HIPAA-Secure Smartphones

Four critical security controls for mobile healthcare workers

by Michael Herrick
Founder & Senior Risk Analyst at Matterform.com

One of the leading causes of HIPAA data breaches is loss or theft of an unprotected device. Don't let hackers use your smartphone to steal your company's protected health information. Learn how to make your smartphone more secure and more HIPAA compliant with four key security controls that you can implement right now.

The EPIC Security Controls

The EPIC Security Controls are four simple cybersecurity controls that should be enabled on any smartphone that can access sensitive systems. Each one is already built-in to your smartphone. All you have to do is make sure each control is turned on and configured correctly.

The EPIC Security Controls are:

- **E** Encryption of the entire device
- **P** PIN-protected screen lock
- **I** Inactivity Timer
- **C** Current OS

Let's dig into each one and see how it will make your smartphone more secure and more HIPAA-compliant.

E Encryption of the entire device

Encryption encodes all the information on your phone so that only you can access it.

Encryption is a deeper level of protection than just a PIN or passcode. An attacker who steals or finds your phone can easily bypass PINs and passcodes and hack directly into the device storage. If the device is not encrypted, the attacker can easily see anything stored or downloaded onto the device, including recent email messages and text messages. Encryption scrambles the storage so the attacker can't possibly see the data without your secret code.

Encryption used to be an optional setting on smartphones but, in recent years, it has become the default setting. You probably already have encryption fully enabled on your phone.

But there are two gotchas to look out for.

First, encryption is *only* active if you have some kind of screen lock set up on your device. If you can open your phone just by pressing a power button or swiping the screen, then your phone isn't locked, it isn't encrypted, and it isn't protected. In the next section, I'll show you why you should use a long, random PIN to lock your device and activate your encryption.

Second, if you are running an Android device, you might still have to turn encryption on manually. Many different companies manufacture Android devices and not all of them enable encryption automatically. Android users should open their phone's Settings app, then tap on Security to make sure encryption is turned on.

P *PIN-protected screen lock*

Remember, encryption only works when you have a secure screen lock configured. There are many kinds of screen locks, but they all depend on one lock method that is the most universal and also the most secure: a long, random PIN (Personal ID Number).

Even if you want to try other screen lock methods, like facial recognition or fingerprint scanners, you still have to start with the PIN, so you should focus first on creating a secure PIN.

Not all PINs are created equally. Unfortunately, most people use (and re-use) short, easy-to-guess PINs, like 1234. No joke. According to research, about 10% of accounts and phones are protected by nothing more than 1234.

In order to be secure, a PIN must be:

- **Long**
  A four-digit PIN is not good enough (and many phones no longer allow such a short PIN). You should use at least 6 digits, and for healthcare workers, I recommend an 8-digit minimum.

- **Random**
  That means you can't use 123456. You can't use 000000. For that matter, you shouldn't use birth dates, patterns up and down the keypad, and other easy mnemonics. Ideally, your PIN should be a totally random number and not a pattern that you invent yourself.

If you are interested in other screen lock methods, like facial recognition or fingerprint scanners, look for my in-depth eBook, *The BYOD Blueprint*.

I *Inactivity Timer*

Locks only work when you lock them.

If you leave your phone unattended and unlocked, anyone who picks it up will be able to access your email and text messages and they may even be able to log into your company systems, secure websites, and more.

So make sure your phone locks itself when you're not using it.

Most phones have an inactivity timer (*a.k.a.,* "auto-lock" or "screen timeout") turned on by default. Probably all you have to do is leave that setting alone, but take a few minutes to check your Settings app to be sure.

There's no hard rule about how long your inactivity timer should be. Personally, I think 30 seconds is too short, and 5 minutes is too long. How about a minute? That's probably a good setting for most companies. But if you pick a different number, I won't criticize your choice.

Because any inactivity timer of any duration will be more secure than no inactivity timer at all.

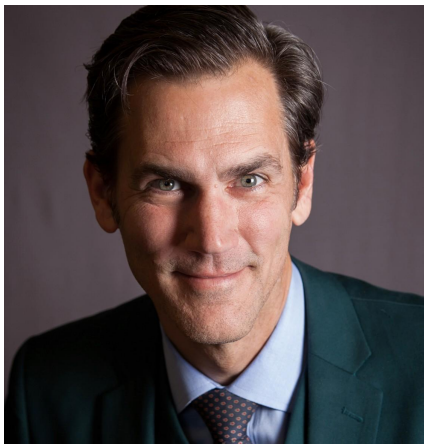
C *Current OS*

This last control is often overlooked. Don't make that mistake. In some ways, it's the most important one of all.

Make sure your phone is running an up-to-date version of its operating system and still receiving security updates from the manufacturer.

