Workarounds in Healthcare, a Risky Trend.

Produced by HIMSS media

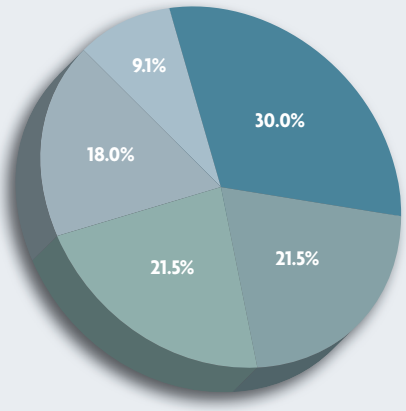
When healthcare workers bring their own laptop computers, tablets and smartphone devices to work, and use them to perform workarounds – a way to bypass an organization's systems and processes to accomplish an activity – the likelihood that patient data privacy and security may be compromised is increased significantly. This is further exacerbated by healthcare worker use of powerful collaboration apps, social media and texting, and builds upon old risks of USB keys and personal email. Even though the use of workarounds poses serious implications for managing data security, a majority of healthcare workers use this practice anyway, according to a new international survey of healthcare workers.

A recent survey, conducted in January 2013 by HIMSS Media and sponsored by Intel Corporation, relied on responses from 674 frontline healthcare workers from around the globe, most of whom (67 percent) are employed at organizations with 500 or more employees. Among the doctors, physician assistants and nurse practitioners, as well as chief information officers, IT directors and other healthcare executives surveyed, 21 percent (Graph 1) of respondents said they practice workarounds every day, while another 30 percent said they sometimes use this method to perform their tasks.

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?

- Sometimes 30.0%
- Every Day 21.5%
- Rarely 21.5%
- Don't Know 18.0%
- Never 9.1%



Workaround trend: Endangering privacy and security of patient information

Workarounds enable healthcare workers to access, share and store patient information outside the hospital's IT network. For example, a healthcare worker may use a file transfer app on a personal device to exchange unencrypted patient records. Importantly, risks associated with these workarounds apply not only to personal devices, but also to corporate devices, and even where a thin client or VDI compute model is being used.

Another aspect of workarounds is that they are not purely a client device phenomenon since in many cases they involve sensitive healthcare data moving through or being stored in "side clouds", whether for exchanging information via technologies such as file or note sharing, social media, personal email or texting. Workarounds are not in compliance with the healthcare organization's security policies and procedures, and devices may not have the proper encryption technology, antitheft software or identity protection applications that can adequately support a hospital's patient data security and privacy policies. This poses risk to the confidentiality of patient information, and increases risk of breaches. Furthermore, this practice can compromise the integrity of the patient record since patient information moving in workaround "side channels" may not be updated in the patient record leading to an incomplete or out of date electronic health record. In a best case scenario this can lead to suboptimal healthcare; in the worst case it can compromise patient safety.

Still, healthcare workers said they resort to workarounds because their organizations' IT infrastructure prevents them from performing their jobs effectively. For example, 45 percent (Graph 2) of those surveyed said workarounds are easier to use than the current system in place, while 40 percent identified their IT department as too slow to enable new technologies. The poll also revealed that 35 percent of respondents said the frustrations of having multiple layers of login to enter the system drove them to use workarounds, and 24 percent said workarounds helped them deliver better care. Additionally, 22 percent said their healthcare organizations' list of approved apps is too restrictive, 15 percent said web browser-based apps don't always work because the organization has limited network coverage, and 14 percent said separate hardware tokens required for login, and associated usability issues, make using workarounds much more attractive.

Workarounds are also popular with the 154 survey respondents located outside North America – 47 percent of whom are based in Europe, 19 percent in the Middle East, and 17 percent in the Asian Pacific region. According to these respondents, half said their number one reason for using workarounds is that their IT department is too slow to enable new technologies, 42 percent cited workarounds as being easier to use and 29 percent identified workarounds as being a process that helps them deliver better healthcare.

