eFolder White Paper:
12 HIPAA FAQs for MSPs and VARs

October 2015

Disclaimer

eFolder has made every attempt to ensure the accuracy of the information provided in this document. eFolder assumes no legal liability for the accuracy, completeness, and reliability of the information in this document. eFolder strongly advises that all businesses with questions regarding HIPAA seek the services of a professional HIPAA consultant and auditor.

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was first passed in an effort to increase the portability of health insurance. Today, HIPAA has guidelines and regulations aimed reduce fraud and simplify administration. Although HIPAA regulations apply to health care professionals and entities that have access to patient health information, it is little-known that business associates of health care professionals must comply as well.

The penalties for non-compliance can be hefty: capping at $50,000 per violation and $1.5 million per year. Therefore, it is important that all parties in which HIPAA applies to should have at least the basic knowledge of the act. In this white paper, we will discuss 12 HIPAA FAQs that cover who HIPAA actually protects, who must adhere to its guidelines, and how MSPs and VARs can appropriately comply.

1. What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) was passed into law by Congress in 1996. The purpose of the act is to improve health insurance portability, as well as to reduce fraud and simplify administration. Title I of HIPAA, the original title of the act, works to allow individuals changing or losing their jobs to be able to retain their health insurance coverage without complications. In Title II, HIPAA ensures the privacy and security of individually identifiable patient health information by regulating how protected health information (PHI) and electronic PHI (ePHI) are transmitted, maintained, and disclosed.

The Privacy Rule and Security Rule in HIPAA create guidelines for day-to-day business operations of covered entities. The Privacy Rule protects patient health information by mandating in which situations and with whom PHI can be shared. The Security Rule defines standards for protecting the confidentiality, integrity, and availability of ePHI.

The covered entities under HIPAA include health plans, health care clearinghouses, and any health care providers who uses or transmits electronic personally identifiable health information. In 2013, the final HIPAA Omnibus Rule further expanded HIPAA so that business associates (BA) of covered entities are also required to comply with the Privacy and Security rules. Penalties for non-compliance can result in fines of up to $50,000 per violation and $1.5 million per year.

2. What information is protected by HIPAA?

18 Identifiers Recognized by HIPAA

1. Names
2. Geographical subdivisions smaller than a State
3. All elements of date directly related to an individual; birth date, admission date, discharge data, date of death
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

HIPAA protects individually identifiable health information, termed protected health information (PHI) or electronic PHI (ePHI).

Any combination of an identifier and health information is considered PHI. An identifier is information that reveals the demographics of a patient such as a patient's name or medical record number. There are currently 18 identifiers recognized by HIPAA. Health information is any piece of information related to a patient's health history, diagnoses, treatment, and payment information.

HIPAA protects PHI in all its forms whether written, verbal, or electronic. Electronic forms of PHI include those stored on devices and in the cloud.

3. Why do MSPs and VARs have to comply as Business Associates?

Business associates are any business entities who support covered entities by performing duties that involve the usage, storage, or transmission of PHI. Business associates are also subcontractors who support or perform duties for other business associates. An MSP or VAR who manages data and security for a covered entity, such as a medical clinic, is considered a business associate. An MSP or VAR who manages data and security for another business associate, such as an accounting firm that provides services for a hospital, is also considered a business associate. Business associates come in contact with, or have access to PHI and therefore must comply with HIPAA regulations.

4. What do MSPs and VARs need to have to be HIPAA compliant?

In order to be compliant with HIPAA, MSPs and VARs who are considered business associates must follow HIPAA's standards for administrative, technical, and physical safeguards.

Administrative safeguards are policies and procedures created in the workplace of a covered entity or business associate that define how that entity will comply with the act. These written policies should outline how the business of an MSP or VAR will maintain its HIPAA compliance, such as who has access to ePHI, training programs for the handling of PHI, and how violations will be detected and corrected. A key part of this safeguard is the written contingency plan, which requires that MSPs and VARs have a reasonable plan for ensuring the integrity and availability of ePHI in the event of an emergency or disaster.

Physical safeguards are standards to control physical access to PHI. Only authorized personnel should have physical access to PHI. Policies and procedures need to be written to control how employees of MSPs and VARs use their workstations, how they access equipment containing PHI, and how to properly remove, transfer, or dispose of hardware and software containing PHI.

Technical safeguards are standards to control access to computer systems in order to maintain the security of ePHI. These standards include password encryption so that only authorized employees can access ePHI, proper firewalls to prevent intrusions to information systems that contain PHI, and appropriate network security measures

for the secure electronic transmission of PHI. Finally, audit and integrity controls need to be in place, and MSPs and VARs who are business associates must also complete a documented risk analysis on the security of their ePHI.

5. Can we still do business with a client if they refuse to sign a Business Associate Agreement?

MSPs and VARs can still do business with a client if the client refuses to sign a Business Associate Agreement. However, to ensure that MSPs and VARs won't be responsible for any loss or leakage of ePHI, IT solution providers working with covered entities must act as a business associate, even without a BAA in place. By following all of HIPAA's standards for administrative, technical, and physical safeguards, MSPs and VARs can avoid any penalties that result from a clients' violation of HIPAA.

