IPRO

WHITEPAPER

How to Manage Risks Related to Electronic Protected Health Information (ePHI)

What is ePHI and Why is it at Risk?

The storage of electronic protected health information (ePHI) opens your healthcare/insurance organization up to substantial liability. Data breaches of healthcare data are on the rise, up 40% between 2012 and 2018. Unauthorized access and disclosure incidents are up substantially as well, 553% since 2012 **(HIPAA Journal).**

Most healthcare organizations continuously amass this personal information. Over time, the vast amount of data can become unwieldy and unmanageable. The result is sensitive patient data remaining vulnerable to breaches and/or being stored away unknowingly in some remote data store.

What Happens if an Organization Doesn't Protect ePHI?

What healthcare businesses need is continuous risk assessment/auditing to know what ePHI they have and where it resides. In fact, HIPAA mandates that organizations perform enterprise-wide risk analyses to "determine whether any vulnerabilities to the confidentiality, integrity, and availability of PHI exist". Organizations that fail to conduct these analyses run the risk of steep financial penalties.

Just in **2018**, there were also 365 data breaches in the U.S. among healthcare organizations. Anthem Inc., for example, paid a settlement of $16M due to a data breach, and UnityPoint Health was the victim of a hacking incident that exposed the PHI of 1,421,107 individuals.

Recent settlements include (hipaajournal.com):

2.7M **Oregon Health & Science University** $2.7 million settlement for the lack of an enterprise-wide risk analysis.

2.5M **Cardionet** $2.5 million settlement for an incomplete risk analysis and lack of risk management processes.

750K **Cancer Care Group** $750,000 settlement for the failure to conduct an enterprise-wide risk analysis.

850K **Lahey Hospital and Medical Center** $850,000 settlement for the failure to conduct an organization-wide risk assessment and other HIPAA violations.

ePHI Risk Mitigation

By taking centralized control of your ePHI storage, you will minimize your organization's overall risk exposure, thereby saving potentially millions in avoidable fines and lawsuits. You will also protect your business reputation in the eyes of your patients. Big, costly data breaches are made public in the news. You don't need that negative publicity. It could force future patients to seek treatment or insurance coverage elsewhere.

How Technology Can Help

Information auditing software can illuminate the unknown inside unstructured data (within documents, emails, chat messages, mobile devices, electronic calendars, etc.) to uncover compliance and personal data vulnerabilities.

It enables internal auditors to view all unstructured data and have a direct look into its content wherever it is located, whether it's in file systems, email archives, SharePoint, SharePoint O365, Box.com, Citrix ShareFile, and so on. This enterprise software also enables admins to take control of any malicious data contained within employee emails to thwart dangerous phishing and malware attacks which could expose stored PHI.

Administrators can set up automated audits according to their organization's policies. The solution will then proactively audit newly created and stored documents even between audits with the automatic detection of all non-compliant data. In other words, if two employees are discussing a patient, for example, and accidentally include PHI in their electronic communications, the solution will detect this vulnerability and quarantine the stored communication so it can be reviewed and ultimately deleted.

To help automate this process and keep managers notified of potential issues, alerts and email reports can be sent every morning or as soon as non-compliant information is saved. Compliance, privacy, or security teams can act by tagging, deleting or quarantining data directly from email reports. This way, potential vulnerabilities can be detected on time and remediated to ensure no unnecessary PHI is stored where it shouldn't or for too long.