Navigating BYOD and BYOA in healthcare without compromising security

HIMSS Analytics survey highlights IT security risks, opportunities

A surgeon accesses a cloud-based music streaming app on the hospital network so he can listen to music during a procedure. A specialist traveling between sites accesses patient data on her personal smartphone to respond to a colleague's time-sensitive question. Like it or not, BYOD (bring your own device) – and its corollary, bring your own app (BYOA) – are unavoidable facts of life for healthcare organizations. Unfortunately, these seemingly benign clinician choices can have a damaging impact on a provider's security posture.

In a recent survey of clinicians conducted by HIMSS Analytics on behalf of Citrix, 17 percent of survey respondents admitted to having used unauthorized technology to complete a work-related task. Not only do the violations by survey respondents include devices – such as cell phones and personal computers – but also, unauthorized applications, such as those for file sharing (Figure 1).

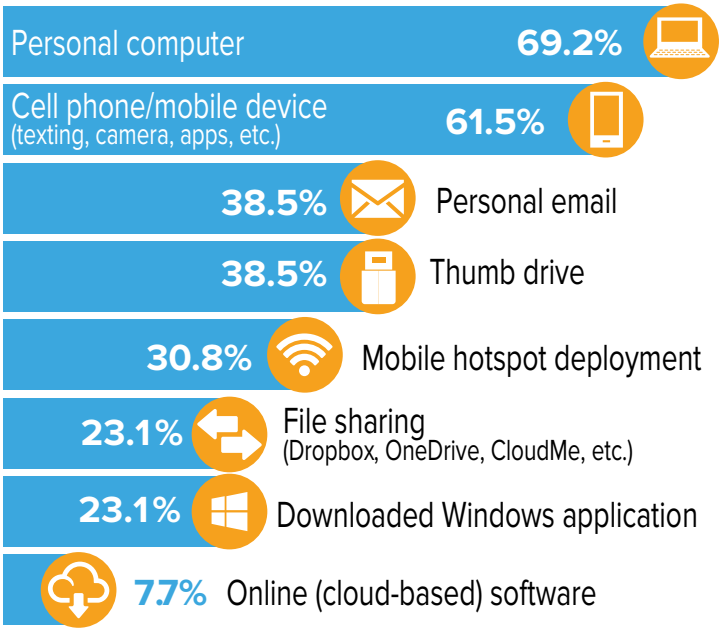
Produced in partnership with HIMSS Media

Produced in partnership with HIMSS Analytics

"Even a single instance of the use of unauthorized technology can weaken the security posture of your organization by providing a gateway for hackers and other bad actors."

Lee Kim | Director, Privacy and Security | HIMSS

Figure 1. Respondents noted that the most common unauthorized technology usage was personal computers or mobile devices.



The consequences of using unauthorized technology

The consequences of unauthorized technology use can include data breaches, HIPAA violations, patient identity theft, compromised patient safety, the introduction of malware or ransomware and more. The HIMSS Analytics survey data showed that 41 percent of respondents had experienced repercussions from the use of unauthorized technology. Of those organizations that experienced repercussions, 47 percent reported HIPAA violations (Figure 2).

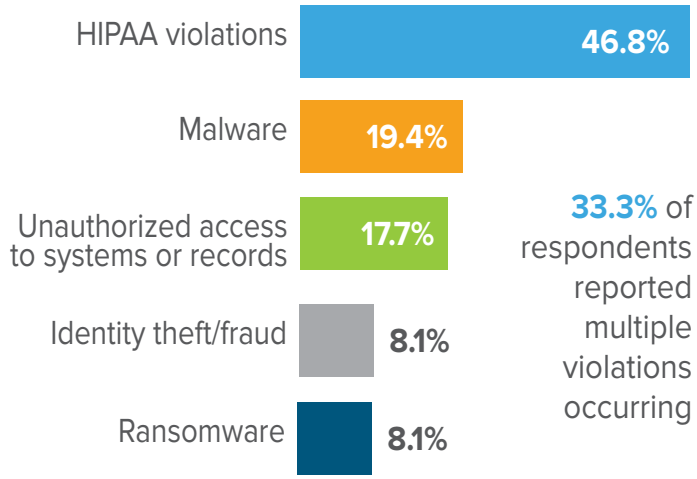
The percentage of people using unauthorized technology is likely underreported, both because employees don't want to admit to violating their organizations' acceptable use policies and because people don't always understand the gravity of the situation. "It's called 'negligent insider threat' – or as some researchers perhaps more accurately call it, 'unintentional insider threat" – and it's a big problem in healthcare," said Lee Kim, director of Privacy and Security for HIMSS.

