Curbing Healthcare Workarounds:
Driving Efficient Coworker Collaboration

Featuring industry research by
HIMSS Analytics

Produced by
HIMSS Media

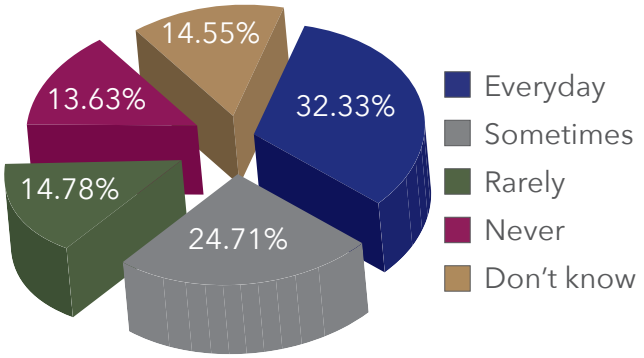
With the ubiquity of personal electronic devices, healthcare workers are all too commonly performing workarounds – alternatives to approved workflows that bypass their organizations' privacy and security measures.

Exacerbating this problem is the unapproved use of powerful consumer-accessible applications, many of which healthcare workers access via personal devices. Workarounds compromise patient data privacy and security, and resultant breaches compromise healthcare organizations' reputations and lead to fines for U.S.-based companies under the HITECH Act's protection of HIPAA-covered entities. Furthermore, because workarounds typically involve third-party data stores – often in place of approved containers – they can also compromise the integrity of patient records stored within electronic health records (EHRs) and health information exchanges (HIEs). Despite these risks, most healthcare organizations are still facing the frequent use of workarounds, according to a January 2013 Intel-sponsored survey of healthcare workers.

To investigate continuation of the workaround trend, Intel sponsored HIMSS Analytics to conduct a follow-up survey in January 2014 of 433 healthcare workers, 90 percent of whom practice in North America and 60 percent of whom work in organizations of 500 or more employees. Forty-seven percent of physicians, nurses, Information Technology directors, administrators and other healthcare employees surveyed said workarounds occur in their organizations "sometimes" or "every day," while only 15 percent said they never occur (Figure 1). This constitutes only a 4 percent reduction in the use of workarounds from the prior year.

Figure 1:

How commonly do workarounds happen in your organization, which may involve the use of alternative tools, such as personal devices, apps or social media that may be out of compliance with policy?



"Institutions have been concerned about privacy and security for a long time, but some recent and very vilifying public breaches have made people more aware and willing to act."

Nancy Vuckovic | Senior Researcher | Intel

The Aim of workarounds: Increasing collaboration to improve patient care

Although clinicians' behaviors have shown little change, the survey does indicate improvements to organizations' overall willingness to respond to workarounds. Sixty-eight percent of the 2014 respondents said they do not view security solutions' complexities as deterrents to their implementation, a 10 percent increase from the previous year. Seventy percent of healthcare entities are also now offering annual security training, while only 50 percent of respondents' organizations were doing so in 2013. "Institutions have been concerned about privacy and security for a long time, but some recent and very vilifying public breaches have made people more aware and willing to act," said Nancy Vuckovic, Intel senior researcher.

Despite these administrative improvements, the daily need for efficient collaboration is still driving the frequent use of workarounds. At 57 percent, coworker collaboration was the most often cited reason for workarounds within respondents' organizations (Figure 2).

While most healthcare providers are implementing HIEs to improve inter-institutional collaboration and meet the HITECH Act's meaningful use objectives, HIE initiatives have done little to enhance

collaboration on the individual level. "There are still immediate needs not necessarily covered by HIEs," said Vuckovic. "For example, a home health nurse might look at a patient's sore in a skilled nursing facility. An HIE won't help her connect efficiently with a colleague for a second opinion; you still need something like secure texting or message sharing."

Furthermore, while HIEs are doing little to help employees share data on a daily basis, approved processes are actually inhibiting clinicians as they attempt to collaborate. At 55 percent, "frustration with the current system" was the most common reason respondents cited for employee workarounds, and "workarounds make the job easier" was a close second at just under 50 percent. When asked which specific frustrations were driving the use of workarounds, respondents listed multiple log-in layers, slow IT departments and restrictive sets of approved applications as their primary causes of concern.

"Usability was seen as a 'nice to have' 10 to 15 years ago, but it's more important today because users have so many other tools."

