Practice Management Bridge®

HIPAA and Business Associates: The IT Professional

Many IT professionals and companies fail to understand that HIPAA obligations, and the consequences for non-compliance, extend beyond the dental and healthcare practices they serve. The relatively recent enactment of HIPAA's Omnibus Rule on September 23, 2013 added new requirements and responsibilities. With Omnibus, the U.S. Department of Health and Human Services now has the authority to investigate business associates directly, and will undoubtedly pursue actions against data breaches initiated by business associates. Of the data breaches reported to the Department of Health and Human Services since the enactment of the Omnibus Rule, almost 20% involved or originated with a business associate.

HIPAA uses a broad definition of "business associate": anyone who creates, receives, maintains or transmits protected health information ("PHI") for a function or activity covered under HIPAA. Simply selling software to a practice subject to HIPAA will not necessarily establish a business associate relationship with them. But if a vendor needs access to the customer's PHI, the business associate relationship most likely exists. The vendor can also inadvertently create a business associate relationship simply by storing PHI data – even when there isn't a formal agreement in place or not. These dynamics create inherent risk for IT professionals working with dental and medical practices.

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.In addition to direct HIPAA requirements, the type of work performed and specific provisions contained in IT consulting agreements can broaden or add to HIPAA requirements.

> **Of the data breaches reported to the Department of Health and Human Services since the enactment of the Omnibus Rule, almost 20% involved or originated with a business associate.**

Failure to comply with the HIPAA obligations or any existing business associate agreement can result in liability for you as 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 customer and litigation from individuals affected by data breaches. To help IT professionals better understand the current landscape and potential pitfalls, we've spelled out selected HIPAA requirements on the following pages.

ADMINISTRATIVE SAFEGUARDS

HIPAA contains a variety of required administrative safeguards, including conducting a risk analysis, risk management, and multiple policies and procedures relating to the proper protection and accountability of PHI. All business associates must conduct an assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of PHI. They also must prioritize the risks and implement an appropriate management plan, which incorporates sufficient security measures to reduce risks and vulnerabilities to a reasonable and appropriate level.

HIPAA and Business Associates: The IT Professional

HIPAA also requires that covered IT professionals implement a HIPAA security awareness and training program for all employees, including management and regularly review records of information system activity, including audit logs, access reports and security incident tracking reports.

Employees who fail to follow HIPAA compliant security policies and procedures must be sanctioned and business associates must also perform a periodic technical and nontechnical evaluation of the policies and procedures designed to meet the various requirements laid out in the subsection on administrative safeguards. HIPAA requires that documentation of "satisfactory assurances" that the administrative safeguards required are in fact in place.

These safeguards, and satisfactory assurances requirements also apply to any subcontractors used to create, receive, maintain or transmit protected health information. Business associates typically satisfy this requirement through the agreement between a covered entity and a business associate or between a business associate and its sub-contractor.

PHYSICAL SAFEGUARDS

HIPAA imposes additional safeguards to limit physical access to a customer's PHI, along with policies and procedures governing the receipt and removal of hardware and electronic media containing PHI into and out of a facility, and the movement of these items within a facility.

TECHNICAL SAFEGUARDS

The section of HIPAA covering technical policies and procedures for electronic information systems that contain or maintain PHI requires that this information is only accessible to individuals or software programs that have been granted access rights. Requirements under this subsection include unique user identification, emergency access procedures, automatic log off and encryption of PHI in transit.

All covered entities must implement hardware, software, and/or procedural mechanisms that record and examine activity of any information system containing or using PHI. Finally, this section requires policies and procedures to prevent improper alteration or destruction of PHI.

CONTRACTURAL PROVISIONS

HIPAA requires that covered entities and their business associates enter a formal business associate agreement. This agreement typically incorporates by reference HIPAA Security Rule and the obligations. Additionally, these agreements may require business associates to indemnify customers from any claims resulting from violating any HIPAA provision or the formal agreement. Even if a covered entity isn't initially found liable for a HIPAA violation, business associates could end up being responsible for any HIPAA costs and penalties as a result of the indemnity provisions. Further, these agreements may require further mitigation of any harmful effect caused by a breach of PHI. This mitigation can include notification to affected individuals, identity protection services for the affected individuals and other costs to restore patient good will or reputational repair, all of which can be extremely costly.

Even if a covered entity isn't initially found liable for a HIPAA violation, business associates could end up being responsible for any HIPAA costs and penalties as a result of the indemnity provisions.

HIPAA and Business Associates: The IT Professional

CONSEQUENCES

The consequences of non-compliance can vary. Aside from being held directly liable by the Department of Health and Human Services, business associates can be required to cover a multitude of costs associated with any loss or exposure of PHI, including attorney's fees, forensics costs, costs associated with notification and protection services for affected individuals, fines or assessments levied by regulators and potentially costs associated with litigation resulting from a breach of PHI.

By way of example, a collection and billing services firm caused a breach of approximately 20,000 individuals' PHI. In this case, the business associate received an encrypted spreadsheet containing the PHI. The business associate used this data to create a spreadsheet that was then passed along to the business associate's vendor for the purpose of creating a graph. The PHI inadvertently ended up displayed on a public website for almost a year. This incident resulted in litigation against the covered entity, the business associate and the business associate's vendor. The parties ultimately settled the case for $4.125 million dollars, of which the business associate and its vendor contributed $3.3 million. Business associates are subject to direct investigation and enforcement by the Department of Health and Human Services for such incidents.

Aside from being held directly liable by the Department of Health and Human Services, business associates can be required to cover a multitude of costs associated with any loss or exposure of PHI

The steep financial cost to both the business associate and its vendor may have been avoided if the entities had complied with the requirements laid out in HIPAA.

