securityMETRICS®

White paper

5 TIPS FOR HIPAA COMPLIANT MOBILE DEVICES

PROTECTING PHI ON PORTABLE DEVICES

5 TIPS FOR HIPAA COMPLIANT MOBILE DEVICES

PROTECTING PHI ON PORTABLE DEVICES

INTRODUCTION

To many organizations, the rise of mobile devices means simplicity and efficiency in the workplace.

But mobile devices (e.g., smartphones, tablets, and laptops) present serious vulnerabilities in data security plans. If mobile devices aren't properly secured, patient data could be stolen. Unfortunately, most healthcare providers using mobile devices don't place appropriate privacy and security protections to secure patient data.

In this white paper, we discuss how the healthcare industry can embrace the future of mobile devices and remain secure.

DANGERS OF MOBILE DEVICES

THE RISKS OF USING A MOBILE DEVICE

Mobile devices in general aren't as secure as computers. The same security measures organizations use for workstations and servers usually aren't in place for mobile devices. Because of this, mobile devices may not be protected with technology like firewalls, encryption, or antivirus software.

In addition to loss and theft, there are many other ways a mobile device could be harmful to protected health information (PHI). Other risks include lack of authentication, mobile malware, unsecured Wi-Fi networks, outdated operating systems, and accidentally disclosing data by sharing the mobile device with friends, family, or coworkers.

No matter the type of technology a healthcare provider uses, they are obligated to protect PHI. If a smartphone or tablet is used to access, transmit, receive, or store information, it must have certain security precautions in place. Some other examples of why mobile devices can be dangerous:

- Mobile devices are easy to lose and steal.
- Passwords are seldomly used to protect access to the smartphone or tablet.
- Doctors typically don't encrypt the emails they send or receive on mobile devices.
- Insufficient BYOD (Bring Your Own Device) procedures.

BYOD PROCEDURES

When a healthcare provider uses their own personal smartphone or tablet to access patient data, these devices don't have adequate security regulations in place and are vulnerable due to other apps on the device. With each downloaded app, the risk grows.

What about others who have access to that mobile device when the doctor isn't in the office? Sometimes physicians, dentists, office managers, etc., let their kids play with their personal/work smartphone. What if their kids access patient data? Technically, this would be a HIPAA violation.

What if the kid or owner of the smartphone accidentally downloads a malicious app that can read the keyboard patterns of the user? The next time the doctor accesses his patient data, that malware can steal the password to the EHR.

Because of all these issues that come along with the convenient BYOD strategy, there are a few precautions you should follow to comply with HIPAA and ensure patient data security.

5 TIPS TO SECURE MOBILE DEVICES

The best mobile security advice is: don't implement a BYOD strategy. But in today's world, that can be impractical.

Protecting and securing health information while using a mobile device is a healthcare provider's responsibility. To address these concerns, use the National Institute of Standards and Technology (NIST) mobile guidelines for healthcare security engineers and providers.

Here's a summary of the most important takeaways from those mobile suggestions:

- Mobile devices should be individually authorized to add, modify, remove, and access PHI
- Passcode protection should be enabled
- Encrypt mobile devices
- Mobile devices should only access a specific Wi-Fi (WPA2) created for mobile devices
- Each mobile device needs to be registered with the organization
- Enable certificates to help prove the authenticity of users and devices
- Enable security policies for mobile security
- Use role-based access

1. FOLLOW BASIC MOBILE SECURITY PRACTICES

There are some obvious things you should and shouldn't do with your patient data while using your mobile device. For example:

- Accept all OS and app updates immediately. Just like computers, mobile devices must be patched often to eliminate software or hardware vulnerabilities found after initial release.
- Never connect to unsecured Wi-Fi.
- Use discretion when downloading apps. Even if apps look legitimate, they may be infected with malware that could compromise patient data, and cause a serious data breach.
- Don't jailbreak your device. Jailbreaking your device removes a lot of its built-in security. While this may let you do more with your device, it also leaves it more vulnerable to attacks.
- Make sure the devices you plug your mobile device into (e.g., your home computer, work laptop, etc.) are secure. If your computer/network isn't secure, it could act as a portal for hackers to gain access to your mobile device.
- Implement a password/pin on your mobile device. It's not foolproof, but it's another layer of security.
- Connect to your EHR via secured remote access, either a virtual private network (VPN) or through two-factor authentication.
- Encrypt your data. If you have sensitive data on your mobile device, make sure it's encrypted. Patient data will then remain secure, even if malware steals it.
- Use mobile vulnerability scanning. You can't prevent what you don't know about. A vulnerability scanner like SecurityMetrics Mobile for your mobile device can help discover weaknesses.

- Establish mobile device policies. Whether your company owns the devices, or your employees use their own, you need to have security policies set up that address the use of mobile devices.
- Train employees on mobile device policies. Your employees should know about malware and take the right measures to avoid it. Make sure to include mobile device security in your training.

Hackers are constantly finding new ways to steal information from mobile devices. When it comes to data security, you need to treat mobile devices the same way you treat servers and other computers.

Even though mobile devices can be hard to fit into a traditional network or data security model, they need to be considered. It's critical to include them in your information security planning.

IF YOU AREN'T SECURING YOUR MOBILE DEVICES, YOUR COMPANY'S SENSITIVE DATA COULD BE **AT RISK.**

2. IMPLEMENT MOBILE ENCRYPTION

HIPAA requires healthcare entities to “implement a method to encrypt and decrypt electronic protected health information” in Requirement §164.312(a)(2)(iv). All electronic PHI that is stored or transmitted in systems and work devices must be encrypted (e.g., mobile phone, laptop, desktop, flash drive, hard drive, etc.).