Generally, the best practice is to run the very latest version of iOS or Android and apply all updates and security patches as they become available. If your phone is too old to run the latest version of its operating system, it's time to buy a new phone. Smartphones generally have a security life of about 5 years. After that, they are no longer kept up-to-date and using an outdated phone can put your patient data at risk.

About the author



Michael Herrick is a healthtech serial entrepreneur with more than 25 years experience building technology companies. Michael is the founder and CEO of Matterform where he offers HIPAA and cybersecurity expertise to healthtech startups, hospitals, and healthcare practices. Michael is also the co-founding Chief Technology Officer of Medicheck, a Mexico startup bringing electronic health records to Latin America. Michael's cybersecurity consulting is driven by his unique perspective combining technology and policy with an unwavering focus on human-centered design. Michael and his family live in downtown Albuquerque, New Mexico.

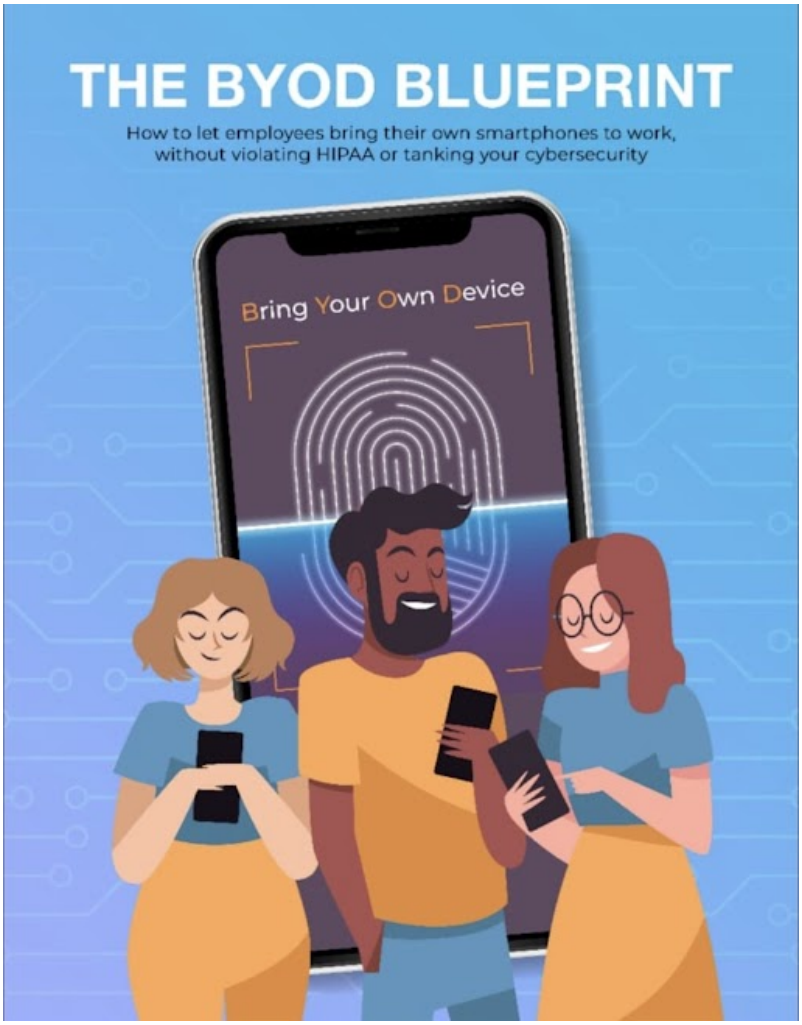
Follow Michael for regular cybersecurity updates at:

https://www.linkedin.com/in/michael-herrick-ceo/

Get my eBook to learn more

I'm so glad you found this short whitepaper and I hope you'll follow the simple steps I've shared to make your smartphone more secure and more HIPAA compliant. If you would like to create a BYOD security policy to help improve cybersecurity at your company, I hope you'll check out my in-depth ebook, The BYOD Blueprint.

Get the book now at : https://bit.ly/3uNtiG3



Getting a handle on employee smartphones is one of the easiest and most cost-effective ways to improve cybersecurity at your company.

You already have all the technology you need to secure smartphones at your company. All you need is some guidance about what really works.

In our BYOD Blueprint, I'll show you **simple steps** you can take right now to reduce cybersecurity threats from employee smartphones.

I'll also **steer you away** from the overly complicated stuff that looks fancy but doesn't actually improve your security.

I'll show you how to **get your employees on board.** Because security is a team sport and you have to get everyone's buy-in.

PLUS I'll show you how to draft a simple **BYOD Security Policy** to document your cybersecurity controls, support your compliance obligations, and hold team members accountable.

Contents of *The BYOD Blueprint*

More info at https://bit.ly/3uNtiG3