Intel IT Center

OCTOBER 2012

Pioneering Consumerization in Healthcare

The technology healthcare workers use every day—applications, hardware, and even Internet services—impacts your bottom line. Efficiency depends on balancing the need to protect and safeguard the enterprise environment with the need to provide healthcare workers with tools that deliver work experiences similar to those they experience in their personal lives. When it comes to protecting data and personal health records, IT decision makers often take a conservative approach because even small changes can have profound effects. Early adoption is typically not an option—and it's easier and safer to block access to anything but approved devices. However, this strategy is having the opposite effect.

Very likely, healthcare workers within your institution are bypassing safeguards to gain access to the latest productivity tools and technologies—and inadvertently risking patient data. According to the iPass Global Mobile Workforce Report[1], 24 percent of employees have used their smart phone to perform a workaround to access corporate data. Startling numbers, considering it only takes one healthcare worker to breach an entire organization.

As an IT organization, you can minimize this risk by embracing consumerization to improve experiences for healthcare workers and patients alike.

Simply Irresistible: The Appeal of Compelling Tools

It's important to understand why consumerization is happening across the board within healthcare, from high-level executives and doctors to nurses, clinicians, and home health workers. Healthcare often attracts professionals that tend to gravitate toward more expensive consumer products. Smart phones and tablets are pervasive within the industry, and most healthcare workers personally own both types of devices. In addition, they make use of many of the social media and consumer applications currently in market. Their experience with these products makes it easy and appealing to bring them into the workplace, inadvertently introducing significant privacy and security risks into what is a typically safe and conservative healthcare computing environment.

Embracing Consumerization across the Continuum of Care

Why not use free file hosting services to exchange x-rays and medical images with colleagues? What's the harm in sending a photo of a patient's wound to a specialist to expedite triage? Why not take advantage of other collaborative applications, such as social media, touchscreen-enabled reference libraries, visualization apps, video conferencing, mobile text messaging, instant messaging, and emergency medical response and patient monitoring? Done right, these are powerful examples of collaborative healthcare, but they risk patient privacy.

The IT organization is in a unique position to lead the charge to achieve this significant transformation. In an environment where physicians spend an average of three minutes with patients during well checks, a 30-second delay caused by technology can decrease productivity by nearly 20 percent. By taking a proactive approach to analyzing compute models and selecting the right tools for the right task, IT can improve productivity and transform paper-based workflows into highly efficient digitized processes.

Since many emerging applications and data need to be accessible from multiple devices over a variety of operating systems, security and manageability move to the forefront of IT concerns. A well-managed environment requires control of employee-owned and employer-provided devices, bandwidth, usage models, and policies.

Adopting a Layered Approach to Security and Privacy

Thin client compute models can help manage risk by controlling where sensitive data resides and how it moves over networks. This is a safe approach if a device is lost or stolen, since patient health information is not stored on the device. However, connectivity can slow response times, and networks are not always available.

Alternative compute models, such as sandboxing technologies, improve functionality by enabling devices to securely store limited sensitive healthcare data. This allows some enterprise-grade collaboration, even in rural or home health use cases that are outside of corporate networks. Sandboxing enables a more balanced compute model, leveraging the considerable multi-core processor computing capabilities of the latest smart phones, tablets, and PCs, as well as the innovative convertible tablet designs that deliver better on-the-go user experiences.

Fully equipped tablets and PCs can digitize workflows and both improve the quality and cut the costs of patient care, especially as the point of care expands beyond traditional healthcare facilities. The challenge is finding the right security measures that mitigate risk and, at the same time, appeal to healthcare workers. A layered approach, including hardware-assisted security, can be used to accelerate and harden safeguards, and make them more usable and cost effective. This strategy enables healthcare organizations to safely embrace consumerization while minimizing the risk of security incidents or breaches.

Intel®-based tablets and PCs deliver high-performance protection and rich user experiences:

- **Connect with experts**
  - Electronic patient records can be easily shared to improve quality of care, while Intel technologies provide remote lock and wipe capabilities if devices are lost or stolen.[2]
  - Advice can be safely transmitted to a remote home health nurse practitioner with Intel Identity Protection Technology[3], ensuring the data is in the right hands.
- **Expedite triage and diagnosis**
  - Mobile point-of-care and collaborative workflows improve real-time communication between EMS and hospital-based caregivers, supported by Intel Advanced Encryption Standard-New Instructions (Intel AES-NI) to mitigate risk.[4]
  - Vast databases of information and proven modes of care can affect patient outcomes—at the personal level, and in cases of epidemics, public health, and emergency response.
- **Empower patients**
  - The patient portal helps increase patient engagement with care plans, using familiar devices to increase ease of use and compliance.
  - Built-in encryption accelerators and two-factor authentication in Intel® vPro™ technology[5]– powered devices help safeguard personal health information without additional hardware.

Looking Ahead

Intel hardware-assisted security is targeted for future tablets, laptops, Ultrabook™ devices, and servers—further safeguarding consumerization in healthcare IT. For more information, visit intel.com/consumerization.

1012/BC/ME/PDF-USA 328049-001

[1] *The iPass Global Workforce Report: Understanding Global Mobility Trends and Mobile Device Usage among Business Users*, September 2012.

[2] Security features enabled by Intel AMT require an enabled chipset, network hardware and software, and a corporate network connection. Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating, or powered off. Setup requires configuration and may require scripting with the management console or further integration into existing security frameworks, and modifications or implementation of new business processes. For more information, see intel.com/technology/platform-technology/intel-amt/.

[3] No system can provide absolute security under all conditions. Requires an Intel Identity Protection Technology-enabled system, including a 2nd or 3rd gen Intel Core processor, enabled chipset, firmware, and software, and participating website. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit intel.com/content/www/us/en/architecture-and-technology/identityprotection/identity-protection-technology-general.html.

[4] Intel Advanced Encryption Standard -New Instructions (Intel AES-NI) requires a computer system with an AES-NI-enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel Core processors. For availability, consult your system manufacturer. For more information, see intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/data-protection-aes-generaltechnology.html.

[5] Intel vPro Technology is sophisticated and requires setup and configuration. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more about the breadth of security features, visit intel.com/technology/vpro.

Sponsors of Tomorrow.™