Lookout

Whitepaper

Lookout for Healthcare organizations

Embracing mobility while staying compliant

Healthcare Industry and Mobile Security

It's no secret that the healthcare industry holds some of the most important and personal data. The Ponemon Institute put it best in their Annual Benchmark Study on Privacy & Security of Healthcare Data, "Cyber criminals recognize two critical facts of the healthcare industry: 1) healthcare organizations manage a treasure trove of financially lucrative personal information and 2) healthcare organizations do not have the resources, processes, and technologies to prevent and detect attacks and adequately protect patient data."

The growth of data in the healthcare industry doesn't stop or slow down to make time for security resources to catch up. Between 2008 and 2014, the use of digital records in US hospitals skyrocketed from 9.4% to 75.5% .

Breaches can be critical hits for healthcare companies. Upon breaches, healthcare organizations not only lose billions of dollars in revenue and credibility, but they also suffer from long-term penalties. When a breach occurs, healthcare organizations face fines, audits from the government, and are forced to implement multi-million dollar corrective programs. Even worse, the company could be completely shut down.

What's the Motivation?

Cyber criminals are aware of the amount of valuable data collected by Healthcare organizations, making it one of the most targeted industries. The use of "ransomware" in particular has targeted hospitals, crippling computer systems until ransoms are paid. According to a recent report from the Justice Department, ransomware has quadrupled in 2016 from the prior year, averaging 4,000 per day.

Healthcare is a very broad category encompassing multiple segments that each has unique data that, if stolen, can be crucial to the survival of a company:

HEALTHCARE SEGMENT	DATA
Healthcare Providers (Hospitals)	Patient data EHR Insurance information
Healthcare Payers (Insurance)	Financial information Insurance information Identifications
Pharmaceuticals	DEA numbers Intellectual property e-Prescribing data
Biotech / Lab / Medical Devices	Intellectual property

What data is at risk on mobile?

Let's examine a couple healthcare segments that must take compliance considerations into account when bringing mobile devices into the organization.

HEALTHCARE PROVIDERS (HOSPITALS)

At risk: Healthcare providers' most important data is patient data. Electronic Health Records (EHR) have skyrocketed over the past few years. This data is accessible by many people within a healthcare provider organization. Physicians are one of the main people that are able to access this information.

Use case on mobile: Healthcare providers are increasingly using mobile as a work tool, but also offering mobile apps to patients as a means of convenience. Apps such as Epic Haiku allow users—physicians—to see their appointment schedule, look up patient charts, and easily access all this information via mobile. Other use cases for mobile devices specific to healthcare providers include the apps that healthcare providers make available to their patients. Since the use of Electronic Health Records (EHR) has increased, healthcare providers have developed apps to make this information readily available for patients to schedule exams, check on prescriptions, and access important information regarding their health.

HEALTHCARE PAYERS (INSURANCE)

At risk: To payers, high value data flowing through mobile devices includes financial data, such as credit card information, as well as health information regarding their members. Mobile devices are also used to access government records for those healthcare payer companies that are government contractors. Other important data for this segment includes intellectual property for the software they create.

The consequence of this data being stolen is enabling hackers to commit holistic fraud. Healthcare payers come across many types of data within their organization—from health records to credit card information to even location information such as addresses—and when cyber criminals get their hands onto these types of data, they can easily commit identity theft or even insurance fraud. More than that, if government employee records were compromised, a lot could be at stake for agencies who are offering their employees healthcare through a payer.

Use case on mobile: No doubt there's been a growth of BYOD for payers. Many companies allow BYOD into their organization to increase productivity, but they are also aware of the risks. Many organizations will opt for a containerization solution to protect these devices, but that's not enough to protect against all the sophisticated malware that we see today. Aside from just applications, email is also a big part of mobile usage in the healthcare industry.

A QUICK RECAP OF HIPAA-HITECH

What is HIPAA?

