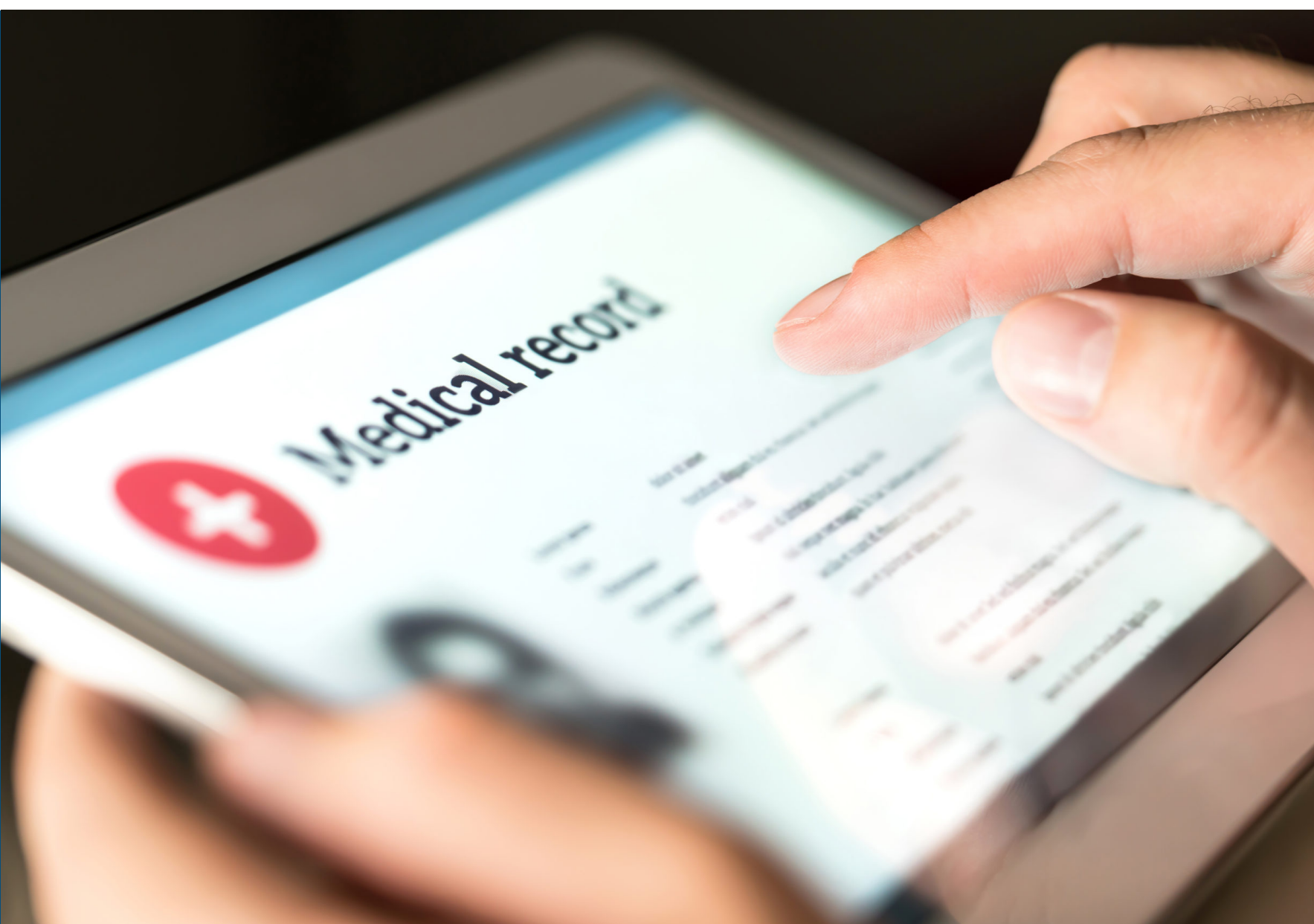


Protecting ePHI Requires More Than Encryption



HEALTHCARE
August 5, 2020

Share
f t in

With healthcare increasingly going online, it’s more important than ever that healthcare organizations be proactive about meeting the HIPAA Security rule and protecting ePHI. Any healthcare organization worth its salt knows that a HIPAA breach can have major legal and clinical repercussions and seriously damage the relationship between patients and healthcare providers. While healthcare providers have understandably turned to encryption as a way to protect ePHI, it’s important to recognize that encryption is not enough. While encryption is an important part of protecting ePHI, it often doesn’t account for compliance – an absolute must when it comes to keeping sensitive information safe. Let’s explore why.

The Limits of Encryption

Encryption is a must-have – but while using it means sensitive information can’t be compromised en-route by a man in the middle attack, it *can* still be breached on devices. Think of end-to-end encryption **like a bodyguard** that picks you up at your house, rides with you to your next destination and escorts you to the destination. You’re safe when you leave the house, en-route, and up until the door of the next destination. But before you leave the house and once you reach your destination, you’re at risk. That’s pretty much how encryption works when sharing ePHI. EPHI can still be compromised through situations like ransomware or human error and that’s a problem for compliance. To really protect ePHI with encryption, you to have tools in place that also protect the information once its on the device.

What That Means for Compliance

