CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

GW | GARFUNKEL WILD, P.C.
ATTORNEYS AT LAW

Significant Developments in Healthcare

Presented by:
Karen Painter Randall, Partner, Connell Foley LLP
Stacey L. Gulick, Partner, Garfunkel Wild, P.C.

Recent Enforcement Actions

What Are the Concerns?
(Just a reminder)

- Civil Monetary Penalties
- Criminal Penalties
- Private Rights of Action (there is no private right of action under HIPAA, but the courts have said that violation of HIPAA can be used to prove other claims such as negligence)
- Class Action Suits
- Costs of an OCR Investigation

Largest Settlements to Date

(Failure to Terminate Employee Access)

On February 16, 2017, the OCR announced that, as a result failing to remove access upon termination of an employee, Memorial Healthcare System (MHS) paid the OCR $5.5 million. MHS operates hospitals, and a variety of ancillary health care facilities in Florida. In addition, MHS is affiliated with physician offices through an OHCA.

MHS reported to the OCR that the PHI of 115,143 individuals had been impermissibly accessed and disclosed. The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI maintained by MHS on a daily basis without detection from April 2011 to April 2012, affecting 80,000 individuals. The OCR specifically noted that (1) **MHS failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access**, and (2) failed to audit computer system activity, despite having identified this risk on several risk analyses conducted by MHS from 2007 to 2012.

Largest Settlements to Date

In August 2016, Advocate Health Care Network (Advocate) entered into a settlement with the OCR to pay $5.55 million and adopt a corrective action plan. The investigation occurred after Advocate reported three large breaches (involving different of the Advocate entities). The OCR alleged that Advocate failed to:

- **conduct an accurate and thorough risk analysis of all of its facilities, equipment, applications and data systems;**
- limit physical access to its electronic information systems;
- obtain a BAA from a vendor that had access to PHI resulting in impermissible disclosure of ePHI; and
- failed to reasonably safeguard the ePHI when an AMG workforce member left an unencrypted laptop in an unlocked vehicle.

Lack of Timely Breach Notification

In January 2017, the OCR announced the first HIPAA settlement based on the untimely reporting of a security breach Presence Health agreed to pay $475,000 and implement a corrective action plan. The OCR claims that this settlement balanced the need to emphasize the importance of timely breach reporting with the desire not to disincentive breach reporting altogether.

On January 31, 2014, Presence Health reported to the OCR that on October 22, 2013, Presence Health discovered that operating room schedules, which contained the PHI of 836 individuals, were missing. The OCR's investigation revealed that Presence Health failed to notify, within 60 days of discovering the breach, each of the 836 affected individuals, media outlets, and the OCR.

Malware

On June 4, 2013, OCR received notification from UMass regarding a workstation that was infected by mal ware, which may have resulted in a breach affecting approximately 1 ,670 individuals. As a result UMass entered into a settlement for $650,000. The OCR found that UMass failed to:

- Include all entities that would meet the definition of a CE or BA in its hybrid entity designation and implement policies accordingly;
- conduct an accurate and thorough risk analysis; and
- implement appropriate firewalls.

Unsecured Wireless Network

In July 2016, Univ. of Mississippi Medical Center ("UMMC") settled with the OCR for $2.75m following a breach involving 10,000 patients. The breach involved a password-protected laptop that went missing from UMMC. OCR identified that ePHI stored on a UMMC network drive was vulnerable to unauthorized access via UMMC's wireless network because users could access an active directory with a generic username and password.

Storage of PHI on Cloud Server (without BAA) Leads to Settlement

Oregon Health & Science University (OHSU) settled with the OCR for $2.7m and a comprehensive three-year corrective action plan. OCR's investigation began after multiple breach reports, including three reports involving unencrypted portable devices. OCR identified evidence of widespread vulnerabilities within OHSU's HIPAA compliance program, **including the storage of ePHI of over 3,000 individuals on a cloud-based server without a BAA.**

Storage of PHI on Cloud Server (without BAA) Leads to Settlement

- OCR noted that OHSU performed risk analyses in 2003, 2005, 2006, 2008, 2010, and 2013, but these analyses **did not cover** all ePHI in OHSU's enterprise. Furthermore, while the analyses identified vulnerabilities and risks to ePHI located in many areas of the organization, **OHSU did not act in a timely manner to implement measures to address these documented risks and vulnerabilities.**
- For example, OHSU also failed to implement a mechanism to encrypt and decrypt ePHI, **despite having identified this lack of encryption as a risk.**

Business Associate Enters Into Settlement for Stolen Iphone

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) (a management and information technology company for SNFs) entered into a settlement agreement with OCR for $650,000 following a breach involving the theft of an unencrypted Iphone. Only 412 individuals were involved.

Note: ***This is the first OCR settlement with a business associate.***

Other Significant Settlements

- Complete P.T. settled for $25,000 after posting patient testimonials, including full names and full face images, to its website **without obtaining HIPAA authorizations**.

- The University of Washington Medicine settled for $750,000 following a breach caused when an employee downloaded an email attachment containing **malicious software**.

