CLM Claims & Litigation Management Alliance™
ADVANCING ETHICS, COOPERATION AND EDUCATION

CLM 2016 Cyber Liability Summit
October 5, 2016 in New York City

The Brave New World of HIPAA Enforcement

I. Introduction/Healthcare Industry is Perfect Target for Cyber-Attack

According to a 2015 study by the Ponemon Institute, the total cost of a data breach is $6.5 million or $217 per lost or stolen record. However, according to the same study, a healthcare record lost or stolen in a breach could cost as much as $363. The increase in cyber incidents overall is due to a number of factors including: data is now easier than ever to store; organizations are not properly monitoring data; data is incredibly valuable; and demand for sensitive information is coming from all around the world as companies try to gain competitive edge in a global marketplace.

With regard to the healthcare industry, with the increased use of digitized records, the creation of HealthCare.gov, and the exchange of ePHI online, the healthcare industry has become perfect target for hacker. In particular, five of the eight largest breaches over the last 5 years happened the first six months of 2015. Additionally, according to information gathered by IBM X-Force, healthcare ranked number 1 in terms of records compromised, with nearly 34% of all records compromised across all industries.

The healthcare industry is a perfect target for a cyber-attack because of the valuable data these organizations possess, including patient's email, SSN, banking, employment info, and health and medical data. Moreover, the PHI maintained by these organizations has excellent resale value on the black market.

II. What Are Some of the Top Breaches in 2015/2016 Involving the Healthcare Industry?

A report released by the American Action Forum estimated that the cost to deal with just the first six months of security breaches at healthcare organizations in 2015 to be more than $37 billion. The following are some of the top recent breaches.

In February 2015, Anthem, Inc. the United States' second largest health insurer, was the victim of a very sophisticated external cyber-attack wherein hackers broke into one of its databases, potentially compromising 78.8 million individuals' personal information. Affected data included names, dates of birth, medical IDs or Social Security numbers, street addresses, and email addresses. Both Anthem patients and employees were possibly affected. Anthem also came under scrutiny from certain lawmakers for its timeline in the data breach notification process. The breach was discovered on Jan. 29, 2015, and the company waited until Feb. 4, 2015 to make a public announcement. However, the databases were potentially accessed as early as April 2014, which meant personal data could have been in the wrong hands for some time, the lawmakers stated. Current estimates on the breach cost are expected to surpass $100 million

The second largest healthcare data breach for 2015 took place at Premera Blue Cross, wherein 11 million individuals potentially had their information accessed in a hacking incident. As with the Anthem data breach, Premera discovered the data breach on January 29, 2015. However, it is believed that the initial attack occurred on May 5, 2014. Applicants and members' names, dates of birth, email addresses, addresses, telephone numbers, Social Security numbers, member identification numbers, bank account information, and claims information, including clinical information, were all possibly exposed. While Premera says it did not have evidence that the data was removed from the system or "used inappropriately," the company mailed letters to affected customers today and offered two years of free credit monitoring and identity theft protection.

Originally reported as affecting 7 million individuals, the Excellus data breach potentially compromised 10 million individuals' PHI, according to the OCR data breach reporting database. Excellus Blue Cross Blue Shield (Excellus BCBS) announced in September 2015 that it discovered on August 5, 2015 that it had been the victim of a cyber-attack. However, the initial attack took place on December 23, 2013. Potentially exposed information included individuals' names, dates of birth, Social Security numbers, mailing addresses, telephone numbers, member identification numbers, financial account information and claims information.

UCLA Health System was the victim of a large-scale cyber-attack, reporting in July 2015 that approximately 4.5 million patients may have had their information exposed in a healthcare data breach. The attack was discovered on May 5, 2015, and affected individuals include UCLA Health patients and providers who sought privileges at any UCLA Health hospital, or was maintained on the impacted parts of the UCLA Health network. Suspicious activity on the UCLA Health network was first discovered in October 2014 and an investigation was reportedly opened. However, UCLA Health said that it did not appear at the time that attackers had gained access to the parts of the network that contained personal and medical information. UCLA said that prior to the attack on its system it had been taking steps and spending tens of millions of dollars to strengthen its computer security. It added that it has successfully thwarted hacker attacks in the past. However, some security experts were unimpressed questioning the lack of encryption at UCLA in light of other breaches across the country. Class action lawsuits were subsequently filed seeking damages for fraud, negligence, invasion of privacy, breach of contract, violation of medical confidentiality, unlawful business practices, and unjust enrichment, plus legal costs.

