Cyber Risks a University Faces as a HIPAA Business Associate

Anurag Shankar
Center for Applied Cybersecurity Research <ashankar@iu.edu>
Indiana University
October 21, 2016

Background

HIPAA defines a "Business Associate" or BA as a third party that provides a function or performs an activity for a covered entity (CE) that involves the use or disclosure of protected health information (PHI). With a few exceptions, a BA under HIPAA is any vendor who is exposed or could potentially be exposed to the CE's PHI whether or not it does or can view it. An organization can also be a CE and a BA simultaneously. Universities with medical centers often belong to this category. Their healthcare components nearly always have BAs that provide services such as billing, medical transcription, IT, etc., but they also provide services to other CEs such as hospitals and medical practices. Some of these services may involve exposure to the BA's ePHI, with or without the university's knowledge. This exposes universities to the risk of breaches of the BA's PHI.

HIPAA breaches can have a large impact on an organization, including financial and reputational loss. While much has been written about BA breaches affecting a CE, scant attention has been paid to the risk a third party assumes by deciding to become a BA. This document attempts to address this gap in the special case when a university is the BA.

Legal Liability

Since its inception, HIPAA has required a formal business associate agreement (BAA) between a CE and a BA that includes HIPAA specific clauses for issues such as breach notification, reporting, etc. BAs were however exempt from HIPAA liability and penalties until recent HITECH changes to the regulation made BAs directly liable under the HIPAA Security Rule.

Risk

A Ponemon Institute study[1] indicates that 90% of all healthcare organizations and almost 60% of their BAs reported having at least one data breach involving PHI in the past 24 months. Forty one percent of the BAs identified the attacker as a cybercriminal and 9% a malicious insider. The study reported the average cost of a breach to the BA to be $1 million. This includes many factors such as risk incident response, risk remediation, notification, etc.

[1] https://www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data

© Indiana University

When external CEs use a university's systems to either manage PHI for joint projects or for their own, internal use, they are exposing the university to the following risk and liability ("CE" below refers to the entity to who the university is acting as a BA):

1. Legal and Financial

    a. *Breach attributable to the CE*. Let us assume that the breach exposes only the CE's PHI (and not the university's). The university faces limited risk in this case since the customer bears most of the liability. The CE has to:

        i. Investigate the breach
        ii. Notify the government, media, and those affected
        iii. Face penalties and litigation from customers
        iv. Provide identity protection
        v. Face potential loss of revenue
        vi. Rebuild reputation and trust

        The university on the other hand has to:

        i. Investigate the breach
        ii. Notify the customer (CE) of the breach within 60 days
        iii. Work with the CE on a joint notification to the government
        iv. Face (some) media exposure
        v. Mitigate risk

        The primary liability for the university in this case is the cost of the breach investigation and FTEs required for risk mitigation.

    b. *Breach attributable to the university*. Again, let us assume that the breach exposes only the CE's PHI. Due to attribution, the university now faces new risks in addition to those listed in (a). They include:

        i. Indemnification and Litigation – if the Business Associate Agreement (BAA) with the CE includes an indemnification clause and/or if the CE decides to take legal action against the university.

        ii. Termination of Contract/Loss of Revenue – if the university is being compensated for services provided and the breach results in the CE terminating the contract.

    c. *Breach of the university's PHI*. The university acting as a BA faces an added risk of exposing its own PHI due to an increased threat surface from the CE accessing its systems. In case of a breach exposing both the CE and its PHI, it now faces the additional burden of responding to the breach as a covered entity itself. It should

however be noted that, if the breach is entirely attributable to the university, it may not be caused by the university being a BA, i.e., it may be due to existing vulnerabilities waiting to be exploited, independently of the university's BA status.

2. Administrative

    a. *Loss of Control*. There is an inherent asymmetry to the BA-CE relationship. The BA typically has little or no control over the CE's security practices. This may increase the chance of a breach at the university, for instance if the CE lacks security rigor.

    b. *Audits*. As a BA, the university exposes itself to the risk of an audit.

        i. The CE or the government can request access to the university's documentation of its internal policies and procedures, books, and records relating to the use and disclosures of PHI.

        ii. The university becomes subject to a random BA audit by the government.

    c. *Overhead*. the university subjects itself to administrative overhead as a BA.

        i. BAA. There can be a significant cost due to the time and effort it takes to create, execute, and maintain a BAA.

        ii. Subcontractor BAAs. Being a BA obliges the university to establish BAAs with subcontractors (such as software or hardware support vendors) that may have access to the CE's PHI.

        iii. Accounting of Disclosures. Being a BA obliges the university to provide an accounting of disclosures to the CE or the individual whose PHI the university holds.

        iv. Disposal of PHI. The BAA may require the university to bear the cost of returning and destroying the PHI it holds.

3. Attacks

    a. *Secondary Attacks*. As a BA, the university exposes itself to an increased risk of a breach from attackers originally targeting the CE but moving laterally to the university. The likelihood of such attacks is on the rise since CEs such as hospitals are now a rich source of medical records that yield a premium on the black market.

    b. *Insider Attacks*. As a BA, the university becomes a target for disgruntled employees and other malevolent actors associated with the CE.

Conclusion

This short article attempts to outline the factors that come into play when a university or another organization decides to become a HIPAA business associate for another covered entity. The issues discussed are sometimes unknown or unappreciated, leading to an incomplete understanding and potentially unfortunate consequences. It is sincerely hoped that the material presented above is useful to both existing business associates and those contemplating such a move.

Acknowledgements

The author is grateful to Leslie Pfeffer and Andrew Marsh, the University HIPAA Privacy and Security Officers at Indiana University, for useful discussions relevant to the material presented and for reviewing this paper.