- Cornell Prescription Pharmacy settled for $125,000 following **notification by the media** that the pharmacy disposed of unsecured (i.e., not shredded) documents in an unlocked, open container on the premises. **Reminding us that paper documents are still a concern**.

- Raleigh Orthopaedic Clinic settled with OCR for $750,000 when it disclosed information of 17,300 patients to a potential business partner (that was transferring films to digital media) **without first executing a BAA**.

Takeaways

- The most important thing you need to do to protect your organization is to have a comprehensive up-to-date Risk Analysis and corresponding Risk Management Plan.
- Nearly every settlement to date has involved failure to have a comprehensive Risk Analysis and corresponding Risk Management Plan.
- When the OCR walks through the door, for ANY reason (breach, complaint, audit), the first thing it will request is the Risk Analysis.

Ransomware

- What is Ransomware?
  - Ransomware can take different forms, but in essence it denies access to a device or file until a ransom has been paid.
  - Not only can ransomware encrypt the files on a workstation, the software is mart enough to travel across your network and encrypt any files located on both mapped and unmapped network drives.
  - This can lead to a catastrophic situation whereby one infected user can bring a department or entire organization to a halt

Ransomware

- Once the files are encrypted, the hackers will display some sort of screen or webpage explaining how to unlock the files.
- Paying the “ransom” invariably involves paying a form of e-currency (cryptocurrency) such as Bitcoins.
- Once the hackers verify payment, they provide the “decryptor” software, and the computers start the arduous process of decrypting all of the files.

Ransomware

- New Strains of Ransomware
  - Popcorn Time
    - Offers free decryption if you infect two others and they pay.
    - Still proof of concept.
  - Koolava (a.k.a. Nice Jigsaw)
    - Offers free decryption if you learn how not to be infected.
    - Still work in progress and not high quality code.
    - Once the victim reads two articles, the Decrypt My Files button becomes available.
    - It will delete all files if the articles are not read.

Ransomware

- New Strains of Ransomware (cont.)
  - Goldeneye
    - Infects files, then infects the hard drive.
    - Potentially forces paying a double ransom.
    - Spreads as a fake job application email with a .pdf attachment. The .pdf points the victim to an infected Excel file.
    - After file encryption, the machine reboots and looks like it is doing a filesystem repair. It is actually encrypting.
    - After paying the money to decrypt, logging in may demand more to decrypt the file.

Ransomware

- New Strains of Ransomware (cont.)
  - Spora
    - Offers an option of future immunity (for a fee).
    - No C&C server so blocking outbound communication does not help.
    - Adds the hidden attribute to files and folders on the desktop, the root of USB drives and the system drive. These files and folders are now hidden by the standard folder options.
    - It now makes Window shortcuts with the same name and icon as the hidden files and folders.

Ransomware

- The Hollywood Presbyterian Medical Center
  - In February 2016, the Hollywood Presbyterian Medical Center was hit by a ransomware attack that knocked the hospital’s network offline.
  - The attach affected the facility’s daily operations, as urgent scans, lab work, pharmaceutical needs, and documentation could not be accessed.
  - Paid $17,000 in Bitcoins.

Ransomware

- MedStar Health
  - In March 2016, one of country’s leading healthcare providers with a network of ten hospitals and 250 outpatient centers was affected by a ransomware attack.
  - The organization acted quickly and took down all system interfaces to prevent the malware from spreading.
  - The ransom was set at 45 Bitcoins (approx. $19,000) with a ten-day deadline, but MedStar reportedly able to bring system back online without paying

Ransomware

- Takeaways
  - Experts disagree as to whether or not a company should pay. On one hand unless you have a powerful computer and a lot of time to spend guessing keys, there is really no way to get your data back unless you pay the ransom.
  - However, The Department of Homeland Security tells people to not negotiate with the hackers as it will encourage more attacks
  - The very best defense to prevent a ransomware attack is to have a backup that is not connected to your machine in any way.

Changes to Substance Abuse Regulations

- March 27, 2017 revised regulations under 42 CFR Part 2 went into effect .
- Expands the requirements of 42 CFR Part 2 to “lawful holders” of substance abuse treatment information (e.g., individual or entity who has received the information as the results of a part 2-compliant patient consent (with notice of prohibition on redisclosure) and other entities that legally receive such information without consent).

Changes to Substance Abuse Regulations

- Creates new requirements for security of substance abuse treatment information – consistent with HIPAA.
- Establish requirements for disposition of records by discontinued programs.
- Requires Notice of Privacy Practices to include contact information to report violations of 42 CFR Part 2.

Changes to Substance Abuse Regulations

- Expands the permitted designations allowed in the "to whom" Section of the consent for release of substance abuse treatment information.
- Includes a new requirement that consent forms explicitly describe the information to be disclosed (e.g., diagnostic information, medications, etc.).
- Includes a requirement, that if general designation is used, the provider must be able to provide patient with a list of individuals to whom the information was provided.

Changes to Substance Abuse Regulations

- Loosens the requirements for use of substance abuse treatment information for research – consistent with HIPAA.
- Allows ACOs to access substance abuse treatment information for audit purposes

Q&A