HIPAA BASICS: YOUR BREACH NOTIFICATION OBLIGATIONS

safemodeIT

HIPAA BASICS: YOUR BREACH NOTIFICATION OBLIGATIONS

Most people are generally familiar with the acronym HIPAA, the federal law that protects the privacy of an individual's health information-- The Health Information Portability and Accountability Act of 1996. We encounter it everytime we visit a medical office.

What tends to get the most attention from businesses that may be affected by the law is the first section of the act, the Privacy Rule. This portion of the law sets the standards and restrictions defining when an individual's health data may be used and disclosed. It is easy to find information about this part of the law. However, the law also has a Breach Notification Rule, which specifies the required actions an entity must take when the Privacy Rule has been violated. This e-guide will define the Breach Notification Rule, outline the major notification requirements, and briefly discuss the exceptions to those notification requirements. It is important to be aware of the Breach Notification Rule because failure to adhere to the timelines can result in significant penalties.

SOME BACKGROUND ON HIPAA

To make sense of your notification obligations under HIPAA, let's take some time to define what HIPAA is all about.

WHAT IS HIPAA?

HIPAA was passed in 1996, and then it was strengthened and expanded in 2006 with the passage of the HITECH ACT. This Act recognized the expansion of electronic health records and seriously increased the penalties and enforcement of HIPAA rules, including a requirement for audits by the Department of Health and Human Services (HHS) of those who are covered by the law. HIPAA creates three basic rules regarding patient healthcare data.

1. **The Privacy Rule:** This rule creates a right for patients to have the privacy of their healthcare data secured, and sets standards about how health data may be used and when it may be disclosed.

2. **The Security Rule**: This second part creates security regulations regarding all Protected Health Information and electronic Protected Health Information (PHI/ePHI). It defines what must be done to protect patient data privacy.

3. **The Breach Notification Rule:** This rule states to whom and when notification must be made when a breach of patient data privacy has occurred. It is the topic of this e-guide.

WHO IS REGULATED BY HIPAA (*WHO WILL NEED TO WORRY ABOUT NOTIFICATION?*)

There are two groups who are covered by these HIPAA rules. The most obvious are healthcare providers, medical offices, insurance companies, pharmacies, nursing homes and other similar organizations. These groups directly handle protected patient data and are called "Covered Entities." There is another set of entities who, one might say, have a secondary role in handling protected health information. These entities are known under the law as "Business Associates." A Business Associate is an entity that, in the role of a

provider of a service or product to a covered entity, has access to, or come in contact with, protected health data. It is not always immediately obvious that an entity is a Business Associate (BA). For example, a BA might be an IT contractor, an accountant, a billing firm, a managed service provider, or a data storage center. Even cloud service providers are covered. Fundamentally, any entity that comes in contact with such data is regulated by HIPAA. Even if they only touch the data in the aggregate and never deal with data at the individual patient level, or if they handle the data in a purely pass-through sense, they are covered by HIPAA and are required to adhere to HIPAA notification rules if a breach occurs on their watch.

WHAT IS A BREACH?

A breach is the unauthorized access by employees or a third party to PHI/ePHI or the disclosure of the data to unauthorized parties. As the Department of Health and Human Services, who administers the Act defines it, "A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information [generally breaches aren't considered to have occurred if it can be demonstrated] that there is a low probability that the protected health information has been compromised."**

Whether you are a Covered Entity or a Business Associate, you are required to provide notification if a breach occurs while you are "in possession" of the PHI/ePHI. Anything that is not permitted under the Privacy Rule is considered a breach.

Examples of breaches that are common are ransomware attacks, successful hacks into the data, and cyber attacks. Another common cause of a violation of the Privacy Rule is when a laptop or the phone of a subcontractor that contains unencrypted PHI/ePHI is lost or stolen. If you follow the news, you are probably aware that these situations are all too common. It is important to note here that if data has been encrypted such that it is rendered useless, the above situations would most likely not be a breach of PHI/ePHI, so be sure all of your data is encrypted.

WHO MUST BE NOTIFIED

It would be very easy to get lost in the weeds of notification, but we can safely narrow it down to the three categories of those who must be notified if a breach occurs: individuals, the US Department of Health and Human Services (HHS), and the media. (Note: state laws may layer additional notifications requirements; however, we are only addressing HIPAA in this guide)

Covered Entities are required to notify individuals of a breach of their PHI/ePHI. HHS specifies the method of contact, usually first class mail, no longer than 60 days after the discovery of the breach. They also specify when notification needs to appear on the Covered Entity's website.

HHS NOTIFICATION

The overall guidelines are that HHS must be notified no later than 60 days after discovery of the breach if greater the 500 individual PHI/ePHIs have been affected. If less than 500 are affected in a single event, HHS generally allows for an annual notification process. In all cases, notifications should occur as soon as possible without unreasonable delay.

MEDIA

Media must be notified if greater than 500 have been affected in a single state or jurisdiction. Generally a press release would be the standard method for notification.

AND FINALLY, EXCEPTIONS.

So are there exceptions? Are there occasions where a breach is not considered a breach?

There a three situations that are exceptions to the Breach Notification Rule and these exceptions *apply only to a breach which occurred at the hands of a person or persons authorized to handle PHI/ePHI under the Covered Entity or Business associate designation.*

1. A person acting in good faith who unintentionally accessed, acquired or used PHI/ePHI

2. A person acting in good faith who unintentionally/inadvertently disclosed protected data to a person who is also authorised to work with the protected data.

3. In the case where the Covered Entity or Business Associate has a reasonable, good faith belief that the unauthorized person to whom the disclosure was made, would not be able to retain the information.

Finally, always remember, the breach notification rule only applies to unsecured PHI — that is, PHI "that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance," according to HHS.

What is the takeaway? You need to understand what your notification responsibilities are in case of a security breach. It is easy to get caught up in compliance policy and forget that HIPAA has rules to follow when a breach occurs, which sadly, is always a very real possibility. This e-guide should be a quick primer and a jumping off point for learning more from a qualified IT services provider how you can be sure you are addressing all of the regulations under HIPAA and the HITECH Act. Remember, there are stiff penalties for any violation of the Breach Notification Rule.

**Disclaimer: This document is for general informational purposes only and is not a substitute for professional legal guidance and the support of a qualified managed service provider specializing in HIPAA ePHI compliance.*

*** https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html*

CONTACT DETAILS

Ron Kulik
CTO-Partner | SafeMode IT
Email: ron.kulik@rmkc.it
Phone: 512-761-7652

View Website