HIPAA is the Health Insurance Portability and Accountability Act. Introduced in 1996, the intention of HIPAA is to improve portability of health insurance coverage, reduce healthcare fraud and abuse and to protect individual privacy of personal health records.

What is the HITECH Act?

Health Information Technology for Economic and Clinical Health Act. Introduced in 2009 as part of the Affordable Care Act, HITECH takes HIPAA controls and adds on additional obligations. When people refer to "HIPAA" now, they generally mean both HIPAA and HITECH.

Who does HIPAA-HITECH apply to?

Covered entities such as healthcare providers (such as hospitals, health clinics), healthcare insurers and pharmacies, as well as the business associates of those covered entities.

How does Lookout help HIPAA-HITECH compliance?

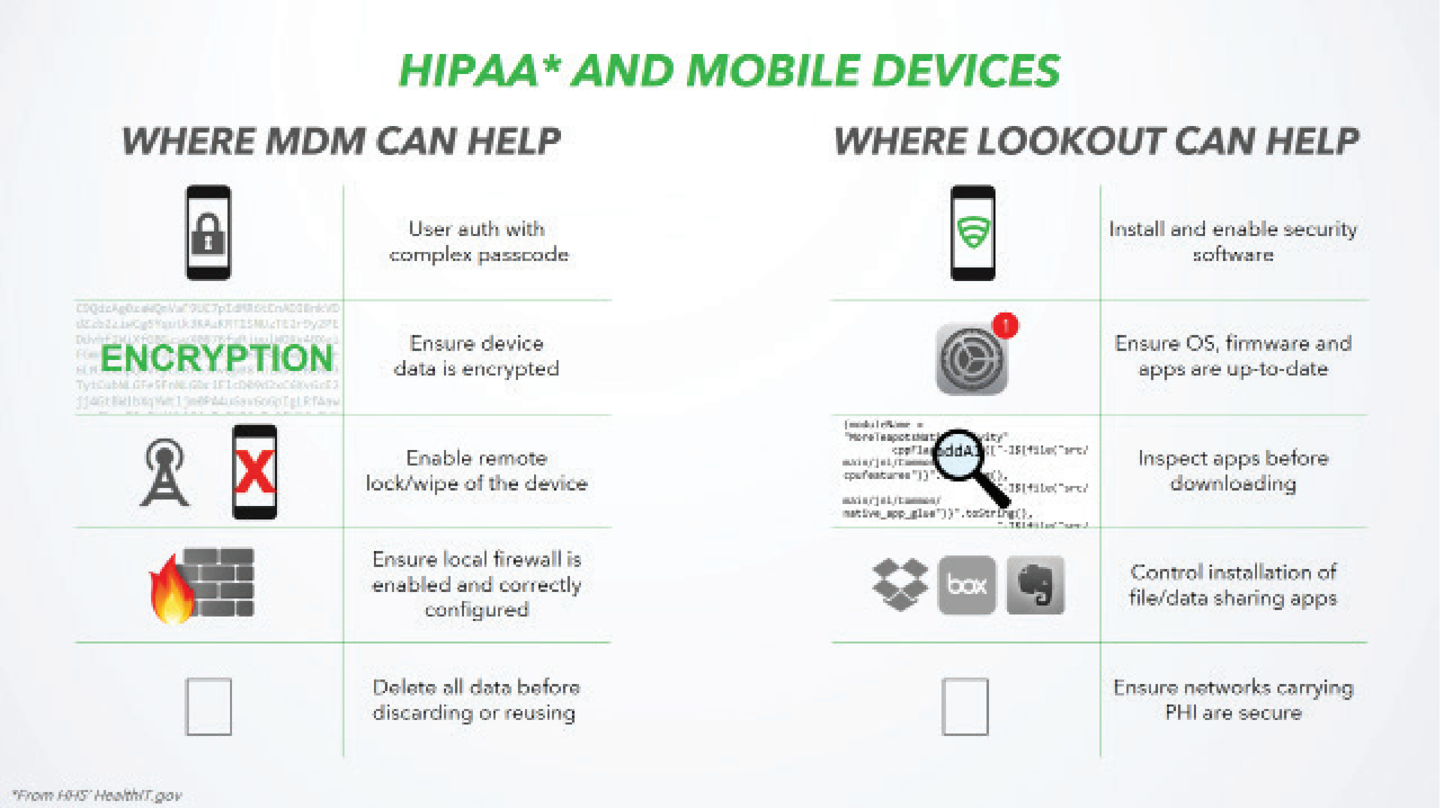
Lookout can help protect inappropriate access to patient data. HIPAA's security and privacy components are focused on protecting personal/protected health information (PHI). A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. Reasonable efforts must be made to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request. A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary.