The **HIPAA Security Rule** expects safeguards to be in place protect ePHI from *any type of* information breach, including situations like the sharing of information with an unintended recipient. That’s where encryption doesn’t cut it because information gets breached after it’s already on the device. Truly protecting ePHI requires having safeguards in place to protect information from being sent, whether on purpose or accidentally, to the wrong person and having safeguards in place to wipe information from lost or stolen devices.

On top of all of this, encryption is not a substitution for compliance requirements like documentation. Take WhatsApp as an example.

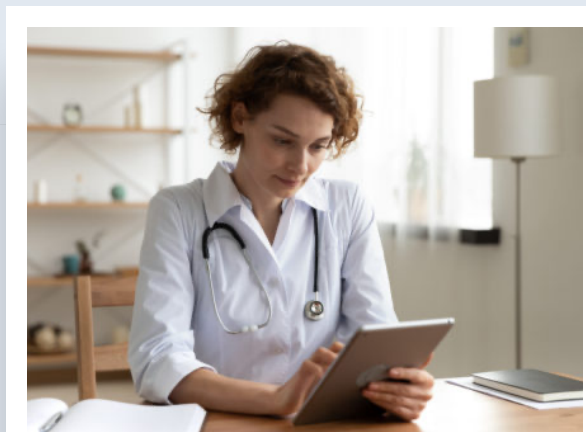
Let’s Talk Documentation

When WhatsApp rolled out end-to-end encryption a few years ago, there was some discussion about whether or not that made it HIPAA-compliant – and some healthcare providers were quick to use it to send ePHI. The conclusion was that WhatsApp **was not, in fact, HIPAA-compliant** because even though it offered end-to-end encryption, the tool didn’t include any measures to audit the conversations occurring and keep an archive of them for compliance purposes – and it also didn’t have measures to permanently delete ePHI off employees’ devices if they left the organization. This gets at the crux of the issue – end-to-end encryption without measures to document and to control ePHI on devices is simply not HIPAA-compliant.

The upshot? End-to-end encryption is an important aspect of protecting ePHI but on its own, it’s not enough. It needs to be used in conjunction with features that protect information once it reaches its destination and archives sensitive information.