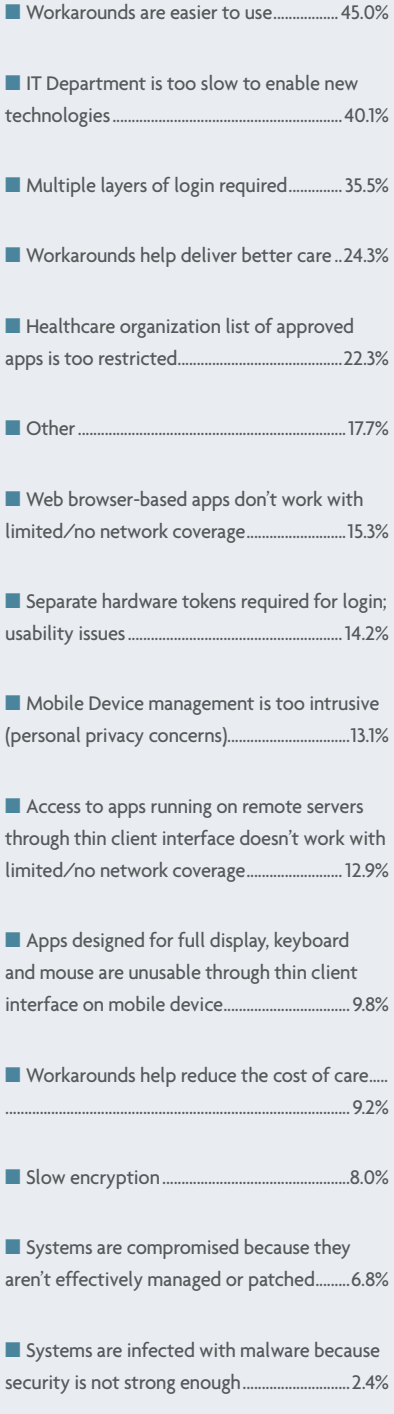
The need for IT department responsiveness

"The survey results point to a lack of actual organizational responsiveness of the IT department within the healthcare organization; if they are too slow in enabling new technology that alone can compel people to use workarounds," said David Houlding, healthcare privacy and security lead

architect at the Intel Healthcare IT Program Office. "Having usable healthcare solutions and security is important but equally important is that a healthcare organizations' IT department needs to be responsive in enabling new technologies otherwise people will bypass them."

Figure 2

What factors motivate the use of workarounds in your organization?



In the Bring Your Own Device (BYOD) era, where healthcare workers use their own smartphones, tablets and laptops to perform health-related tasks, respondents also indicated that a personal smartphone is their number one device of choice (59 percent) (Graph 3) to help them conduct workarounds as they deliver better care at a faster pace. Personal tablets came in second with 50 percent and 39 percent cited personal laptops or notebooks.

"The healthcare community must guard against situations such as a nurse taking a photo of a patient's wound on their tablet and then sending that photo to a doctor who retrieves it on his tablet, yet that photo is never entered into the electronic health record."

Linda Harrington
Vice President and Regional Chief Nursing Informatics Officer
Catholic Health Initiatives

"I have worked in healthcare environments, and have observed and spoken with nurses about workarounds. When nurses use workarounds it's a way of communicating to me that the technology is not working in the way they need it to work," said Linda Harrington, vice president and regional chief nursing informatics officer at Catholic Health Initiatives, a national nonprofit health organization based in Englewood, CO.

Harrington said the use of mobile devices enhances the reach and speed of connecting different members of the healthcare team and thus will be a key factor in gaining greater efficiency and lowering costs in healthcare. However, if the right training, regulations and security policies are not in place, the use of workarounds on mobile devices can contribute to the incompleteness of clinical documentation, and worse, can raise the risk of data breaches. "The healthcare community must guard against situations such as a nurse taking a photo of a patient's wound on their tablet and then sending that photo to a doctor who retrieves it on his tablet, yet that photo is never entered into the electronic health record," Harrington said. "Sometimes end-users with very good intentions can get ahead of the technology if you will, and it does create issues."