David Houlding | Senior Privacy Researcher | Intel

"What this survey is telling us is that if a solution is lacking in usability, workers will still pursue workarounds," said David Houlding, senior privacy researcher at Intel. "Usability was seen as a 'nice to have' 10 to 15 years ago, but it's more important today because users have so many other tools. If the official solution is lacking in usability, or if security around it is too cumbersome, then workers will pick up alternative devices." As they attempt to deliver the highest quality care possible – a task often only achievable through efficient collaboration – clinicians are opting for improved care and ease of use over privacy and security.

Figure 2:

What are the key purposes of the workarounds?

Co-worker collaboration	56%
Patient communication	34%
Patient recordkeeping	23%
Documentation for reimbursement	9%
Reminders	35%
Other	8%
Don't know	12%

The Importance of effective BYOD policies

Perhaps the most crucial – but often lacking – element of safe coworker collaboration is an up-to-date bring your own device (BYOD) policy. As compromising as third-party applications can be, employees' personal devices account for the vast majority of workarounds. When asked to identify the most common workarounds within their organizations, respondents listed personal smartphones and text messaging at 60 percent and 50 percent, respectively. Even personal tablets and laptops accounted for more workarounds than paper-based processes, personal apps and social media combined.

However, only 47 percent of respondents' organizations currently have policies enabling BYOD, and even that figure is just a 3 percent improvement compared to 2013 (Figure 3). "That's extremely risky because healthcare workers have personal devices, and they're going to use them," said Houlding. "If an organization has a hardline denial or 'just say no' approach, it will just drive their use underground, not eliminate them." While these statistics indicate a clear gap between organizational policies and employee needs and

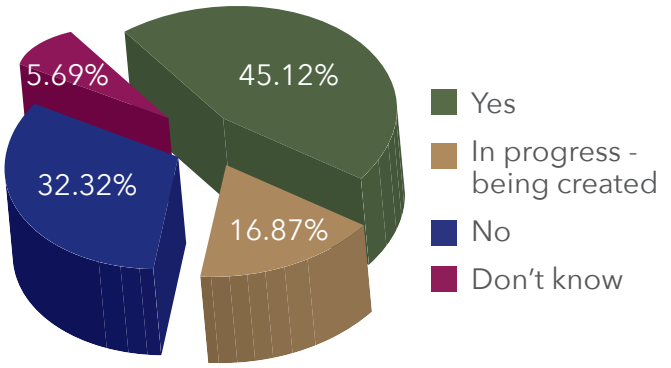
preferences, they also present a clear opportunity for improvement in both security and collaboration.

One organization that permits the use of personal devices is Massachusetts-based Partners Healthcare, a teaching affiliate of Harvard Medical School and national leader in biomedical research. "Partners is not immune to the risks posed by consumer technology, and I understand why this happens," said Christina Mazzone, information security officer for Partners Continuing Care, the non-acute care services division of Partners Healthcare. "Personal devices and public applications have been a part of healthcare's technological ecosystem long before BYOD really took off." Recognizing the need to protect patient information, Partners trains its workforce in privacy and security risks and secures their personal devices through Mobile Device Management (MDM) technology. Smartphones and tablets are secured through MDM applications such as Active Sync* and Airwatch*, and laptops are encrypted with programs such as BitLocker*, Safeboot*, PGP* and Truecrypt*.

No technology can completely prevent workarounds, however, so Partners also incorporates a variety of training measures and enforcement policies to guide its workforce away from using unapproved solutions. "Our approach has been to leverage current technology such as MDM, but also to leverage training and other administrative controls that require the individual to do the right thing," said Mazzone. "Our MDM strategy utilizes tools to block certain applications and websites and presents approved tools, but we also train, educate and sanction where appropriate."

Figure 3:

Does your organization have a policy enabling BYOD (Bring your own device) – e.g. using your personal smartphone / tablet / laptop for work purposes?



"Our approach has been to leverage current technology such as MDM, but also to leverage training and other administrative controls that require the individual to do the right thing."

Christina Mazzone | Information Security Officer
Partners Continuing Care

Enabling the use of similar alternatives to popular productivity applications gives Partners' workforce and administrators the best of both worlds. Clinicians can efficiently collaborate with their personal devices using the applications their IT departments have approved, and security personnel can enjoy greater confidence that those approved programs are protecting the safety and integrity of patient records. "We try to offer secure and comparable technologies to the DropBoxes of the world," said Mazzone.

Finally, to avoid future workarounds, Partners strives to add to its list of approved programs, limiting the risks associated with improved but still unvetted applications. "Our materials management and risk management departments have been focused on partnering with companies like Amazon Web Services* who are recognized for consumer products, but who are willing to sign HIPAA BAAs [business associate agreements] and make security a priority," Mazzone said. Houlding offered similar insights, noting that, "Lots of new technology is pushing the envelope – new apps, the internet of things and more powerful device features. Once a policy is in place, keeping it current is extremely

important." Whereas a stagnant BYOD policy might lead to the same problems as a nonexistent one, frequent updates prevent further compromises between security and efficiency.