HIPAA-HITECH COMPLIANCE APPLIES TO ANY MOBILE DEVICE THAT ACCESSES PHI

- Patient contact info such as name, phone number, address, email address
- Medical information, medical record number, date of birth, SSN
- Billing information
- Insurance information
- Text or emails from or to patients
- Text or emails to or from providers and other professionals regarding patients

HIPAA-HITECH for Mobile Devices

The Department of Health and Human Services' outlines the below guidance for mobile device privacy and security. We believe a combination of Mobile Device Management and Lookout's Mobile Endpoint Security products or similar is needed by covered entities to comply with HIPAA's recommended guidelines for mobile devices.



HIPAA* AND MOBILE DEVICES

WHERE MDM CAN HELP		WHERE LOOKOUT CAN HELP	
	User auth with complex passcode		Install and enable security software
ENCRYPTION	Ensure device data is encrypted		Ensure OS, firmware and apps are up-to-date
	Enable remote lock/wipe of the device		Inspect apps before downloading
	Ensure local firewall is enabled and correctly configured		Control installation of file/data sharing apps
☐	Delete all data before discarding or reusing	☐	Ensure networks carrying PHI are secure

*From HHS' HealthIT.gov

Source: https://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device

MDM HELPS WITH CONFIGURATION CONTROLS:

- User authentication with complex passcodes
- Ensure device data is encrypted
- Enable remote lock/wipe of the device
- Ensure local firewall is enabled and correctly configured
- Delete all data before discarding or reusing

LOOKOUT HELPS WITH ADVANCED SECURITY CONTROLS:

- Install and enable security software. HIPAA wants to ensure software is installed to protect against malicious applications, viruses, spyware and malware-based attacks. Lookout provides security to protect across the network, OS and app threat vectors
- Ensure OS, firmware and apps are up-to-date. Lookout provides consolidated. reporting on devices OS, firmware and app versions, as well as potential vulnerabilities affecting specific OS versions for managed and unmanaged devices, providing the necessary visibility to ensure that the devices connecting to your network and transmitting PHI are safe to do so.
- Inspect apps before downloading. HIPAA recommends researching apps before they are downloaded to ensure they will perform only functions you approve of. Lookout's big data security solution removes the manual burden by automatically detecting and notifying the administrator and end user when a mobile app is non-compliant or contains malware.
- Control installation of file/data sharing apps. With >50k new apps hitting the App Stores every day it is impossible to block file/data sharing apps using manually maintained black lists. Lookout can identify file/data sharing apps in an automated, policy-driven manner, then integrate with MDM to block the usage of those apps.
- Ensure networks carrying PHI are secure. Lookout detects man-in-the-middle and other network based attacks that may allow bad actors to intercept and decrypt your network traffic. Lookout also detects apps that do not employ the appropriate levels of encryption to protect data in transit.

Embracing mobility while staying compliant

Progressive Healthcare organizations are embracing smartphones and tablets in the workplace to enable more productivity from employees. As more sensitive data flows through these endpoints, Healthcare organizations are looking to solutions that provide visibility into emerging risks on this platform to comply regulatory and organizational security policies.

To learn how Lookout can help your organization stay compliant while enabling mobility within your organization, contact us at info@lookout.com