Health Information Compliance Alert

HIPAA Compliance: How To Protect Against The Dangers Of BYOD

What HIPAA requirements apply to clinicians' own devices?

The rapidly growing phenomenon of BYOD "bring your own device" is both a potential boon and a very real danger for the healthcare industry. And if your clinicians are subscribing to the BYOD trend, your organization could be at serious risk for leaking unsecured electronic protected health information (ePHI), leading to a costly HIPAA breach.

"Mobile health applications and devices can ensure a smoother workflow and increased productivity, but only if healthcare organizations tackle the challenge of ePHI security with the right mindset keeping sensitive data off of the device, and enlisting a HIPAA-compliant hosting provider to reduce the risk of a costly data breach," **April Sage,** director of healthcare vertical at **Online Tech**, said in a recent **Porter Research** blog posting.

Delve Into BYOD Questions & Risks

When it comes to BYOD, you have some grave questions of ownership, control and liability, says HIPAA expert **Jim Sheldon-Dean,** director of compliance services for **Lewis Creek Systems** in Charlotte, Vt. "How can you manage these devices in such a way that if something goes wrong, you can make sure things don't happen to cause a breach?"

According to Sheldon-Dean, you must look at three security and privacy aspects of mobile devices:

1. **Authentication** Who is accessing or providing ePHI?
2. **Authorization** What is the right information to provide to whom via a mobile device?
3. **Access** What access controls should you have in place to protect privacy? How secure for the entity is the interaction point? Is the ePHI secure in transmission and/or on the device?

Follow 5 Steps for a Mobile Device Management Plan

Among the very best ways to prevent BYOD from causing HIPAA breaches is to execute a mobile device management plan. HealthIT.gov offers the following five steps to develop such a plan for your facility:

1. **Decide** First and foremost, you need to decide whether you'll allow staff to use their own mobile devices to access, receive, transmit, or store patients' health information, or whether you'll allow staff to use their mobile devices as part of your organization's internal networks or systems, like your electronic health record (EHR) system.
2. **Assess** Conduct a risk analysis (see HICA Vol. 13, No. 1, Pages 1–3) to evaluate the potential risks of BYOD to your organization. Serious risks can include a lost or stolen mobile device, inadvertently downloading viruses or other malware, using an unsecured Wi-Fi network, and unintentional disclosure to unauthorized users when sharing mobile devices with family, friends and co-workers.
3. **Identify** Identify your organization's mobile device risk management strategy, including privacy and security safeguards. You should develop and implement safeguards to reduce the threats and vulnerabilities you identified in your risk analysis.
4. **Develop, Document & Implement** Formalize your policies and procedures regarding safeguarding ePHI when using mobile devices. Include your mobile device management plan, BYOD policies, restrictions on mobile device use, security/configuration settings for mobile devices, information storage on mobile devices,

procedures for mobile device misuse, recovery/deactivation of mobile devices, and staff training.

5. **Train** — All staff should undergo HIPAA privacy and security training specific to mobile devices. In the training, cover topics like the risks posed by using mobile devices at work, how to secure mobile devices, how to protect and secure ePHI, and how to avoid mistakes when using mobile devices.

Prevent BYOD From Turning Into A Breach Disaster

Although training your staff on the potential dangers of using their mobile devices at work is absolutely essential to preventing breaches, you need to take your HIPAA protection a step farther to really secure those devices.

Best bet: "One mobile security best practice is to never store ePHI on the mobile device itself," Sage said. "Instead, keep data in HIPAA-compliant data centers and services, and use a secure virtual private network (VPN) to access the data remotely with devices." And if you're outsourcing your IT infrastructure, make sure you "partner with a HIPAA-compliant hosting supplier that can provide evidence of its compliance," she adds.

But how can you know whether your BA provides HIPAA-compliant hosting? "HIPAA-compliant hosting means the data-hosting supplier has undergone an independent HIPAA audit by a third party to determine that their hosting solutions and facilities have the appropriate technical, physical and administrative security controls in place to keep ePHI secure, even when being accessed remotely with a mobile application and/or device," Sage explained.

Bottom line: Whatever you decide to do to keep your staff members' BYOD predilections HIPAA-friendly, don't assume that your staff will safeguard their devices properly on their own. You must take some control of personal mobile devices when your staff is using them to transmit, store, or view your patients' ePHI.