A Holistic approach to privacy and security

Given the growing importance of coworker collaboration in today's ever-more interconnected healthcare environment, healthcare organizations must ultimately curb workarounds by addressing both usability and security concerns. "There's so much more data out there now, and there's so much potential benefit that can be unlocked by increasing collaboration," said Houlding. "We don't want to see this impeded by privacy and security, and there are ways of dealing with the risk." To that end, Houlding advises a multi-faceted approach to curbing workarounds that includes support for collaborative technologies, technical safeguards, up-to-date training and administrative policies, and concrete procedures for securing and dealing with lost personal devices.

On the support of collaborative technologies, Houlding said, "If you don't provide workers with viable alternatives, you'll just put a wall around them, and they'll find a way around it." He also noted that healthcare executives must consider the confidentiality, integrity and availability of those alternative solutions. Viable applications must safeguard sensitive data from breaches, ensure that data ends up in the proper master record and allow easy access to the clinicians who use them. Compromising any of these qualities will likely lead to a security breach, lost data or another workaround altogether.

> *"There's so much more data out there now, and there's so much potential benefit that can be unlocked by increasing collaboration. We don't want to see this impeded by privacy and security, and there are ways of dealing with the risk."*
>
> David Houlding | Intel

Training policies and methods must also drastically improve. While the proportion of organizations offering an annual security training increased from 50 percent in 2013 to 70 percent in 2014, security training offered on demand and during new employee orientation remained stagnant (Figure 4). "A lot of organizations have a once per year annual security and awareness training where all healthcare workers do is scroll to the bottom and click accept," Houlding noted. "That's just not effective in terms of absorption." Likewise, only 40 percent of respondents said the employees using workarounds are even aware of the risks involved, and a majority cited lack of oversight as the main reason people are unaware of the risks. "There's an increased need for on-the-job training, for reaching employees at teachable moments," Houlding said.

In order to implement its safe BYOD policies and secure collaborative applications, Partners has also created training practices that effectively increase awareness and change behaviors. Their primary activities include face-to-face and annual real-time online information sessions, but they also hold contests and release newsletters related to recent security risks. In November 2013, Partners even hosted its first system-wide Security and Privacy Week, which included webcasts, information tables and quizzes, and fabricated phishing schemes designed to test its workforce's knowledge of security breaches.

Just as importantly, Partners has supported its separate institutions in implementing different training and awareness programs to meet their unique needs. "For information security and privacy awareness to be effective, it really needs to be baked into the culture of its organization," Mazzone stressed. "Each institution has its own information privacy and security officers, and they all share best practices." At a time when so many hospitals and health systems are merging into accountable care organizations (ACOs), patient-

centered medical homes (PCMHs) and other new models of care, this level of independence may be crucial for institutions with different cultures to effectively curb workarounds.

Finally, any organization that implements a policy for the use of personal devices must also enforce firm rules regarding their loss. Employees must often accept that all data, personal and clinical, will have to be wiped if they lose their devices. Still, requirements for locks and device check-ins can help to prevent losses, and future MDM applications may obviate the need to remotely wipe all data. Clinicians don't want to risk losing their personal data, and they are requesting improved technologies to create secure and separate digital containers that would allow for partial wipes. Until those solutions become available, however, remote device management, encryption and data wipes must all be included in healthcare organizations' BYOD policies.

Leveraging future collaborative technologies

As cutting-edge collaborative technologies become commonplace in the near future, privacy and security policies that improve both safety and usability are only going to become more important in the competitive healthcare environment. A large majority of respondents said that internet-connected medical devices and cloud computing could be beneficial, for instance, but that privacy and security concerns impede their implementation. "To me, this shows there's still a lot of work to be done to help people rationalize privacy and security," Houlding said. "A lot of the limitations keeping people from using technology to its maximum potential come down to fear, uncertainty and doubt, but I think we can use security and privacy as an enabler." Vuckovic agreed, noting, "That's the way the field is moving forward, to have more of these devices connected to clinicians and EHRs and more and more options for the delivery of remote care." Ultimately, effective frameworks for privacy and security should make it easier for healthcare organizations to leverage the most effective collaborative technologies of today and tomorrow. ■

Figure 4:

How often is security awareness training provided by your organization?

New employee orientation	58%
Once per year annual security training	70%
Security training on demand as needed	38%
Other	5%