White Paper

Healthcare-Friendly Security

How usability can coexist with protection and compliance

Table of Contents

Introduction

Doctors and other senior medical professionals are well aware of their obligations to their patients—to uphold the Hippocratic Oath and provide them with the best possible care. In today's clinics and hospitals, new tools, technologies, and practices allow for greater flexibility and efficiency. Laptops, tablets, smartphones, wearable devices, thin client computing, BYOD, mobility, virtualization, and cloud services all make up the varied landscape of healthcare IT. While these technology trends and the great diversity of devices in use facilitate daily tasks and delivery of quality medical care, they also pose a huge risk and increase the likelihood of data breaches and noncompliance with regulatory healthcare mandates. According to Identity Theft Resource Center's 2013 annual list of security breaches, the healthcare sector accounted for more than 43% of all the breaches listed.[1] The Washington Post reports that more than 30 million patients have had their PHI compromised in a breach.[2]

According to Identity Theft Resource Center's 2013 annual list of security breaches, the healthcare sector accounted for more than 43% of all the breaches listed.

Lack of unified defenses that span the entire range of technologies and lack of enforceable IT policies make healthcare organizations an easy target for cybercriminals, who set their sights on accessing highly prized patient healthcare information PHI records, which contain a plethora of data that can be exploited and monetized. Data breaches profit cybercriminals, but they can have a big negative effect on the bottom line for healthcare organizations. In its study, *2014 Cost of Data Breach Study: Global Analysis*, the Ponemon Institute estimates that the average cost of data breach is now $3.5 million USD, which is an increase of 15% over 2013.[3]

Healthcare practitioners themselves, who value usability, often unwittingly put their organizations and their patient's data at risk. Beyond the all-important priority of attending to patients, healthcare professionals are also required by law to protect the privacy and security of PHI. However, the way they use technology to perform their jobs often does not align with that requirement. With large patient loads and heavy schedules, healthcare practitioners feel the need to respond rapidly, so they use whatever means are available to them to capture patient data quickly and send it on its way to the next device or the next practitioner in an effort to mend bodies and save lives. And often, that means data security takes a backseat. Security controls are often seen as an impediment, and security workarounds are commonplace. As a recent HIMSS white paper points out, "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."[4]

What is needed is healthcare-friendly security—easy-to-manage solutions that lock down PHI and enable its efficient and safe collection, transit, and storage in a clinical setting. The probability of a breach is minimized, compliance is maintained, and patients benefit from improved trust and reduced healthcare costs. Intel Security and McAfee, a part of Intel Security, offer a wide range of solutions that integrate security software with security hardware for both improved usability and hardened security on devices used in the healthcare environment, empowering healthcare practitioners with flexible technology options that enable them to deliver the best possible care.

Usability Is King in Healthcare

At today's typical healthcare facility, larger volumes of data move at a higher velocity than ever before. In addition, there are new types of data coming from new sources—from smartphones to networked medical devices. All of this is due in part to the adoption of new technologies and the trend toward greater collaboration—and usability reigns supreme as busy doctors and other ground-floor practitioners under time and cost reduction pressure strive to deliver top-notch care to their patients. In the midst of these exciting and positive developments, it has also become apparent that usability has the upper hand over security, as practitioners are driven by necessity and urgency. But the very technology and practices that empower them to be more efficient and effective also put valuable patient data—and the entire organization—at risk. In this fast-paced environment, time is of the essence, so practitioners often perform security workarounds in an effort to do a better job.

Why Cybercriminals Target Protected Health Information (PHI)[5]

- Credit card information can fetch $1 USD per record in the cybercriminal underground economy. A full identity profile, which is supplied by PHI, is worth 20 to 50 times as much per record.
- PHI theft is difficult to detect.
- Victims can cancel credit cards, but they cannot cancel their PHI.
- With PHI in hand, cybercriminals can open new credit card accounts, access prescription drugs, and submit fraudulent insurance claims.
- There are greater opportunities for blackmail or extortion with respect to sensitive healthcare information.

What Is a Breach?

"A 'breach' means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."[6]

—SEC. 13400. DEFINITIONS, American Recovery and Reinvestment Act of 2009

The risks of convenience and flexibility

Let's take a look at the healthcare computing landscape and the potential risks posed by these new tools and ways of working.

- **Increased collaboration drives frequent security workarounds:** In an HIMSS Analytics survey in 2014 of 433 healthcare workers, mostly in North American, 57% of respondents cited the need to collaborate as the key motivator for workarounds. For example, a doctor who is examining a patient and requires a second opinion from a colleague may use a smartphone to snap a photo and send an SMS text message. In terms of usability, the biggest cause for concern among survey participants was multiple login layers, slow-to-act IT departments, and an overly restricted set of approved applications.
- **BYOD and use of unauthorized applications:** Most workarounds occur on employees' personal devices, including laptops, tablets, and smartphones with many different operating systems. And, the fact is, hospitals and other clinical settings often don't have firm BYOD policies and guidelines on approved applications and security. All too often, practitioners accidentally email patient data via unsecured networks or share it on DropBox or other cloud services. Even USB drives storing unencrypted PHI are risky, as they can be easily misplaced or end up in the wrong hands. Without a solid BYOD program and strong encryption, it's almost impossible to properly secure data and maintain the necessary patches and security upgrades on personal devices.
- **Thin client computing devices or virtualized desktop interfaces (VDIs):** Thin client terminals are often used in healthcare for greater control and are presumed to be more secure, but the problem is, many thin clients rely on common browsers to perform user functions, such as accessing applications and data from the Internet or cloud services. Some thin clients can store data remotely on servers, and some store and acquire data files locally, much like a PC, to enable users to access them—and that includes the use of removable storage devices such as USB flash drives. Of course, it's common knowledge that browsers are probably the most exploitable and vulnerable applications in existence—and no matter where the PHI goes, the cybercriminals will be sure to follow.[7]
- **Wearable computing devices, like smart wristbands, watches, and goggles, create a whole new set of risks:** The Internet of Things (IoT) is quickly gaining ground in all sectors, especially in the health and fitness sector, where devices that monitor heart rate, perspiration, and movement are already popular. Apple Computer is setting the stage for this trend with the Apple HealthKit for iOS 8 developers which will gather a user's health data into a single "storage locker" and make it possible for third-party applications to access and share it. And this is just the beginning. According to Statista, the wearable market will increase by 67%, from 53.9 million devices in 2013 to 1.64 billion devices by 2015.[8] In time, these devices will help doctors gather data for patients to determine the effectiveness of certain treatments, procedures, and medications. Doctors will be able to collect some rich and highly relevant health information from clients, but, unfortunately, like laptops or mobile devices, wearables containing sensitive patient data can be lost or stolen. And that data is often transferred to a mobile app through unsecured Wi-Fi connections or Bluetooth.

