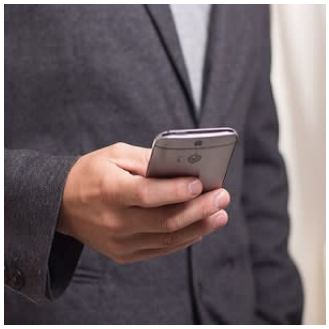
HealthManagement
Promoting Management and Leadership

To BYOD or not to BYOD: the benefits and risks



Like in other industries, use of mobile devices is prevalent in healthcare. A 2017 survey of healthcare workers conducted by HIMSS Analytics revealed that tablets and smartphones were used by the majority of respondents (80% and 42% respectively) to access information to provide and coordinate patient care. This is one reason why many organisations are leaning towards literally opening their doors to employee-owned devices.

Bring your own device (BYOD) programmes offer organisations considerable benefits, including increased productivity and reduced hardware costs. According to a recent study, companies with an effective BYOD policy in place can expect to save on average $350 per year, per employee. These advantages notwithstanding, BYOD also comes with significant risks.

Brad Spannbauer, senior director of product management and HIPAA privacy & compliance officer at j2 Cloud Services, says healthcare facilities should consider these potential pitfalls before adopting a BYOD programme:

Increased device vulnerability

In 2017 nearly 50% of large data breaches in healthcare were attributed to theft and loss, according to the Office of Civil Rights at the U.S. Department of Health and Human Services. To make matters even worse, 28% of doctors have reported storing patient data on their mobile devices.

Device loss and theft is an unfortunate inevitability; even the most cautious of employees misplace things from time to time. But when those misplaced things provide gateways to sensitive data and company networks, major issues can arise. By allowing employees to use the same devices both inside and outside of work, devices become more vulnerable.

Compliance complications

BYOD presents serious compliance challenges for healthcare organisations, particularly when it comes to meeting HIPAA's security and privacy rules. From making sure that all employees are implementing necessary physical safeguards, including strong passwords and multifactor authentication, to ensuring that PHI is only ever exchanged via HIPAA-secure tools that utilise encryption, there's much to consider for compliance officers and IT departments. Therefore, developing a robust BYOD policy is critical for HIPAA covered entities.

Legal difficulties

It's possible that from time to time, an employer may need to gain access to an employee's device to access data, or install or update applications. But what happens if during that period of access, the employer stumbles upon some incriminating information, accidentally deletes personal files, or finds out something about the employee that was intended to remain private? This raises lots of complex legal questions that employers must consider before rolling out BYOD, all of which should be addressed within a clear set of policies and procedures.

Shadow IT

"Shadow IT" refers to the use of any IT system within an organisation without the organisation's knowledge or consent; this could be anything from personal email accounts to workflow tools. While most employees who use unauthorised tools and apps do so without malicious intent, nevertheless they're introducing security vulnerabilities which are almost impossible to identify. This is a growing issue that is only amplified by BYOD; one report estimates that by 2020, a third of successful attacks experienced by enterprises will be on their shadow IT resources.

Employee productivity

As much as BYOD can help boost productivity, it can also have the opposite effect. Allowing employees to manage work on devices, which are also likely to contain personal apps – Facebook, Whatsapp, iMessage and so on – can introduce unwanted distractions. Even with the best will in the world, it's difficult to ignore notifications, work related or otherwise, and BYOD only makes that challenge harder for employees.

Source: Healthcare Business & Technology
Image Credit: Pixabay

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.

Published on : Tue, 23 Jan 2018

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.