6. Do MSPs and VARs have a responsibility to report clients who are in violation of HIPAA?

HIPAA mandates that covered entities who are aware of their business associates' non-compliance with HIPAA should advise business associates on the steps needed to achieve compliance and allow them time to implement changes. If business associates, such as MSPs or VARs, neglect to implement the necessary changes to become compliant, covered entities are required to terminate the business relationship and report the non-compliance to the HIPAA enforcement organization. However, MSPs and VARs who are aware of their clients' non-compliance of HIPAA are not required to report the non-compliance to the HIPAA enforcement organization, the U.S. Department of Health and Human Services.

7. Do our clients really need domain networks instead of workgroup networks?

HIPAA requires that all covered entities must have an Individual User Identification standard, audit logs, and information system activity reviews, which all require the use of domain networks.

An Individual User Identification standard requires users who access systems that store ePHI to use unique credentials in order to access these systems. This standard makes all employees who access ePHI identifiable. Audit logs use Individual User Identification to keep track of when and who accessed ePHI, and what files were accessed. Information system activity reviews are required to be conducted periodically using audit logs to review who accesses ePHI, and to detect any security risks. HIPAA also mandates that audit logs be retained for 6 years.

8. If a laptop or device containing ePHI is encrypted and then lost, is it reportable?

When a laptop or device containing ePHI is lost, HIPAA requires covered entities and business associates to immediately notify affected patients and then report the lost to the federal government.

However, if the lost laptop or device is encrypted according to federal encryption standards, 256-bit AES, then the lost device will not need to be reported.

9. Do MSPs and VARs need to sign Business Associate Agreements (BAA) with backup and cloud vendors?

A business associate agreement is a contract stating that a business associate will appropriately safeguard PHI. Covered entities should sign agreements with their MSPs and VARs, who are considered business associates. MSPs and VARs who are considered business associates should also sign agreements with their backup and cloud vendors, who are considered subcontracted business associates. Either party of the agreement may originate the contract.

The BAA can clarify or limit how IT solution providers or their solution vendors can use, store, and disclose protected health information. Under the agreement, all business associates must also implement proper safeguards to protect ePHI.

10. Are cloud vendors and backup providers exempt from HIPAA because the data is encrypted and they don't have the encryption keys?

Cloud vendors and backup providers are considered to be business associates even if the data they provide service for is encrypted. While the Safe Harbor Policy protects entities who lose devices containing encrypted data, this policy is entirely separate from HIPAA. Therefore, cloud vendors and backup providers who have access to PHI are still required to operate as business associates even if they don't have encryption keys to data.

11. How can we verify that our backup and cloud vendors are really HIPAA compliant?

While there is no official certification for the HIPAA compliance of a covered entity or business associate, a compliant backup and cloud vendor should acknowledge that they are a business associate and sign a BAA. In addition, a backup or cloud vendor should also have a documented risk analysis. A risk analysis carefully examines the risks of a business's operations in their efforts to comply with HIPAA. Finally, MSPs and VARs who are business associates should ask their backup and cloud vendors about policies they have in place to safeguard patient health information. Working with a backup and cloud vendor that is HIPAA compliant is important because when a violation occurs, any party involved can be penalized.

Although there is no definite way to verify the HIPAA compliance of a backup and cloud vendor, asking a vendor for their risk analysis and policies will put pressure on and encourage these entities to be compliant. Furthermore, if a vendor refuses to sign a business associate agreement, denies the request for a risk analysis, or will not disclose its policies, then it is probably safer to do business with a different vendor instead.

12. What do MSPs and VARs have to do to become HIPAA-compliant?

All MSPs and VARs who are business associates should learn about HIPAA and have training programs to educate their workforce about HIPAA. With everyone in the workplace knowledgeable about HIPAA rules, employees will be more mindful of their actions when accessing or handling PHI.

To comply with HIPAA, written policies and procedures should be implemented as outlined by the administrative, technical, and physical safeguards in the Security Rule. Written policies will further encourage employees to be attentive when they are working with PHI. Having procedures in place to detect and correct violations will also help maintain the compliance of a business.

MSPs and VARs who are business associates should also have an up-to-date risk analysis. Having a risk analysis will give companies a good idea about how well the policies implemented to protect PHI are working. Updating the risk analysis will also allow a business to identify whether written policies need to be revised.

Finally, it is the responsibility of the business associate to select the right vendors to do business with. To avoid violation penalties, when choosing a vendor, it is important to choose partners who are transparent about their HIPAA-compliance.

Conclusion

The regulations outlined in HIPAA should not be taken lightly. It is clear that personnel working in the healthcare industry are not the only ones who need to be HIPAA-compliant. Covered entities and business associates, including MSPs and VARs, should review the policies and procedures at their company to ensure that appropriate safeguards are implemented to ensure the privacy and security of protected health information.

It is important that MSPs and VARs not only analyze the HIPAA-compliance of their own company but also that of their backup and cloud vendors'. eFolder offers a range of services that are HIPAA-compliant. eFolder will also always sign a BA agreement with partners who are using HIPAA-compliant eFolder services.

To learn more about HIPAA-compliant eFolder services, including backup, BDR, and sync, visit www.efolder.net.

Sources:

"Health Insurance Portability and Accountability Act." *California Department of Health Care Services.* 2015.

"Health Information Privacy." *U.S. Department of Health and Human Services.* 2015. Web.

Corporate Headquarters
2340 Perimeter Park Drive, Suite 100, Atlanta, GA 30341 ▪ 678-888-0700 ▪ www.efolder.net