As the HIMSS Analytics survey illustrates, negligent insider threat takes a variety of forms. People download apps they aren't supposed to add. They load web extensions and add-ons onto their web browsers. They download free software. They download and use software that's not authorized by their IT departments. They use unencrypted thumb drives to take files home and work on them, or upload files to a free file-sharing program online.

The problem with this behavior is that "even a single instance of the use of unauthorized technology can weaken the security posture of your organization by providing a gateway for hackers and other bad actors," according to Kim. Hackers look for "open doors" to the valuable data found in healthcare organizations' IT systems. "If a workforce member uploads a sensitive document to an online file sharing site, but does not 'lock down' access to that document, then your organization may be in danger of having a reportable breach or, at least, data leakage possibly to unauthorized third parties," she said.

The rampant use of unauthorized technology may nullify or weaken the proactive measures an organization's security department has in place. "If such technology is not properly secured, the data can leak out of it like a sieve," said Kim.

Figure 2. HIPAA violations are the most common repercussion from the use of unauthorized technology.



"The key is vetting the technology in real time so policy can determine if required measures are enabled for secure access."

Kurt Roemer | Chief Security Strategist | Citrix

Mitigating the risk of unauthorized technology use

Given the size of the problem and what is at stake, how should healthcare organizations deal with it? Some organizations have employed an outright ban on the use of unauthorized technology, but as the HIMSS Analytics survey shows, acceptable use policies don't always translate into changes in behavior.

"You have to find the right balance between locking things down versus giving folks access to the information they need to do their jobs," said Kim. "If you don't find the right balance, and the security is so restrictive that people cannot do their jobs effectively, people will circumvent the controls you do have in place."

Kurt Roemer, chief security strategist, Citrix, agrees, noting, "Organizations need to recognize that people will continue to use unauthorized technologies," in spite of the policies organizations put in place to limit that activity. "Employees, clinicians, non-employees, contractors, suppliers, partners and patients want to use their own technology to connect to the organization's" applications and services," he said.

Organizations might not be able to stop the use of unauthorized technologies, but they can manage the associated risks by putting the proper policies, procedures, training and technology tools in place. An important first step is educating clinicians about the many potential negative consequences of using unauthorized technology. Equally important is providing clinicians with technology solutions that allow them flexibility in the use of devices and applications, without compromising organizational security.

"It's not about requiring trusted enterprise devices at every step of the way anymore," said Roemer. "It's more about vetting the entire situation for trust – not only the device, but also the user, the user's location and the sensitivity of the data they are trying to access – combining all of those trust factors to make a dynamic decision about who gets access to what information in that specific situation."

A secure digital workspace offers providers exactly that level of vetting, so that access to information can be provisioned by IT in a risk-appropriate way. In other words, organizations may not be able to prevent clinicians and others from using unauthorized technology, but they can ensure the secure delivery of data and apps to any device on any network, whether that device has been authorized by the organization or not.

Roemer offered the example of a physician in transit who receives a secure message requiring follow up. He logs onto his brother-in-law's home computer and attempts to access the hospital's electronic health records system. He is denied access, receiving a message that says, "This computer will not sufficiently protect patient information. You can only access noncritical/nonconfidential information during this session. You must log in through a secure endpoint to access patient data." *(Note that physicians then can utilize their smartphones to access the requested information).*

"The key issue is not what technology is being used. The key issue is vetting the technology in real time so policy can determine if required measures are enabled for secure access. You may want to degrade access by suppressing access to sensitive data in situations in which a particular technology does not support all of the features and functions required to ensure the necessary level of security," said Roemer.

