records all receive additional protection

NYS General Business Law

GBL § 899-aa:

- Any entity or person which conducts business in New York and owns or licenses computerized data which includes "private information" shall disclose any breach of its security system following discovery or notification of such breach to any resident of New York whose private information was or is reasonably believed to have been disclosed.

Private Information Includes:

- Social security number;
- Drivers license number; or
- Account, credit or debit card number, in combination with:
  - Any required security code or access code, or
  - Password that would permit access to an individual's financial account.
- Other notifications may be required.

Hot Topics

- Retention
- Family Members
- Breach Notification
- Penalties
- Best Practices Learned
- Board Responsibilities

HIPAA Breach Notification Highlights

Upon Discovery of a Breach:

1. A ***Covered Entity*** must notify each individual whose unsecured protected health information has been, or is reasonably believed by the Covered Entity to have been, accessed, acquired, or disclosed as a result of such breach.
2. A ***Business Associate*** must notify the Covered Entity of such a breach, including the relevant individuals' names.

Breach Notification Regulations

Breach:

Unauthorized acquisition, access, use or disclosure of PHI which compromises security or privacy of such information.

Breach Exceptions:

1. Unintentional acquisition, access or use by workforce member if made in good faith
2. Inadvertent disclosure to authorized person in same entity with no future misuse
3. Good faith belief PHI could not reasonably have been retained

Breach Notification

Breach Notification Standard:

- Breach presumed, unless "low probability" that PHI "compromised" based on:
  - Nature and extent of PHI
  - Person who accessed PHI
  - Whether PHI was actually acquired or viewed
  - Extent to which risk mitigated

Protecting PHI

Two Methods of Rendering PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals:

1. **Encryption**– Two processes tested by the National Institute of Standards and Technology (NIST) listed
2. **Destruction**– Prior to disposal:

Paper, Film, or Other Hard Copy Media:	Electronic Media:
• Shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed	• Cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that PHI cannot be retrieved

Breach Discovery & Notification

Discovery:

- Breach is "discovered" on the first day it becomes known to the entity or reasonably should have become known to have occurred
  - This includes any person other than the individual who committed the breach, that is an employee, officer or other agent, or Business Associate of the entity

Breach Notification:

- Notification must be made without "unreasonable delay" and never more than *60 calendar days* after discovery of the breach
  - Burden is on the Covered Entity and Business Associate to demonstrate that notifications were made and/or adequately explain the necessity for any delay in notification

Breach Notification Regulations Highlights

Upon Discovery of a Breach, a Covered Entity Must Notify:

1. Each individual whose unsecured protected health information has been, or is reasonably believed by the Covered Entity to have been, accessed, acquired, or disclosed as a result of such breach.
2. A *Business Associate* must notify the Covered Entity of such a breach, including the relevant individuals' names.

Breach Notice Requirements

First Class Mail— Sent to last known address

- E-mail permissible only if specified by individual

Insufficient or Out-of-Date Contact Information— Laws include provisions for posting

If Urgency— Telephone communication allowed

500 or More Residents of a State— Prominent media outlets

500 or More Individuals— Immediate notice to Secretary of the United States Department of Health and Human Services required

- Less than 500— Covered Entity may maintain a log for annual submissions to the Secretary

When More than 500 Individuals— Secretary will list information regarding the breach on a public website

Breach Notification Requirements

Notice Must Include:

1. Brief description,
   - Including the date of the breach and date of discovery,
2. Description of the information involved,
3. Steps that should be taken to protect themselves from harm,
4. Brief description of what the Covered Entity is doing to investigate, mitigate losses and to protect against further breaches, and
5. Contact information if an individual wanted to get further information.

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?

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.

Tiered Increase in Monetary Penalties

Did Not Know & Would Not Have Known with Reasonable Diligence:

- As low as $100 for each violation, up to $25,000 in a calendar year

Reasonable Cause & No Willful Neglect:

- As low as $1,000 for each violation, up to $100,000 in a calendar year

Willful Neglect:

- $10,000 for each violation, up to $250,000 in a calendar year

Where No Correction:

- As high as $50,000 for each violation, up to $1,500,000 in a calendar year

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 for Civil Rights or other state authorities.