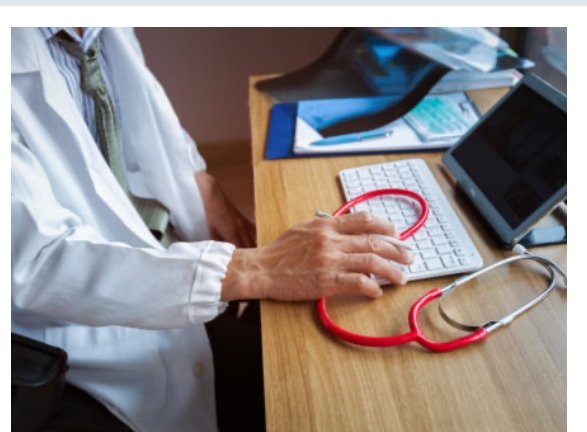
Vaporstream makes it simple for healthcare organizations to share ePHI without risk of information being forwarded or remaining on insecure devices – all while making sure it’s archived to a secure place for compliance purposes. See how healthcare organizations use us **here**.

Interested in More: Related Healthcare Stories




What You Should Know About Telehealth and Cybersecurity

+ Read more




Addressing the Telehealth Burnout Problem

+ Read more



Telehealth Has Exploded. What Now?

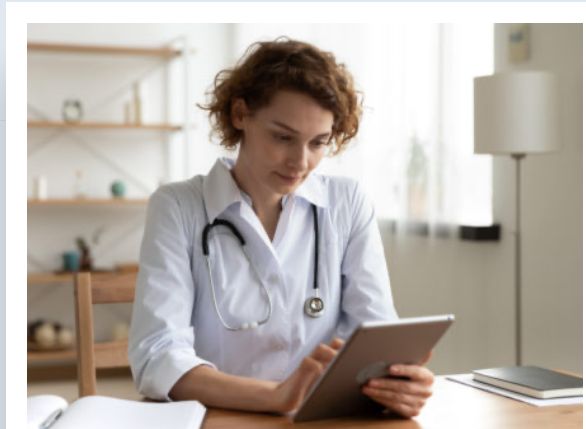
+ Read more



Why Pagers are Bad for Patient Outcomes

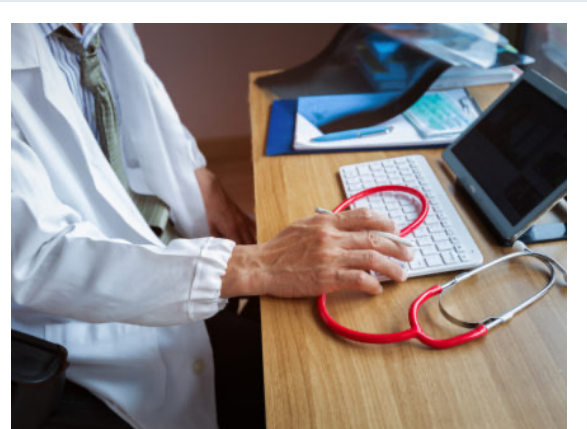
+ Read more

Latest Stories



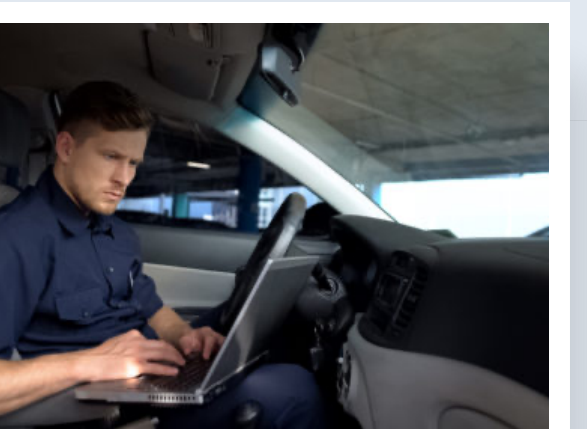
What You Should Know About Telehealth and Cybersecurity

+ Read more




Addressing the Telehealth Burnout Problem

+ Read more



How to Optimize Internal Police Communications

+ Read more



Telehealth Has Exploded. What Now?

+ Read more

Get Our Newsletter, Join The Community: