Health Care Compliance Association
Confidentiality Update

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

BARCLAY DAMON LLP

Today's Agenda

- HIPAA Compliance Update (Melissa)
- Privacy Best Practices (Melissa)
- Healthcare Risk Landscape Overview (Rob)
- Security Best Practices (Rob)

BARCLAY DAMON LLP

Hot Topic in Privacy – Business Associates

- Auditing rights
- Cooperation
- Indemnity
- Insurance

BARCLAY DAMON LLP

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.

BARCLAY DAMON LLP

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.

BARCLAY DAMON LLP

Hot Topic in Privacy - 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 still taking complaints and is required to investigate those.

BARCLAY DAMON LLP

Hot Topic in Privacy - HIV

- Confidential HIV-related information – broad definition, includes negative test; mere receipt of services
- Authorized disclosures – provides services, billing, reimbursement
- Strict minimum necessary
- Public Health Law Article 27-F & 10 NYCRR Part 63
- Consent/authorizations must specifically reference HIV information. No general authorizations. Must be written. Ensure capacity.
- Statement Prohibiting Redisclosure
- Not just subpoena – must be court order or person must authorize.
- Court Order – compelling need; significant risk of life or health; entitlement pursuant to applicable law; application by health officer
  - Sealing of application, supporting documents, and resulting decision
  - Notice
  - Scope of Order

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 for Civil Rights or other state authorities.

Hot Topic in Privacy - Alcohol and Substance Use Records

- 42 U.S.C.S. § 290dd-2; 42 CFR Part 2
- Program – Federally Assisted
- Any information that would lead someone to believe treatment received
- Patient consent for disclosure
- Notice to Accompany Disclosure
- Court Order Authorizing Disclosure
  - Notice
  - Conduct of Hearing
  - Confidential Communications
  - Determination of good cause

Changes to 42 CFR Part 2

- New Consent
  - Patients can list:
    1) Individuals;
    2) Entities with a treating provider relationship;
    3) Third party payors; and
    4) Entities that are not under (3), such as health information exchanges and consents under general designations - e.g., "all my treating providers".
  - Using the general designation is optional, but if it is used, then the disclosing provider must be able to produce a list of disclosures.
    - NOTE: Intermediaries (e.g., HIE, ACO) are responsible for producing a list of disclosures, not the Part 2 Program.
- Amount and Kind
  - "How much and what kind of information?"
  - Disclosable information must be described in a clear and specific manner to allow all parties to comply with the consent request.

Other Changes to 42 CFR Part 2

- **Qualified Service Organizations (QSO)**
  - Definition now includes population health management services as QSO services.
  - QSO-related agreements can be used to provide medical staffing services.
- **Re-Disclosure**
  - Clarifies that re-disclosure is only prohibited where the information would directly or indirectly identify an individual with SUD.
    - Be aware of medical codes, prescriptions and descriptive language that could identify a patient with SUD.
- **Notice to Patients**
  - Written notice of confidentiality rights to patients required.
- **Security of Records**
  - Detailed requirements that align closer to the HIPAA Security Rule.

BARCLAY DAMON LLP

Hot Topic – Breach Notification

- Late Breach Notification - $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?

BARCLAY DAMON LLP

Hot Topic - 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.

BARCLAY DAMON LLP

Hot Topic - 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.

BARCLAY DAMON LLP

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."

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?

BARCLAY DAMON LLP

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.

BARCLAY DAMON LLP

Conclusion and Questions

Thank you for your time.

BARCLAY DAMON LLP