Are You Prepared to Be Hacked? Anthem and Premera Breaches Remind of Need for Data Security Incident Readiness

Anthem and Premera Breaches Remind of Need for Data Security Incident Readiness

The recent record-setting data breach at Anthem, Inc. ("Anthem") involving nearly 80 million individuals, and a similar data breach at Premera Blue Cross ("Premera") involving as many as 11 million more individuals, underscore the important and challenging task of safeguarding consumer health data. When coupled with the looming promise of Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Security Rule audits, the growing number of class action lawsuits being filed on behalf of affected individuals, and the fact that data security incidents have become a high-level focus of a myriad of state and federal regulatory and law enforcement agencies, it is clear that data security is (or should be) on the top of the "to do" list of the executive team, boards of directors, and compliance and privacy officers of health care providers, health plans and their business associates. What lessons do the Anthem and Premera breaches offer?

Details of Anthem Data Breach: On February 5, 2015, Anthem, the nation's second largest health insurance company, announced that it had been the target of a sophisticated external cyber attack involving the information of nearly 80 million current and former Anthem members, as well as Anthem employees. The attack represents the largest reported health care data breach to date. According to Anthem's President and CEO, Joseph Swedish, the attackers gained access to personal information including names, dates of birth, medical IDs/social security numbers, street addresses, e-mail addresses and employment information, including income data. Once the attack was discovered, Anthem reports that it took immediate steps to close the security vulnerability, contacted the Federal Bureau of Investigation ("FBI"), and retained Mandiant, a leading cybersecurity firm, to assist in evaluating Anthem's IT system and identify security solutions. In the midst of ongoing public demands to speed up the notification process,

POSTED:

Apr 2, 2015

RELATED PRACTICES:

Health Care
https://www.reinhartlaw.com/practices/health-care

RELATED SERVICES:

Data Privacy and Cybersecurity
https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity

RELATED PEOPLE:

Heather L. Fields
https://www.reinhartlaw.com/people/heather-fields

Melissa Y. Lanska
https://www.reinhartlaw.com/people/melissa-lanska

Anthem is still in the process of notifying members and employees whose information had been accessed.

Details of Premera Data Breach: On March 17, 2015, Premera, a health plan based in Washington state, announced that it had also been the target of a "sophisticated" cyber attack involving the information of as many as 11 million current and former plan members. The data breach reportedly involved personal information, including names, dates of birth, Social Security numbers and bank account information. Premera discovered the data breach in January 2015, but claims the cyber attack started as early as May 2014. Similar to Anthem, shortly after discovering the data breach, Premera coordinated an investigation with the FBI and Mandiant, as well as offered credit monitoring to affected individuals. A multistate investigation involving officials from Washington, Alaska and Oregon has already been launched to examine Premera's internal operations. Specifically, involved officials have expressed concern with respect to the amount of time it took Premera to notify its policyholders of the breach.

Multiple Levels of Regulation and Potential Liability

Multi-jurisdictional data breaches such as Anthem's implicate a number of federal and state data privacy and cybersecurity laws, as well as trigger an onslaught of notification requirements.

- **HIPAA:** To the extent that breached information constitutes protected health information, it will be subject to HIPAA's Breach Notification Rule and written notice to both the affected individuals and the federal government is required. If OCR determines that appropriate data security safeguards were not in place as required by HIPPA's Security Rule (the "Security Rule"), civil monetary penalties are a real possibility.

- OCR's new enforcement focus is evidenced by its recent actions taken in connection with the breach of unsecured protected health information as reported by Alaska based behavioral health provider Anchorage Community Mental Health Services, Inc. ("ACMHS"). In the resulting December 2, 2014 settlement agreement, ACMHS agreed to pay $150,000 and implement a comprehensive, and costly, corrective action plan. Notably, OCR concluded the breach—caused by malware—was the direct result of ACMHS's failure to ensure its IT resources were up to date, supported and regularly updated with

available patches. Among other things, the settlement agreement required that ACMHS provide OCR its updated Security Rule policies and procedures within 60 days and annually report to OCR the status of its Security Rule compliance for the next two years.

- **Federal Trade Commission Act ("FTC Act"):** The FTC Act prohibits unfair or deceptive commercial practices, including those that affect consumer privacy and data security, and applies to most companies and individuals doing business in the United States. In the event that the Federal Trade Commission ("FTC") determines that an affected provider, plan or business associate failed to take reasonable and appropriate steps to protect personal information, or even failed to comply with its published privacy policies, the FTC may bring an enforcement action for unfair or deceptive trade practices.

- **Other Federal Laws:** Depending on the type of organization and information breached, additional federal privacy and security laws may apply including, among others, the Gramm Leach Bliley Act (regulating the collection, use, protection and disclosure of personal information by financial institutions); the Fair Credit Reporting Act (regulating how consumer reports and credit card account numbers can be used and disclosed); the Fair and Accurate Credit Transactions Act's Red Flags Rule (regulating the identity theft monitoring and mitigation programs of financial institutions and other businesses offering credit); and the Health Breach Notification Rule (regulating the breach of unsecured health information by certain businesses not covered by HIPAA).

- **State Laws:** In addition to the aforementioned array of federal data privacy and cybersecurity laws, more than 40 states have enacted some form of data breach notification laws. Some of these exceed what is required in other federal statutes, such as HIPAA. For example, under the recently enacted Florida Information Protection Act of 2014, any entity (health care or not) that acquires, maintains, stores or uses personal information of Florida residents must report data breaches to affected consumers within 30 days. State laws range from general privacy statutes to medical information and consumer fraud statutes.

- **Private Lawsuits:** In addition to specific state privacy and security laws, individuals whose information was improperly accessed also often bring claims against the breached entity for common law negligence and traditional privacy torts, including intrusion upon seclusion, public disclosure of private facts, and even negligent infliction of emotional distress. For example, within a month of the Anthem breach, more than 50 civil class action lawsuits related to the

breach had been filed.

Next Steps

Given the increasing frequency of sophisticated cyber attacks aimed at acquiring consumer and patient data, as well as OCR's recent focus on Security Rule compliance, organizations and, specifically, health care providers, should take a proactive approach not only to HIPAA and data security, but also ensure they are prepared to handle a large-scale breach event. To this end, we recommend that health care clients take the following action steps:

- Develop a comprehensive policy aimed at monitoring for, investigating and responding to data breaches. In addition to legally-required steps mandated by state or federal law, this policy should include internal and external communication plans, identify individuals within and without (e.g., outside counsel) responsible for organizing the response and executing mitigation and remediation steps, and agency contact lists to notify appropriate authorities.
- Review the status of HIPAA Security Rule risk analysis and risk assessment documentation and procedures, and ensure that appropriate and required HIPAA Security Rule policies and procedures are in place and current, as well as fully implemented through education and training. Review the previous Headlines in Health Care Law E-Alert about this topic.
- Consider an external review of data security risk assessment and risk management programs to identify potential risks and vulnerabilities.
- Ensure ongoing reviews of IT systems for unpatched vulnerabilities or unsupported software that could expose consumer and patient information to malware or other risks are taking place.

The professionals at Reinhart Boerner Van Deuren s.c. are available to assist you in assessing your data security and Security Rule compliance. Please feel free to contact Heather Fields, Melissa York or your Reinhart attorney to discuss any questions or concerns related to your organization.

these materials to you does not create an attorney/client relationship. You should not provide confidential information to us until Reinhart agrees to represent you.