HIPAA Compliance

HIPAA COMPLIANCE: WHY YOU SHOULD CARE

The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996. The main purpose of HIPAA is to provide data privacy and security guidelines for the confidentiality of medical information.

HIPAA Title II sets very specific standards for processing Electronic Protected Health Information (ePHI). It also requires organizations implement guidelines that secure electronic access to healthcare information so they can remain in compliance with privacy regulations set by Health and Human Services (HHS).

> *"The average total cost for a single breach was $4 million, up 29% from 2013."*

The Risk

HIPAA noncompliance is costly. Not only are violators at risk for hefty fines, but they may also be looking at reputation damage, the subsequent loss of their patient base, as well as time and productivity loss.

Take Advocate Health System for example. According to the Office for Civil Rights (OCR), Advocate has been ordered to pay fines in the amount of $5.55 million in the largest HIPAA violation settlement to date for multiple data breaches that occurred in 2013. Two incidents of theft resulted in a total of five laptops being stolen containing confidential patient information including names, addresses, credit card numbers, clinical information and health insurance data.

Over the summer of the same year, a business associate's network was hacked by an outside party. It was determined that the company failed to comply on multiple levels by not physically safeguarding access to their IT system or assessing the risks to its ePHI.

Every year, the Ponemon Institute conducts an IBM-sponsored benchmark study on the cost of data breaches. The 2016 study indicated that the average total cost for a single breach was $4 million, up 29 percent from 2013. That breaks down to a $158 fine per record containing sensitive information. Even in a small practice, that adds up quickly. Ponemon also found that criminal attacks are the leading cause of data breaches in the healthcare industry at 50 percent. Accidental employee actions and third-party error make up the other half. Hard-copy records still need to be stored and disposed of properly but now, with electronic filing being rapidly adopted, practices must take strict measures to ensure the confidentiality of electronic records as well.

> *"So, what can you do to protect your practice and yourself from ePHI HIPAA violations? The first step is to be proactive."*

The Solution

So, what can you do to protect your practice and yourself from ePHI HIPAA violations? The first step is to be proactive. HIPAA Security Rules enforce the technical safeguard requirement, defined as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it." This includes transmission security. Your practice must guard against unauthorized access to ePHI that is transmitted electronically.

That is where email security becomes critical. AppRiver is an email and web security expert that has the tools you need to ensure the compliance with technical security regulations. We offer Email Encryption to help you avoid compliance issues and send your data with confidence.

Dr. Rick Waters, a renowned Consultant to Healthcare, trusts his email encryption to AppRiver and we think you should too.

"The flexibility to read and send the most absolute secure and encrypted email is empowering, whether from your office PC, or from your laptop or phone while on the road."

"The flexibility to read and send the most absolute secure and encrypted email is empowering, whether from your office PC, or from your laptop or phone while on the road."

AppRiver employs proactive technology such as Email Encryption to ensure that all your ePHI is sent within layers of protection before criminals can extract sensitive patient data.

The Benefits

Why Email Encryption? Think of your email as a postcard and all the places it's visible along its journey. You don't want to expose your email to the same risk. Email Encryption provides true mailbox to mailbox security with just one click from an Outlook plug-in, OWA, or mobile app. Once you click the Send Secure button, you can be sure that your message is securely on its way to its recipient.

And a patented delivery slip shows you when your message was received and what the recipient did with it afterwards. With features like FYEO, forwarding freeze, and message recall, you control your encryption. To make it even easier, all Email Encryption features are available on the go so you can send encrypted email from anywhere.

But most importantly, you can count on Email Encryption to help protect your confidential healthcare information and ensure regulatory compliance for your practice.

"Having been in the dental field since 1982 I have seen an amazing evolution of technology. When the Federal government mandated secure email for healthcare, I did thorough research for my many dental clients and picked Email Encryption. If you select it for your team, its merits will go beyond all expectations."

Dr. Rick Waters
Consultant to Healthcare

appriver®

appriver.com
sales@appriver.com
(866) 223-4645