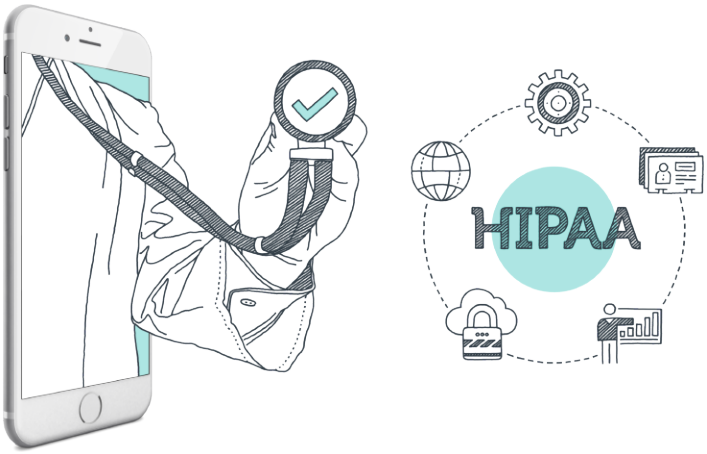

Mobile health & HIPAA: Playing it safe in 2017

For the 72% of U.S. adults who own a smartphone, gaining access to health information has never been easier, with more than 250,000 mobile health (mHealth) apps now available on major app stores.

Consequently, the number of U.S. consumers who use mobile applications for managing their health has doubled in recent years, increasing from 16% in 2014 to 33% in 2016 . By the end of 2017, this number is expected to reach 50%. What's more, of the smartphone owners who use health apps, 40% have discussed or shared mobile app data with their doctor, and around a third of consumers prefer virtual appointments to face-to-face appointments, due to the lower costs, convenience, and timely access to care.

On the other side of the practice door, a growing number of health providers are using mobile devices to improve operational efficiencies and patient health outcomes. However, while 82% of healthcare organizations claim to have a fully implemented mobile strategy, almost all claim to have concerns over the security of mobile applications, with end-to-end HIPAA compliance as their greatest security concern.

Health providers have every right to be concerned - according to an annual study into the privacy & security of healthcare data, nearly 90% of healthcare organizations have fallen victim to a data breach in the past two years, at an average cost of a $2.2 million per breach. The U.S. Department of Health and Human Services (HHS) reported more than 260 major healthcare breaches in 2015, and close to 10% of those breaches involved a mobile device. These numbers considered, it is critical that healthcare organizations take action to identify the risks associated with mobile usage within their own organization, and take necessary steps to mitigate those risks.

Obligations under HIPAA

The Health Insurance Portability and Accountability Act, more commonly known as HIPAA, was enacted in 1996 in order to protect individuals' medical records and other personal health information. Today, some 20 years since HIPAA came into force, covered entities and their business associates face the very real challenge of keeping protected health information (PHI) private, and out of the hands of those who wish to exploit it.

For healthcare organizations, maintaining the confidentiality and privacy of patient information should be the number one priority, as a failure to do so can result in civil penalties up to $1.5 million, criminal penalties, and considerable reputational damage.

Managing mobile in the modern healthcare setting

The increased adoption of mobile in the healthcare setting improves and speeds up care collaboration, and should be embraced, not feared. But the fact remains that mobile devices introduce significant potential for harm, if not managed responsibly. The following steps are intended to help organizations appropriately manage the use of mobile devices in the healthcare setting.

Assess the risk

Every organization needs to carefully consider how the use of mobile devices affects the risks to protected health information (PHI). A mobile risk assessment will help to determine the steps that need to be taken to adequately protect the organization from potential threats. An assessment should analyze and document the levels of risk presented by all mobile devices used within the organization's network, and include the following information:

- A log of all mobile devices that are being used, or have been used in the past, to access the organization's internal systems (such as EHR and CRM systems), regardless of how often or to what extent, and;

- Details of the type of information being accessed, received, stored and transmitted via mobile devices

Conducting a security risk assessment is a key requirement of the HIPAA Security Rule. Organizations seeking further guidance on the risk analysis requirements under HIPAA should consult the HHS.gov website.

Invest in the right tools

Organizations that use mobile devices to access, store, send and receive PHI must ensure they use secure tools and applications when doing so. To ensure PHI is protected throughout its entire lifecycle, organizations should invest in HIPAA-secure solutions that allow them to carry out all operational tasks within a secure environment.

Email, text messaging and faxing are all common yet inherently insecure methods of communication, due to vulnerabilities to hacking, user error, and an inability to verify receipt of information. Purpose-built, HIPAA-secure applications, on the other hand, minimize risks by encrypting data, allowing the user to set role-based permissions, and providing complete activity audit trails.

When it comes to storage, sensitive health information needs to be encrypted at rest, as well as in-transit. By creating role-based permissions, control over access of information can be monitored and recorded, to ensure information is only seen by those who are permitted to do so.

Before entering into a contract with any third-party vendor, it is essential that organizations first gain assurances from the vendor about their commitments to HIPAA compliance, and that no PHI is exchanged until a Business Associate Agreement (BAA) has been signed.

Secure all devices

Password protection is not always enough when it comes to protecting a mobile device. According to the 2016 Verizon Data Breach Investigations Report, user credentials were used in the majority of breaches that occurred in 2015, with some 63% of incidents being tied to weak, default, or stolen passwords. Organizations should implement the following security standards across all mobile devices that come into contact with PHI:

- Use strong passwords, PINs or other forms of user authentication, and ensure they are routinely updated
- Implement user authentication controls and use two-factor authentication (or multi-factor authentication) wherever possible
- Enable device encryption to reduce the risk of unauthorized parties accessing confidential data
- Install remote wiping and/or remote disabling
- Use reputable security applications and ensure operating systems are kept updated
- Install and enable a firewall

Create and maintain mobile policies

Maintaining a comprehensive mobile policy is essential for ensuring best security practices are followed. At the very least, healthcare organizations need to ensure they have policies in place which clearly define a list of dos and don'ts, outline appropriate security measures, and set out a plan of what to do in the event of a device being lost, stolen or compromised.

Additionally, rules should be developed to control application downloads on devices used for work purposes. This is particularly important in Bring Your Own Device (BYOD) environments, where users may be using the same devices for work and leisure. Most employees who download unauthorized tools and applications do not intend to cause harm, however in doing so they introduce potential security vulnerabilities into IT networks. It is the responsibility of employers to extinguish the use of non-secure applications in the workplace through clearly communicated policies.

Educate staff

All of the above counts for very little if staff are not regularly trained. Our recent survey into mobile messaging trends within healthcare organizations revealed that more than half (56%) of professionals believe their organization could be doing more to educate employees on HIPAA-compliance and the rules around sharing PHI.

As long as people make up part of the security equation, they remain one of the biggest vulnerabilities. When it comes to mobile usage in the healthcare setting, it is critical that organizations not only identify the risks and take actions to mitigate those risks, but also ensure all staff understand their responsibilities.