Most mobile encryption services are not as secure and reliable as other devices because most mobile devices themselves aren’t equipped with the most secure encryption. Mobile technology is only as secure as a device’s passcode. For example, Apple’s Data Protection API only encrypts the built-in mail application on iPhones and iPads, and only after you enable a passcode. Encryption does not apply to calendars, contacts, texts, or anything synchronized with iCloud. Some third party applications that use Apple’s Data Protection API are also encrypted, but this is rare.

If someone were to jailbreak your mobile device, information protected by the Data Protection API would remain encrypted only if the thief didn’t know the decryption key. Android’s encryption program works similarly, requiring a password to decrypt a mobile device each time it’s unlocked.

Additionally, if you backup your mobile device on your hard drive, ensure the backups are encrypted.

Although HIPAA regulations don’t specify the required encryption, industry best practice would be to use AES-128 or AES-256 encryption (or better).

If you can, avoid storing sensitive information on mobile devices to limit the threat of a data breach altogether.

MOBILE DEVICES REQUIRE THE SAME RESTRICTIONS AND ENCRYPTION PROCESSES AS OTHER WORK DEVICES LIKE DESKTOP OR LAPTOP COMPUTERS.

3. ENABLE LENGTHIER PASSCODES

While it's true that enabling a four-digit passcode will prevent patients waiting in exam rooms from getting into an unobserved office tablet, they do little to keep a hacker from accessing PHI. A four-digit password can easily be cracked with the right tools. Choosing a longer password (e.g., a 10-character password with a special character and alphanumerics) and enabling the setting that wipes your device of data after 10 failed passcode attempts will help avoid this problem.

In a best practice scenario, mobile device passcodes should be 8 characters or more, contain alphanumeric and special characters, and not contain dictionary words (such as nurse1 or ilovefootball). Both Android and iOS devices have the option to bypass the typical four-digit pin and choose to implement these complex alphanumeric passcodes via a simple device setting change.

4. SOFTWARE AND APPLICATION UPDATES

Older operating system and app versions tend to have errors and older encryption implementations, and they are not considered 'best practice' by the HHS. Just like computers, mobile devices must be patched often to eliminate any software or hardware vulnerabilities found after initial release.

It's important to note that updates must occur to each app installed on the device. If just one insignificant app that doesn't even touch ePHI is vulnerable, cybercriminals might be able to exploit a vulnerability of that app and gain access to all the data on your device.

Luckily for healthcare employees, updating mobile device OS and software is often simple and doesn't take much time.

Configuring a mobile device to be dedicated for healthcare office use only is a great option to secure a smartphone or tablet. That means the ability to install apps, connect to the Internet, access device settings, and make or receive calls is disabled. When the device is on, it's dedicated to a single app used to access patient data in any matter that is in-line with your security policies and strategy.

5. FREQUENT EMPLOYEE TRAINING

Ensure your organization isn't one that creates policies only to forget them. Regular policy training and enforcement is an important part of HIPAA mobile security and helps your employees remember organizational guidelines.

A lot of the risk depends on how your mobile environment is set up and how your employees can access sensitive data. Unless you have policies in place regarding mobile devices, your employees are likely accessing sensitive information in an insecure manner.

AVOID SUSPICIOUS EMAILS

More employees are using their phones to look at and answer corporate email, which is a way that hackers can install malware on your phone.

Here's an example: your employee receives an email that says you've won something (e.g., a tablet, a vacation). They open the email and click on the link, and nothing happens, or you've been taken to a dummy site. But malware was downloaded and installed on your phone. The data on their phone may now be exposed to that hacker.

Just like on employees' computers, make sure they avoid opening suspicious emails on their phone.

BE CAUTIOUS ABOUT INTERNET USAGE

If your employees access insecure websites, they run the risk of exposing sensitive data transmitted from their device. They're also more susceptible to man-in-the-middle attacks and being exposed to malware. Train employees to avoid using insecure websites and Wi-Fi networks, and consider using antivirus protection and a VPN on their phone to secure Wi-Fi communication.

The browser itself on their phone could also be a source of vulnerabilities. This can lead to web browser attacks. Attacks like these are more common on android devices. Make sure your employees have the most current version of whatever browser they use.

TEXT MESSAGE/VOICEMAIL PHISHING

Employees may get a text message or a voicemail from what appears to be a legitimate source asking for personal information either about them or their device.

Hackers often use this information to steal whatever data they can, including social security numbers, credit card data, etc. They may even be able to use it to make a targeted attack to install malware on your phone.

Train employees that whenever they get a text like this, call the company on their legitimate phone and verify with them. Never give out sensitive information through a text.

CONCLUSION

Remember that many healthcare organizations lose data by not protecting and training their employees on how to protect their mobile devices. Take steps now to secure your mobile devices.

ABOUT SECURITYMETRICS

We help customers close security and compliance gaps to avoid data breaches. Our forensic, penetration testing, and audit teams identify best security practices and simplify compliance mandates (PCI DSS, HIPAA, HITRUST, GDPR). As an Approved Scanning Vendor, Qualified Security Assessor, Certified Forensic Investigator, we have tested over 1 million systems for security.

https://www.securitymetrics.com/hipaa-audit