CLM Claims & Litigation Management Alliance™

ADVANCING ETHICS, COOPERATION AND EDUCATION

CLM 2015 Cyber Liability Summit
October 21, 2015 in New York City

Healthcare: Evolving Claims, Exposures and Regulatory Enforcement

1. Evolving Exposures And Associated Risk

What Data is At Risk?

Certain information a health care provider likely collects and stores relating to its patients and responsible parties imposes an obligation on these providers under both state and federal law to take certain steps to protect the information and disclose any unauthorized access, acquisition, or disclosure of the information.

Pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"), certain healthcare organizations – defined as a covered entity or business associate – are responsible for the safety and security of the protected healthcare information ("PHI") in their care. 45 CFR §164.302. PHI includes health information, including demographic information, collected from an individual that is created or received by a health care provider and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present, or future payment for the provision of health care to an individual and that identifies the individual or could reasonably be used to identify the individual. 45 CFR §160.103. Under the HIPAA Security Rule, covered entities and business associates must implement certain administrative, physical, and technical safeguards to protect the PHI in the healthcare organizations' possession. 45 CFR §164.308, 45 CFR §164.310, 45 CFR §164.312.

Healthcare organizations also typically possess certain data, like Social Security numbers, that constitutes personally identifiable information ("PII") and creates duties under various state laws. Additionally, some states, like California, Florida, Montana, Nevada, Oregon and Wyoming, include or will be including, certain types of health or medical information as personal information protected under these states' laws. The duties under these laws typically include notice to the individuals whose information was accessed or acquired without authorization. Under certain state laws, notice to state regulators and consumer reporting agencies may also be required.

What Are The Threat Vectors?

The security of PHI and PII is threatened on a daily basis by a number of sources. Several key threat sources include hackers in the organization's network, phishing scams, malware or viruses, the physical theft of hardware or paper records, employee malfeasance or negligence or through third-party

vendors. Recent, well publicized attacks on healthcare organizations have been attributed to foreign actors but the source of an attack can come from anywhere. Employee negligence can also result in regulatory scrutiny and class action lawsuits.

2. Regulatory Environment – Federal and State

Healthcare organizations face a patchwork of federal and state regulations that govern the protection of health and medical information and the duties or obligations that result from an incident involving unauthorized access or acquisition of such information. Healthcare organizations are under increased scrutiny from federal and state regulators following recent well publicized attacks on healthcare organizations.

a. Federal Regulatory Environment

HIPAA provides a set of national standards to protect PHI that is created, received, used or maintained by a covered entity or business associate. It imposes specific reporting requirements and deadlines upon entities in the event of a breach or security incident. 45 CFR §164.404 - 45 CFR §164.410. A breach is defined as the acquisition, access, use or disclosure of PHI in a manner not permitted that compromises the security or privacy of the PHI. 45 CFR §164.402. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

Under HIPAA, a covered entity must notify individuals whose PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of a breach of unsecured PHI. 45 CFR §164.404 (a). This notice must be provided no later than 60 calendar days following the discovery of a breach, and breaches are treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. 45 CFR §164.404(a) - (b). A covered entity is deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity. 45 CFR §164.404(a)(2). Depending on the circumstances, this notice must be provided by written letter, website posting and/or through the media. 45 CFR §164.404(d), 45 CFR §164.406. Notice must also be provided to the Secretary of the U.S. Department of Health and Human Services (HHS), and this notice is provided via web form and, if it involves more than 500 individuals, will be identified online. 45 CFR §164.408(a). For breaches involving more than 500 individuals, notice must be provided to the Secretary at the same time as notice to affected individuals and no later than 60 calendar days following discovery of a breach. 45 CFR §164.408(b). Breaches affected less than 500 individuals may be reported to the Secretary 60 calendar days after the end of the calendar year of the breach. 45 CFR §164.408(b).