Medical Informatics Engineering (MIE) reported over the summer that it had experienced a cyber-attack affecting 3.9 million individuals. Suspicious activity was first noticed on one of its servers on May 26, 2015 it submitted breach information to OCR on July 23, 2015. MIE referred to the incident as a "sophisticated cyber-attack," and said that the unauthorized access may have begun on May 7, 2015. A class-action lawsuit was soon filed against, MIE, claiming that MIE failed "to take adequate and reasonable measures to ensure its data systems were protected," and also failed "to take available steps to prevent and stop the breach from ever happening."

III. HIPAA/HITECH

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996 to provide federal protection for the privacy and security of PHI held by covered entities and their business associates. A "covered entity" includes: a health care provider that conducts certain transactions in electronic form (called here a "covered health care provider"); a health care clearinghouse; and a health plan. A "Business Associate" is an individual (other than a member of the covered entity's workforce) or organization that performs or furnishes any function, activity or service, for or on behalf of a covered entity involving the use or disclosure of PHI, has been characterized as a "business associate" since the Privacy Rule took effect in 2003.

The responsibility for HIPAA oversight and enforcement efforts rest with the U.S. Department of Health & Human Services ("HHS"). Furthermore, HHS's Office for Civil Rights ("OCR") enforces compliance with PHI data regulations. To fulfill this requirement, HHS publishes what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information.

The Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule") establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' ePHI. The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting ePHI. Specifically, covered entities must: (1) ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit; (2) identify and protect against reasonably anticipated threats to the security or integrity of the information; (3) protect against reasonably anticipated, impermissible uses or disclosures; and (4) ensure compliance by their workforce.

HHS-OCR recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the Security Rule is flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their specific environments. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources. Therefore, when a covered entity is deciding which security measures to use, the Security Rule does not dictate those measures, but requires the covered entity to consider: (1) its size, complexity, and capabilities; (2) its technical, hardware, and software infrastructure; (3) the costs of security measures, and (4) the likelihood and possible impact of potential risks to ePHI.

The Health Information Technology for Economic and Clinical Health Act ("HITECH") was enacted in 2009 as part of an overall effort to modernize the keeping of medical records and PHI and update parts HIPAA. In particular, HITECH expressly requires HIPAA "covered entities" to report PHI data breaches affecting 500 or more individuals to the affected class, the HHS and the media within sixty (60) days of an event. HITECH also extends the complete Privacy and Security Provisions of HIPAA to the business associates of covered entities. This includes the extension of updated civil and criminal penalties to the pertinent business associates.

IV. Different Type of Cyber-Attacks Facing Healthcare Industry

A. Ransomware

As its name suggests, ransomware is malicious software that holds computing assets ransom. The software blocks users from accessing computer systems until money is paid. Ransomware is usually launched in small scale operations against individuals. According McAfee's 2016 Threat Predictions report, ransomware will be a "major and rapidly growing" threat in 2016. The security solutions firm pointed to new malware variants emerging and the success of the "ransomware-as-a-service" business model as drivers for the increase. McAfee predicts the rise in ransomware attacks that started in the third quarter of 2014 and continued throughout 2015 will not slow down this year.

Just this month, hackers took control of Hollywood Presbyterian Medical Center's computer systems and are demanding $3.6 million via $9,000 of bitcoin, a virtual currency, to release the data. Hospital president and CEO Allen Stefanek told the local NBC Channel 4 news station that the ransomware attack is impacting day-to-day operations. Emergency room operations were also taking a hit from the attack, and the hospital has had to transport patients to other medical centers because they could not access patient records. According to the Hospital, there was no evidence that any patient or employee information was the subject of unauthorized access or extraction by the attacker.