If the organization does provide a technology solution such as a digital workspace to help clinicians securely use outside technologies, speed and performance are critical. "Security cannot impede patient care. Security solutions need to enhance, not degrade, the clinician experience," he said. "Otherwise, clinicians will use workarounds – which defeats the purpose of having security tools available."

Can BYOD actually improve patient care?

Is it possible that there is a silver lining to the BYOD world we live in? Sixty-three percent of respondents in the HIMSS Analytics survey of clinicians believe that "the ability to use your own device improves care delivery" (Figure 3).

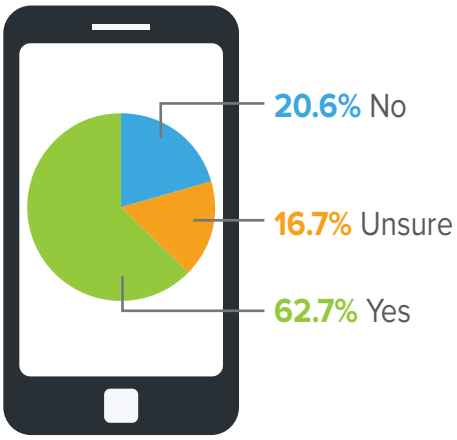
Ash Goel, MD, vice president and system chief medical information officer for Bronson Healthcare, believes there can be a place for BYOD – and its corollary, BYOA – in the world of patient care. Goel understands why clinicians might decide to use technology resources outside of an organization's IT-approved resources.

"Healthcare organizations are getting more sophisticated in terms of the policies, procedures, processes and tools we have available to manage that risk."

Ash Goel, MD | Vice President, System Chief Medical Information Officer | Bronson Healthcare

He offered a case in point – a specialty pediatric cardiothoracic surgeon who wants to access standards of care guidelines or risk calculators specific to that particular specialty. "As healthcare organizations, we provide very broad brush information resources. Because of resource constraints, it is not feasible for us, as a system, to support hundreds of applications for myriad specialties, even though access to those resources has the potential to improve care delivery," he said. "In those situations, access to external technology resources can support patient care."

Figure 3. Do you think the ability to use your own device improves care delivery?



Likewise, Roemer understands why clinicians want to use their own smartphones. He noted that it is common for providers such as clinical specialists to work for more than one healthcare organization. In that case, it is not really practical for a clinician to have to carry around multiple organization-issued phones or tablets or laptops in order to get work done. "We have to allow clinicians to use their own technology, but we also have to make certain they are using it securely – according to specific organizational policies. This ensures that sensitive or confidential information is protected from unauthorized access" he said.

As specialization continues to drive innovation in healthcare, Roemer expects to see even more clinicians and other healthcare professionals work for more than one organization. In this scenario, provisioning of a secure and flexible computing platform that supports BYOD/BYOA might even become a critical factor in attracting and recruiting in-demand healthcare providers. "Will clinicians tend to want to work more with the organizations that provide a better experience for them?" Roemer asked. "If one organization offers a terribly slow, unwieldy computing platform, and another organization offers a flexible, secure and highly efficient platform, will the physicians' experience drive where they spend most of their time?"

Goel agrees that BYOD is the reality of the future for healthcare organizations. He said, "The issue is only going to become more complex as the number and type of devices and applications that access a healthcare organization's network increases. At the same time, however, healthcare organizations are getting more sophisticated in terms of the policies, procedures, processes and tools we have available to manage that risk."

With the appropriate cyber-risk management strategies in place, clinicians' growing reliance on BYOD and BYOA no longer needs to strike fear in the hearts of IT administrators. Technology tools exist that can ensure secured, mobilized and optimized app and data delivery, so that BYOD and BYOA can facilitate improved patient care, rather than compromised security.