Lost or stolen unencrypted laptops also represent significant potential liability. In one case, an encrypted laptop used by the business associate to assist with software troubleshooting for a medical practice or provider was stolen. The business associate was a third party IT vendor assisting a medical practice or provider with a variety of IT needs, including troubleshooting problems with the practice's records software. The IT vendor could receive notice of problems by email from the practice that included screenshots of the issue. These screenshots contained PHI and the emails were stored locally on the computer. As a result of the theft of the business associate's laptop, the IT vendor first had to notify the medical practice or provider. The IT vendor then had to cooperate with its covered entity client with expert forensics brought in to help efficiently identify the affected and potentially affected individuals. In cases where the population affected is large enough, additional printing and mailing assistance may be needed, as well as a call center to adequately support the notice recipients. HHS will also have to be notified.

This type of situation creates additional risk of investigation from HHS and potential litigation. Under the HIPAA Final Rule, HHS will be able to investigate both the healthcare provider as the covered entity and the IT vendor as the business associate responsible for the breach. Any investigation would likely include requests for information beyond just the facts of the breach and will likely extend to requests for copies the policies and procedures, risk assessment documentation, risk management documentation, training documentation and other information required under the various provisions of the Security Rule. The business associate will be required to show compliance or face possible assessments or a corrective action plan.

HIPAA and Business Associates: The IT Professional

Under the corrective action plan, the business associate might have to bring itself into compliance and work with HHS until HHS is satisfied with the policies and procedures put in place. The business entity may also have certain regular ongoing reporting requirements to HHS as a result of a corrective action plan in addition to the fines or assessments HHS imposed for initially failing to comply with the Security Rule.

IT vendors who maintain the network and software for a medical practice must follow the policies and procedures in place and not just put them in place. In some cases IT vendors will undertake responsibilities for patching and updating a practice's IT resources and virus detection systems. Despite these good policies and the presence of virus detection, in one recent case malware managed to make its way onto the practice's system and unauthorized individuals were able to exploit system vulnerabilities to obtain unauthorized access to the PHI of approximately 2,800 patients. A subsequent investigation showed that the malware and resulting compromise could have been prevented had the IT vendor been following the Security Rule policies and procedures in place and regularly updated the practice's IT resources, software and in particular, anti-virus systems. The IT vendor was unaware of the technical requirements under the Security Rule and consequently failed to comply with these requirements on behalf of its covered entity client. The resulting HHS investigation that confirmed the policies and procedures were in established but were not followed. As a result, HHS issued a $150,000 fine and a corrective action plan requiring regular reporting to HHS. While the fine may have been issued against the covered entity practice, the practice looked to the IT vendor to cover the fine under the terms of the business associate agreement in place or alternatively sought recovery outside of the agreement on a negligence theory. Under this agreement, the IT vendor agreed to indemnify the covered entity practice for any breach resulting from the IT vendor's negligence or failure to comply with the requirements of HIPAA.

Ensuring full compliance with the obligations and duties laid out in HIPAA puts both dental and medical practices and IT professionals in the best position to reduce or even avoid potential liabilities.

The liability imposed on the business associate and covered entity could have been prevented had the vendor been aware of the requirements imposed by HIPAA and satisfied these obligations.

CONCLUSION

IT professionals must recognize the exposure they face now that HIPAA can apply directly to business associate operations. Compliance with the requirements laid out in HIPAA, particularly the Security Rule, can significantly reduce exposure. Ensuring full compliance with the obligations and duties laid out in HIPAA puts both dental and medical practices and IT professionals in the best position to reduce or even avoid potential liabilities. Compliance starts, however, with an awareness of what HIPAA actually requires. With that awareness, business associates can begin to develop and implement the necessary policies and procedures. It is important to remember, however, that these obligations are not "set and forget," but require ongoing commitment to periodically review HIPAA compliance to ensure that all requirements continue to be met.

HIPAA and Business Associates: The IT Professional

EXHIBIT A: HIPAA TECHNICAL SAFEGUARDS

Note: HIPAA implementation specifications are designated as **Required (R)** or **Addressable (A).**

Addressable specifications must be implemented if reasonable and appropriate, or an equivalent safeguard must be documented.

Access Control — 45 C.F.R. § 164.312(a)

Specification	Type	Description
Unique User Identification	R	Assign a unique name and/or number to identify and track user activity.
Emergency Access Procedure	R	Establish procedures for obtaining necessary ePHI access during emergencies.
Automatic Logoff	A	Implement session timeouts after periods of inactivity.
Encryption and Decryption	A	Encrypt and decrypt ePHI where appropriate, including data at rest and in transit.

Audit Controls — 45 C.F.R. § 164.312(b)

Specification	Type	Description
Audit Logs and Monitoring	R	Implement mechanisms to record and review system activity involving ePHI.

Integrity — 45 C.F.R. § 164.312(c)

Specification	Type	Description
Data Integrity Controls	R	Protect ePHI from improper alteration or destruction.
Mechanism to Authenticate ePHI	A	Implement processes to verify that ePHI has not been altered or destroyed in an unauthorized manner.

Person or Entity Authentication — 45 C.F.R. § 164.312(d)

Specification	Type	Description
Authentication	R	Verify that a person or system seeking access to ePHI is who they claim to be.

Transmission Security — 45 C.F.R. § 164.312(e)

Specification	Type	Description
Integrity Controls	A	Protect ePHI from unauthorized modification during transmission.
Encryption (in Transit)	A	Encrypt ePHI transmitted over electronic networks where appropriate.