B. Unauthorized Access

This is what happened in the now infamous 2013 Target POS breach when hackers collected 40 million credit card records and 70 million customer records. The malware attacker accessed Target's private data by using the network access privileges of one of Target's third party vendors, a heating and air conditioning subcontractor, Fazio Mechanical Services Inc. By acting as a portal, Fazio, a $12.5 million dollar company, opened up Target, a $72.6 billion dollar company, to $420 million in potential losses.

C. Social Engineering

This is a non-technical method of intrusion hackers use that relies heavily upon human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. It is often caused by employees who receive and mistakenly open a phishing email or hit "reply all" to emails; fail to use hard to decipher passwords; fail to update password; fail to use encryption when sending highly confidential information such as financial or health information; or default a computer password to "123456" without considering the consequences. In fact, Verizon's 2013 Data Breach report found that over 75% of data breaches stemmed from weak or stolen credentials

D. Theft of Digital Assets

Stolen equipment such as laptops, thumb drives or smart phones can be another way for a data breach to take place. According to the U.S. Department of Health & Human Services' data on HIPAA breaches affecting 500 or more individuals, a company's number one security and compliance risk is theft of PHI on laptop computers.

E. Hacktivists

Hacktivist groups such as Anonymous, target healthcare institutions involved in controversial cases. The computer hacker group Anonymous is believed to be responsible for repeated cyber-attacks against the website of Boston Children's Hospital over the child-custody case involving 15-year-old Justina Pelletier. Children's Hospital filed child abuse charges against Pelletier's family after they brought her there last year for treatment of intestinal and other issues, which doctors concluded were unnecessary and that her problems were psychiatric.

V. New Cyber Threats Facing the Healthcare Industry

A. Internet of Things and Medical Devices

Medical device-makers need to protect their products from cyber-attack, according to recent draft guidance the U.S. Food and Drug Administration. The FDA also prodded hospitals to step up future reporting of any cyber-attacks. The Food and Drug Administration proposed new guidelines for how medical device manufacturers should secure their products. Among the FDA's recommendations, manufacturers are being asked to: Develop a risk management program that includes a plan for when a vulnerability is discovered; write disclosure policies, so hospitals and patients understand which aspects of a device may be less secure; and release regular software and hardware updates for medical devices after they're on the market.

B. Situations the FDA guidance is designed to prevent

First, Researchers at the University of Washington proved they could hack into the public communication systems that control teleoperated robots. They accessed the network that controlled the robot and disrupted the signals, making the robot's movement jerky and difficult to control. Also, by moving the robotic arms too quickly or beyond a predetermined point they could get the robot to shut down completely. If this had occurred during an actual life-saving procedure the outcome could have been fatal. Fortunately, the researchers also figured out ways to encrypt the device—the exact type of precaution the FDA encourages in its new draft guidance.

Second, in 2013, cybersecurity expert Billy Rios remotely hacked into a Hospira infusion pump. The pump releases controlled amounts of a substance and can be used to administer insulin to a diabetic or chemotherapy drugs to a cancer patient. These pumps are found in almost every hospital and usually sit next to a patient's bed. Hundreds of them can be monitored and controlled from a central station in the hospital. Rios ordered the pump off of eBay for $100 and was able to figure out the device's pre-programmed password by reading its technical manuals. This information, in conjunction with knowledge about the device's software and what network it was operating on was enough to give him access. He then proved he could remotely administer a lethal dose of drugs through the Hospira pump. Luckily Rios is a benign or "white hat hacker" and turned over his findings to the Department of Homeland security. His report galvanized the FDA to issue its first warning about a medical device.