While many other countries around the world don't have laws that financially penalize health organizations when data breaches occur, in the United States the federal government fines health organizations if a data breach has caused harm to their patients. In fact, a much more aggressive stand has been taken by federal authorities since the Health Information Technology for Economic and Clinical Health Act (HITECH Act) became law in 2009. The law stipulates that Health Insurance Portability and Accountability Act (HIPAA) covered entities (hospitals, health plans, a group of medical professionals and so on) that uncover a data breach affecting 500 or more individuals must provide the U.S. Department of Health and Human Services (HHS) Secretary with a notice of the breach without unreasonable delay and no later than 60 days after the breach has been discovered.

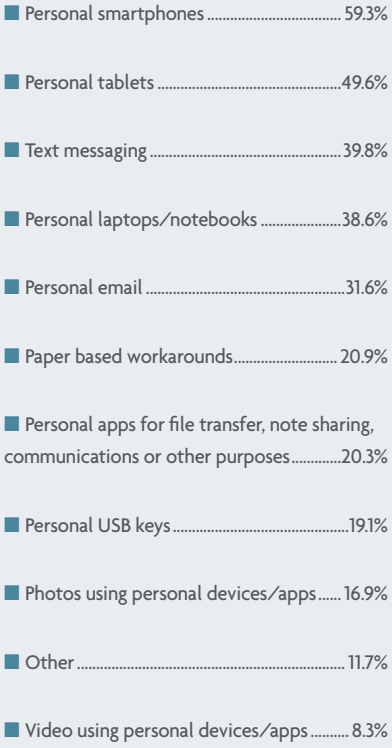
Since the law was signed, HHS estimates that as of February 21st there were 543 breaches that have affected 500 or more individuals. In fact, these breaches of health information have affected more than 21 million individuals. According to HHS's latest estimates, 23 percent of breaches of 500 or more individuals involved theft of a laptop, while roughly 14 percent involved stolen tablets, smartphones and other portable electronic devices. To prevent data breaches of patient information that occur on mobile devices, HHS included language in the Meaning Use Stage 2 final rule, which was released August 2012, that called for mobile devices to be encrypted to protect personally identifiable health data stored on the device.

Curbing workaround usage

One health organization that has embraced mobile devices and reduced the use of workarounds is Beth Israel Deaconess Medical Center (BIDMC), where John Halamka, the hospital's chief information officer, has implemented encryption technology on 5,000 smartphones, 1,000 tablets and 2,000 laptops that healthcare workers use daily at the preeminent Boston, MA-based academic medical center. According to Halamka, BIDMC implemented a policy in September 2012 disallowing BYODs that are not encrypted from using the hospital's network. "As a result of this policy, 600 smartphones

Figure 3

What types of workarounds help deliver better care more quickly? (Choose all that apply)



had to be taken out of service because they were models of personal smartphones that were not compatible with the encryption requirements that we have," he said.

While Halamka insists that each device that links to the hospital network must have encryption and use antitheft software and password authentication technology, he also pointed out following security policies is equally important to a patient data security strategy. "There's nothing like motivating a doctor by saying 'if you do a workaround you'll be fired; oh and did I mention the million-dollar fine the hospital will have to pay if we have a patient data breach'," he said.

To further strengthen security and privacy of health information, HHS announced in January the release of the final omnibus rule that makes sweeping changes to the HIPAA privacy and security rules and expands many of the requirements to protect health information to business associates of health organizations such as contractors and subcontractors. Increased penalties will apply for noncompliance based on the level of negligence with a maximum penalty of $1.5 million per violation.

The balancing act: quality of care, workflow and security

However, even while there is greater urgency to protect patient data, a significant number of survey respondents (36 percent) said they think healthcare workers using workarounds are aware of the associated privacy and security risks, yet use this practice anyway. Why? Because they are frustrated with the current system (53 percent), workarounds make the job easier (52 percent), risks are perceived to be insignificant (37 percent), improving the quality of patient care takes priority over security (29 percent) and improving efficiency and reducing the cost of patient care takes precedent over security (29 percent).

"They [healthcare workers] are compelled to do workarounds to get their job done even though many know that it may not be in keeping with their organization's privacy and security policy."

Nancy Vuckovic
Senior Ethnographer
Intel Corp.

