AXELEOS CONSULTING

Introduction

This case study provides a high-level overview of a security breach of a healthcare provider that resulted in the disclosure of electronic protected health information (ePHI) of over 1,200 individuals. The purpose of this case study is to provide information on the nature of the breach and a review of security measures that, if implemented, would have significantly reduced the likelihood of a breach. The name of the provider and some non-salient details have been anonymized, omitted, or modified to protect the provider's privacy.

HIPAA/HITECH Compliance Case Study

Business Profile

Acme Health Services is a nonprofit healthcare clinic with approximately 20 providers offering primary care, dental, and mental health services. In addition to the providers, Acme employs around 25 employees. Acme has been in business for approximately 25 years, with an estimated patient base of roughly 5,000 patients.

Details of Breach

The breach was discovered in July 2014 and reported to the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) shortly thereafter. An investigation revealed that the breach affected the ePHI of over 1,200 individuals or roughly 25% of Acme's patient base.

Key Points

- **Acme Health Services, a nonprofit healthcare clinic, suffered a breach affecting over 1,200 individuals**
- **OCR's investigation into Acme revealed systemic noncompliance with the HIPAA Security Rule.**
- **Acme failed to implement any policies and procedures necessary for HIPAA compliance.**
- **OCR levied a $75,000 fine and required Acme to adhere to a Corrective Action Plan, including two years of monitoring by OCR.**
- **The total estimated cost of Acme's breach is estimated between $350,000 and $600,000**
- **The estimated cost to have implemented proper security measures pre-breach is less than a tenth of the total estimated cost of the breach.**

HHS OCR Investigation & Corrective Action

During OCR's investigation of the clinic, multiple serious violations were discovered. Specifically, the OCR noted that:

- Acme failed to implement any policies and procedures under the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164).
- Acme failed to conduct any risk analyses of its systems, security controls, and business associate agreements.
- Acme did not provide security awareness training for its providers and employees.

The OCR's corrective action agreement required that:

- Acme pays a $75,000 fine.
- Acme conducts a thorough and complete risk analysis of their IT infrastructure, which includes performing a full inventory of all computer assets including, but not limited to, workstations, laptops, tablets, and servers. The risk analysis must be submitted to OCR for review and approval.
- Acme implements complete policies and procedures that address, at a minimum, Privacy Rule, Security Rule, and Breach Notification provisions under 45 C.F.R. §164. The policies and procedures must be updated annually and submitted to OCR for review and approval.
- Acme must implement a security awareness training program and require all employees and providers to take the training. The training program must be submitted to OCR for review and approval.
- Acme will be subject to monitoring by OCR for a period of two years. During this time, Acme must submit annual reports to OCR that include, among other items, copies of policies and procedures, training materials, and evidence of the implementation of security measures.

Estimated Costs as a Result of Breach

In addition to the fine levied by the OCR, the costs associated with the breach are estimated to be between $350,000 and $600,000. This estimate takes into consideration the following elements:

- Potential costs of hiring and retaining competent, qualified IT and information security professionals to analyze, remediate, and adequately maintain the clinic's technological landscape.
- Potential costs of developing and implementing a security awareness training program and tracking employee compliance with the training.
- Potential administrative costs of developing, disseminating, and maintaining a proper risk management program and required policies and procedures.
- Potential administrative costs associated with maintaining compliance with the OCR's Corrective Action Plan.
- Potential costs of providing identity theft monitoring services to the affected individuals.
- Potential settlement of legal action brought by the affected individuals, including legal representation costs.

Analysis & Prevention Theory

Acme's breach uncovered several elements that contributed to the impermissible disclosure of their patient's ePHI.

Written Security

All security measures taken by an organization begin with written policies and procedures. It is impossible to adhere to proper security practices without these crucial documents. At a minimum, the following policies and procedures should have been implemented and adequately disseminated to all employees and providers:

- Proper Uses and Disclosures of PHI
- Risk Analysis Policy & Risk Management Process
- Acceptable Use Policy
- Encryption Policy
- Minimum Security Standards Policy
- HIPAA Training Policy

Although this is not an exhaustive list, these six policies would have provided the beginning elements of a proper security posture for Acme.

Practical Security

Although the in-depth details of Acme's IT infrastructure are not known, the following aspects of a practical security program would likely have significantly reduced the chances of a breach:

- Proper file permissions should have been implemented. By employing the security principle of "least privilege," securing files related to ePHI would have made it more difficult to exploit that data.
- Robust encryption, both in-transit and at rest, is the single most effective method to protect data against unauthorized use or disclosure. Although encryption is not a "silver bullet," encryption dramatically enhances the protection of the data. Most hackers are looking for "low hanging fruit" and are much less likely to attempt to decrypt data and will instead look for easily accessible unencrypted data.
- Antivirus and antimalware systems would have protected Acme's systems from malicious software and reduced the likelihood of a breach caused by a virus or malware.
- Data loss prevention (DLP) software would have prevented the likelihood of ePHI being intentionally or unintentionally placed on a jump drive or sent out via email. Most DLP solutions will detect the presence of protected information such as ePHI in email attachments and will block emails with this information from being sent. Further, DLP solutions will disallow the copying of protected information onto portable media such as external hard drives and jump drives.

Security Training

All organizations should have a comprehensive security awareness training program that educates employees on the importance of good security practices. Indeed, HIPAA requires such training for all covered entities and business associates (see 45 CFR § 164.530(b)(1)). While HIPAA does not explicitly require recurring training, it is considered a best practice to require employees to undergo training at least annually to ensure security remains top of mind.

Conclusion

Acme Health Services failed to implement many of the crucial elements required of a covered entity under HIPAA. OCR uncovered longstanding and systemic non-compliance with HIPAA's Security Rule. As a result, Acme was fined tens of thousands of dollars and will likely incur hundreds of thousands of dollars to effectively remediate the numerous vulnerabilities in their organization. Acme could likely have avoided these expenses for less than a tenth of the total cost because of this breach.

The breach of Acme Health Services is just one of numerous breaches that have occurred in the healthcare space. It is not a question of if, but when a healthcare provider will encounter a breach in their systems.

Axeleos has in-depth subject-matter expertise in assisting HIPAA covered entities and business associates with implementing proper security measures, developing policies and procedures, and creating a structured and practical training program for their employees.

Contact Axeleos today by emailing hipaa@axeleos.com and let us help you protect your practice from becoming the next Acme Health Services.