If a covered entity or business associate suffers a security incident, HIPAA does not impose an obligation on the organization to disclose the incident to impacted individuals or to the U.S. Department of Health and Human Services; however, if the security incident is suffered by the business associate, it must disclose it to the covered entity without unreasonable delay and in no case later than 60 days following discovery of the security incident. 14 CFR §164.314(a)(2)(i)(C). This will not change a contractual obligation a business associate may have to report it sooner, and in a specific fashion, to the covered

entity and other parties that may not be impacted but may require notice of any security incidents the business associate suffers while in contract with the parties.

The Office for Civil Rights ("OCR") within HHS has the authority to investigate compliance with HIPAA. 45 CFR §160, Subparts C, D, and E. OCR will likely investigate any breach involving over 500 affected individuals; however, incidents involving less than 500 individuals are not immune to such scrutiny. As part of this investigation, OCR will request information relating to the reporting entity's compliance with the Privacy Rule, Security Rule and Breach Notification Rule. Likely initial requests include documentation supporting compliance with these rules, including:

- A written narrative of the incident and any policies or procedures for reporting known or suspected data incidents;
- Description and documentation of corrective actions taken in response to the incident, including relevant policies and procedures;
- A copy of the entity's Risk Analysis and procedures for performing the Risk Analysis;
- A copy of the entity's most recent Risk Management Plan;
- A description of relevant HIPAA training for employees;
- A copy of all relevant notices and any policies or procedures for providing notice; and
- A copy of any law enforcement reports.

The length and results of OCR's investigation may vary, and can conclude in one of several ways:

- No Further Action Taken: letter to the entity indicating that the Secretary has determined that further action is not warranted.

- Voluntary Compliance: the entity cooperates with HHS in obtaining compliance with applicable administrative provisions.

- Corrective Action Plan: entity agrees to comply with an agreement prepared by HHS to ensure entity's compliance with applicable HIPAA provisions.

- Lawsuit: OCR may refer a complaint to the Department of Justice for investigation if complaint describes action that could be in violation of criminal provision of HIPAA. Entity may also appeal imposition of civil money penalty by the Secretary.

HHS has entered into 21 resolution agreements to date,
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

Concentra Health Services (Concentra)

- Unencrypted laptop containing protected health information of 870 patients.
- OCR found: Concentra failed to adequately remediate and manage its identified lack of encryption and failed to sufficiently implement policies and procedures to prevent, detect, contain, and correct security violations to reduce its identified lack of encryption.
- **$1,725,220 settlement**

State-Run Community Mental Health Facility

- Organization failed to patch systems and continued to run outdated, unsupported software

- This condition led to malware infection resulting in exposure of 2,743 medical records
- **$150,000 settlement**

Presbyterian Hospital & Columbia University (2014)

- PHI accessible through internet search engines related to 6,800 individuals.
- OCR investigation found: hospital made no effort to assure the server was secure or contained appropriate software protections; no thorough risk analysis or risk management plan; failed to implement appropriate policies or to enforce those it did have in place
- **$4.8 million settlement**

The Federal Trade Commission ("FTC") also has a health breach notification rule. 16 CFR Part 318. This rule applies to vendors of personal health records not governed by HIPAA and related entities and requires these vendors and entities to notify consumers of a breach of unsecured information. 16 CFR §318.3(a)(1). The rule applies if you are: a vendor of personal health records (PHRs); a PHR-related entity; or a third-party service provider for a vendor of PHRs or a PHR-related entity. Examples of such a vendor include companies like Microsoft Corporation and Intuit, Inc. Under this Rule, the vendor or entity must also notify the FTC. 16 CFR §318.3(a)(2). This notice is provided via a standard form found at www.ftc.gov/healthbreach. As with HIPAA, notice must be provided within 60 days of discovery of a breach. 16 CFR §318.4(a). If more than 500 individuals are affected, notice is required to the FTC within 10 business days of the discovery of a breach. 16 CFR §318.5(c). If the breach affects less than 500 individuals, notice must be provided to the FTC within 60 days following the end of the calendar year. 16 CFR §318.5(c). Similar to HIPAA, notice may also be required to the media and/or through the vendor or entities website. 16 CFR §318.5(a)-(b). The FTC may audit or investigate incidents and may issue fines of up to $16,000 per violation. The FTC has become increasingly active in investigating breached entities and it is expected that the FTC will continue to aggressively investigate reported breaches under the authority granted it through, among other things, its health breach notification rule.