"The results of this survey indicate that frontline healthcare workers are taking action to streamline workflows and be more efficient," said Nancy Vuckovic, senior ethnographer at Intel Corp. "They are compelled to do workarounds to get their job done even though many know that it may not be in keeping with their organization's privacy and security policy." It is notable that workarounds are occurring in an environment where respondents describe themselves as knowledgeable about their organization's privacy and security policies. Indeed, half of the respondents said they are very familiar with and know in detail their organization's privacy and security policy, while another 47 percent said they are somewhat familiar with and know the general point of these policies. Furthermore, 68 percent said their organization's policy on security is enforced via audits, 62 percent said verbal warnings are used and 60 percent said they receive warning documents in employees' files.

Effective training is emerging as a critical part of a successful privacy and security practice. Sixty-three percent said they receive online security training and half said they attend in-person training classes. Fifty-seven percent of respondents also said their organization provides security training during new employee orientation, 56 percent said they receive security training annually, and 38 percent said they obtain security training on demand and as needed. "There's a contradiction here," Vuckovic said. "In some sense there is a fair amount of training going on, but because workarounds are occurring frequently it appears that training is not particularly effective at conveying the risks of this practice."

Part of the problem could be that only 44 percent of respondents said their organizations have a policy enabling BYOD; 33 percent said they did not, 16 percent said a policy is currently being created and 8 percent said they did not know. The survey also found 54 percent identified security risks as a barrier that limits their organization's ability to make use of new technologies that could improve healthcare. With regard to encryption, while a majority of respondents (58 percent) did not feel that security solutions such as encryption are too complex to keep their organization from implementing these technologies, 20 percent said they did share the idea that solutions such as encryption are complex enough to prevent their organization from adopting such software.

Deploying a three-pronged strategy

In conclusion, as mobile devices continue to be used by frontline healthcare workers both to monitor patients as well as to deliver patient care anywhere and anytime, health CIOs, IT managers and other healthcare executives must develop a privacy and security strategy that minimizes workarounds. Health IT leaders must also craft a mobile management strategy that balances the need to implement security tools with the requirements of healthcare workers to perform their tasks with user-friendly tools that speeds up their workflow while alleviating their fears that security technology limits their opportunities to explore new applications.

"Healthcare IT managers need to convey to their clinicians that security technology is an enabler that can help them deliver improved care in a user-friendly way while minimizing the risk of security incidents such as breaches," Intel's Houlding said. "Hardware-based technologies such as encryption acceleration, hardware based remote lock and wipe, and 2-factor

"Healthcare IT managers need to convey to their clinicians that security technology is an enabler that can help them deliver improved care in a user-friendly way while minimizing the risk of security incidents such as breaches."

David Houlding
Healthcare Privacy & Security Lead Architect
Intel Healthcare IT Program Office

authentication can provide healthcare workers with usable security and strong safeguards to protect patient data. These technologies also enhance the users' experience while increasing productivity and worker satisfaction."

Intel strongly recommends healthcare organizations embrace a practical three-pronged strategy to embrace trends and technologies that improve care, while minimizing risks of workarounds:

1. Be aware of the use of workarounds in your healthcare organization, update your policy, procedures risk assessments, and implement effective training. Be explicit in addressing the practice of workarounds and help healthcare workers understand the hidden risks, rationale for safeguards, proper procedures, and their roles and responsibilities. Be creative in implementing effective training, continually.

2. To mitigate the highest priority risks in your risk assessments, implement safeguards that are not only strong, but usable, to avoid cumbersome security controls compelling the use of workarounds. Examples of usable safeguards may include hardware based 2-factor authentication without the usability issues of separate hardware tokens, high performance hardware accelerated encryption, and hardware based remote lock and wipe technology.

3. Ensure that your IT department within your healthcare organization is agile and responsive in evaluating, securing and enabling timely use of new technologies by frontline healthcare workers to improve care. This strategy also helps minimize the use of work arounds motivated by healthcare worker frustration with perceptions that IT departments are moving too slowly or being overly restrictive for example on apps approved for use.

A DIVISION OF HIMSS MEDIA
medtech media

Produced by MedTech Media, a division of HIMSS Media. ©2013
71 Pineland Drive, Suite 203, New Gloucester, ME 04260
207.688.6270 • www.medtechmedia.com