Third, in 2012, Surgeons of Lake County, a small medical practice in Illinois, fell victim to a digital data breach. Hackers accessed the practice's server where e-mails and more than 7,000 electronic medical records were stored. The hackers then encrypted the files and demanded a ransom. The doctors refused to comply and alerted local authorities. They also offered free credit monitoring services to patients following the attack. The medical practice would not discuss the investigation. However, the practice issued a press release to alert the public and the HHS. In a recent alert the U.S. Department of Homeland Security highlighted one weakness affecting approximately 300 medical devices, including drug infusion pumps, ventilators and external defibrillators. It warns that hard-coded passwords that normally allow service technicians to gain access to myriad machines could be used to make nefarious changes if they fall into the wrong hands. A range of medical devices run on standard software such as Windows XP and are vulnerable to common viruses that plague home and office computers. Because the number of events is on the rise, the FDA decided it was time to issue formal guidance about the need to act.

VI. Cybersecurity Principles—Where to Begin!

Cybersecurity refers to ways to prevent, detect, and respond to attacks or unauthorized access against a computer system and its information. Moreover, because cybersecurity affects everyone, cybersecurity is a shared responsibility.

The U.S. Department of Health and Human Services supports the following non-exhaustive list of best practice tips to prevent a cyber incident in the health care industry:

1. Establish a Security Culture
2. Protect Mobile Devices
3. Maintain Good Computer Habits
4. Use a Firewall
5. Install and Maintain Anti-Virus Software
6. Plan for the Unexpected
7. Control Access to Protected Health Information
8. Use Strong Passwords and Change Them Regularly
9. Limit Network Access
10. Control Physical Access

With regard to risk management, a company should have a strategic approach to cybersecurity, which includes performing a risk assessment to its current computer network, as well as policies and procedures. Additionally, a risk assessment will help an organization understand how well equipped it is to protect against, detect, and respond to cyber threats. Once a risk assessment has been completed, an organization should create and develop information technology standards, policies, and procedures that are appropriate, enforceable, and effective within applicable laws and regulations.

A committee should also be created to develop and implement a risk management plan for preventing a data breach. Once a committee has been established, policies should be drafted regarding the privacy and security of business data, which includes the use of encryption, remote access, mobile devices, laptops, email accounts, and social networking sites. In addition, the committee will conduct an inventory of the software systems and data, and assign ownership and categorization of risk; the higher the sensitivity of the information, the stronger the security protections and access control must be.

Thereafter, an organization's IT department, or a third-party consultant should conduct periodic vulnerability scans, penetration tests, and malware scans to protect against potential data breaches, as well as identify new vulnerabilities. Moreover, trainings should be performed for employees so that they are aware of organization's security protocol in place, and protect against the potential for accidentally exposing a client's PHI.

In the event of a breach, an organization should also create a rapid response plan, which includes a variety of specific elements and covers a wide-range of disciplines. Ultimately, a well-constructed data plan, no matter how comprehensive and detailed, is only as good as the team that is responsible for putting the plan into action. Thus, an organization should assemble a rapid response team comprised of strong, capable representatives who will ensure an efficient executed response. The members of the team may include, but are not limited, to the following:

a. <u>Incident Lead</u> - serve as the "captain" of the team, and ensure that the attorney-client privilege is maintained.

b. <u>Executive Leaders</u> - the company's key decision makers as advisors to the data breach response team to ensure that leadership, backing and resources available.

c. <u>IT Department</u> - must ensure that all safeguards are in place to protect against a data breach

d. <u>Legal & Privacy</u> - in-house counsel and/or external counsel to shape a data breach response and help minimize the risk of litigation and fines.

e. <u>Forensics</u> - a third-party who provides investigation/incident response and reputation-saving remediation, data breach notification and cyber litigation support.

f. <u>Public Relations</u> - depending on the size of the data breach may need to report the breach to the media and/or notify affected individuals.

g. <u>Customer Care & Human Resources</u> - appoint representatives from both customer service and HR to provided needed support.

h. <u>Insurance Broker</u> - hire an insurance broker well-versed in cyber coverage to ensure company has the right policy in place in the event of a cyber-breach.

Furthermore, a company should perform Table Top exercises with its Rapid Response Team to test its readiness to respond to a real attack. Thus, by simulating a cyber-attack and incident response it will help an organization to prevent future attacks, and be ready in the event one occurs in order to maintain business continuity.