HIPAA Penalties
Offsite Information

- HIPAA Violation: An in-home health care provider was investigated after an employee removed documents containing protected health information (PHI) from the company office and abandoned the information for an unauthorized person (ex-husband) to access. Although the agency claimed the PHI was stolen by the individual who discovered it, the Administrative Law Judge said the agency was obligated to take reasonable steps to protected PHI from theft.
  - Breach affected up to 278 individuals.
  - Disgruntled ex-husband filed a complaint with OCR after ex-wife left behind PHI from agency patients.
- OCR Investigation Indicated Lincare, Inc.:
  - Failed to have adequate policies and procedures in place to protect patient information that was taken offsite.
  - Had an unwritten policy requiring certain employees to store PHI in their own vehicles.
  - Only took minimal action to correct its policies and strengthen safeguards after becoming aware of the complaint and the OCR investigation.
- Penalty: Civil Monetary Penalties (CMP) imposed by OCR: $239,000.

Stolen/Lost Thumb Drives, Laptops

- HIPAA Violation: Adult & Pediatric Dermatology, P.C., of Concord, MA, reported to OCR after an unencrypted thumb drive containing electronic protected health information (ePHI) was stolen from an APDerm staff member's vehicle.
  - Stolen thumb drive contained the ePHI of approximately 2,200 individuals.
  - The thumb drive was never recovered.
- OCR Investigation Indicated APDerm Did Not:
  - Conduct an accurate or thorough analysis of potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process.
  - Comply with requirements of the Breach Notification Rule requiring written policies and procedures and training workforce members.
- Penalty: Settled potential HIPAA violations with OCR for **$150,000.**

PHI on a Driveway

- OCR Investigation Indicated:
  - Parkview is a nonprofit health care system that provides community-based health care services to individuals in northeast Indiana and northwest Ohio.
  - OCR received complaint from a retiring physician.
  - Parkview took custody of medical records pertaining to approximately 5,000 to 8,000 patients while assisting the retiring physician to transition her patients to new providers, and while considering the possibility of purchasing some of the physician's practice.
  - Parkview employees, with notice that the physician was not at home, left 71 cardboard boxes of these medical records unattended and accessible to unauthorized persons on the driveway of the physician's home, within 20 feet of the public road and a short distance away from a heavily trafficked public shopping venue.
  - Parkview cooperated with OCR throughout its investigation.
- Penalty: $800,000.
  - Corrective action plan to revise policies and procedures, train staff, and provide an implementation report to OCR.

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.

Malware:
OCR and HHS Guidance

FACT SHEET: Ransomware and HIPAA

A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015).[1] Ransomware exploits human and technical weaknesses to gain access to an organization's technical infrastructure in order to deny the organization access to its own data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack. This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.

THE SECRETARY OF HEALTH AND HUMAN SERVICES
WASHINGTON, D.C. 20201
JUN 2 0 2016

Dear Colleague:

We are fortunate to spend our days working to improve the health of the nation. We have extraordinary opportunities to improve health and transform health care for millions of Americans—opportunities to improve the quality of the care while spending our dollars more wisely, to strengthen global health security, and to reaffirm American leadership in research, innovation, and science. Foundational to these advances is our ability to maintain and use data to bring health care into the 21st century. Data security is essential to our progress.

Like leaders in all industries, I know you are concerned about cybersecurity. Even when we do our best, problems can occur. As the President has noted, cybersecurity is one of the most important challenges we face as a nation. We understand this challenge first hand as we manage the security of our own department. Like you, we work hard at this every day.

Beware of Malware: OCR Investigation

- HIPAA Violation: The University of Massachusetts Amherst (UMass) reported a breach to the OCR when a workstation in its Center for Language, Speech, and Hearing ("Center") was infected with a malware program. The malware caused the disclosure of 1,670 individuals' ePHI.

- OCR Investigation Indicated UMass Failed to:
  - Designate the Center as a health care component.
  - Implement Policies and Procedures at the Center to ensure HIPAA compliance.
  - Provide technical security measures at the Center, such as a firewall.

- Penalty: UMass agreed to settle potential HIPAA violations by paying $650,000.
  - UMass was also required to implement a corrective action plan.
  - The corrective action plan required a comprehensive and thorough risk analysis, as well as a review of Polices and Procedures.

What Covered Entities Should Do

- Consider internal audits.
- Document internal audit results and efforts towards compliance.
- Coordinate privacy and security staff, policies and procedures.

Remember: If OCR investigates a covered entity, they will ask what steps were taken. Covered entities should do the easy stuff and document each step.

Cyber Liability and Insurance Related to Breach of PHI

- Created to protect against losses from hacking PHI or other breaches.
- These policies also include protection from defense costs.
- Privacy lawsuits not under HIPAA – under a negligence theory – breach, duty, causation, damages.

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 patient 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 patient files 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.