b. State Regulatory Environment

Currently there are 47 states that have laws requiring notice to affected state residents following the unauthorized access and or acquisition of personal information. While each state defines personal information differently, all states include the resident's name plus Social Security number as personal information. As noted above, some states include medical and/or health insurance information as personal information protected under state law. Some state laws, however, do explicitly state that compliance with federal law is deemed to be compliance with state law (even if the state law requirements regarding timing and content of notice differ from the federal timing and content requirements). *See* CA CIVIL § 1798.82 (e).

3. HIPAA Today And Extending To Business Associates

Under HIPAA, a business associate is an entity that creates, receives, maintains or transmits PHI for a function or activity covered under HIPAA. These functions or activities can include claims processing or administration, data analysis, protections or administration, quality assurance, patient safety activities, benefit management, practice management or providing consulting, data aggregation, management or administrative services to or for a covered entity. This can include subcontractors that create, receive, maintain or transmit protected health information on behalf of a business associate.

Federal regulations require that business associates comply with the HIPAA Security Rule, which imposes some specific security standards, in addition to administrative, physical and technical safeguards. Separate from these direct HIPAA requirements, agreements between covered entities and business associates may broaden or add to HIPAA requirements. Failure to comply with the obligations contained in HIPAA or any existing business associate agreement can result in liability for the business associate. This liability can include fines and penalties assessed by the Department of Health and Human Services or state regulators, litigation from the affected covered entity client, and litigation from individuals affected by data breaches. Of the 475 breaches affecting 500 or more people reported to the Department of Health and Human Services between September 23, 2013 to May 31, 2015, almost 20% of those breaches involved or originated with a business associate. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Business associates and covered entities often times enter into contracts whereby a business associate is required to disclose a breach or security incident impacting a covered entity within a period of time shorter than required by law. Sometimes, the contract even requires a business associate to undertake satisfaction of a covered entity's legal obligations to disclose an incident, or pay for the covered entity to do so. It is important that business associates agree in writing to an achievable deadline to provide such notice (i.e. 15 business days as apposed to 24 hours) and to understand what obligations they may have as a result of an incident under the contract, which may be different than those obligations imposed by state or federal law.

4. Data Analytics Role In Cyber Risk Identification

Knowing expected loss due to cyber breach is essential to determine the cyber limits for any business. Data analytics has come a long way in developing predictive modeling to help risk managers with a decision point in addition to traditional benchmarking.

5. State Of Cyber Insurance Market

With the increase in claim activity in retail and managed care, markets are readjusting their underwriting guidelines. Increased demand and change in appetite for limits has led to some interesting results while placing cyber lately.

6. Mitigation Strategies For Healthcare Data Breach Incidents

Mitigation efforts can be undertaken both before an incident, and after an incident. Before an incident occurs, an organization should:

- Identify what information it has, who has access to this information, whether the individuals that can access actually need access to the information, and if the organization has any need for the information to be on its systems or in its possession or controls.
- Train all individuals that have access to protected information on what is permitted and what is not permitted. This training should be done regularly, both at the time of hire and on at least an annual basis.
- Identify what obligations an entity has pursuant to law and contract to protect information in its possession or control, and identify whether these obligations are being satisfied.
- Identify what contracts are in place that may impose obligations different or additional to those imposed by state or federal law.

- Prepare an Incident Response Plan, which identifies the steps to be taken in the event of a potential or actual incident and the key staff identities and roles in the incident response process.
- Vet vendors that may be needed in investigating and responding to an incident. These vendors' services may include legal, forensic, public relations, monitoring, mailing, and call center.

After an incident occurs, an organization should:

- Confirm that incident has been contained.
- Follow applicable state and federal laws governing notification to affected individuals, regulators and consumer reporting agencies.
- Identify contributing factors to incident, develop and implement plan to correct those factors.
- Retrain employees on applicable policies and procedures to prevent future similar incidents.