- **Networks, servers, and data centers are vulnerable:** Just like any other commercial enterprise, hospitals can also be subject to sophisticated network attacks, like stealthy advanced persistent threats (APTs), which enter the network, are difficult to detect, and can stay around for a long time. This year, one of the largest breaches ever reported to HIPAA involved the theft of millions of patient records at a US hospital. Foreign cybercriminals exploited a network vulnerability known as "Operation Heartbleed" and were able to appropriate the records by making their way through the network to a database stored on a server. Network vulnerabilities, negligence in applying security patches on a timely basis, and weak administrative passwords are often to blame for these types of breaches.
- **Lost or stolen devices:** According to the *Verizon 2014 Data Breach Investigations Report*, 46% of data breaches in healthcare result from theft or loss of unencrypted laptops and other devices.[9] Cybercriminals frequently execute cold boot attacks to steal PHI when a PC is powered on or in a standby state—even if it's password-protected. Sensitive data can be easily accessed by rebooting the system and running a small program on the next boot cycle that scans system memory for this information. Hackers then remove the RAM from the powered-on system and transfer it to another system.

Consequences of a PHI Data Breach

Now you have a clear picture of the vast variety of technology tools used every day in healthcare—and the level of risk they bring into an organization. No one wants a breach, and there are some very good reasons why.

"[Physical theft and loss] is the biggest hands-down problem in healthcare that we are seeing. It really surprises me that this is still such a big problem. It's one of those things that encryption is such an easy safe harbor. Other industries seem to have gotten this fairly clearly."[10]

—Suzanne Widup
Senior Analyst
Verizon RISK Team

How does a breach occur?

There are so many reasons why a breach happens—generally from human error or lax IT processes and controls. Here are some recent examples based on actual reported breaches at medical organizations:

- A healthcare worker used unauthorized cloud-based apps with PHI.
- A network server was exploited due to a weak password.
- Backup disks were discovered missing from a storage facility that was left unlocked.
- Excel spreadsheets with PHI information were copied and stolen—most likely by an insider.
- Doctors at a world-renowned medical center provided employees with their user names and passwords, enabling the employees to access patient records, including those of top celebrities.
- A server was hacked, resulting in the misappropriation of more than 400,000 PHI records of past and current patients. Data stolen included Social Security numbers, addresses, and financial information.
- An unencrypted laptop with patient information from a well-known hospital was stolen from an employee's car.

What are the consequences?

- **The US Department of Health and Human Services (HHS) "Wall of Shame":** Healthcare organizations that experience a breach affecting 500 people or more are required by law to report it. HHS then publishes the information online, and it is posted to the "Wall of Shame."
- **OCR audit:** If a patient reports a breach to the HHS Office for Civil Rights (OCR), the healthcare organization must undergo a four-part risk assessment to prove that PHI was not compromised or leaked. If the organization passes the test, the breach does not have to be disclosed. Preparing for the OCR audit can be a costly and time-consuming task in itself. It includes assigning an audit response team, reviewing HIPAA compliance documents, internal risk assessment to identify security gaps and weakness, addressing deficiencies, and identification of third-party business associates (from cloud service providers to insurance companies, all of whom are subject to the same regulatory mandates). Additionally, an organization might need to invest in compliance reporting software—which is yet another cost that is incurred.[11]
- **Failing an OCR audit:** What happens if a healthcare organization does not pass the audit? Aside from all the above-mentioned expenses, steep fines can be expected. The typical fine for a data breach runs up to $1.5 million USD per incident. The recently enacted HIPAA Omnibus rule (and written into the **Health Information Technology for Economic and Clinical Health [HITECH] Act** of 2009) is strict in scope. It requires organizations to provide detailed documentation and authorizations when patient information is released, it limits the use of patient data for marketing and fundraising, and it holds healthcare providers accountable for the actions of their business associates. Requirements for data protection are also tougher than ever before, especially when it comes to storage and transmission of electronic PHI in all forms—scanned images, screen captures, data files, and document files.
- **Your reputation may be tarnished:** No matter how many patient records are involved in a breach, healthcare organizations need to notify the patients whose records were compromised. That can result in a serious loss of "customer confidence"—and potentially negative comments posted on social media sites. Additionally, once the breach is reported (especially when it involves more than 500 records), negative PR is almost inevitable. The last thing any healthcare organization wants is to make headlines due to a security breach. In a recent study conducted by the Ponemon Institute, 54% of companies stated that it could take as long as 10 months to in excess of two years to restore a company's reputation following a breach.[12] In addition, healthcare organizations may be faced with class action lawsuits filed by patients who feel that their trust has been violated.
- **Patients may endure identify theft or financial losses:** It's not just hospitals and medical facilities that suffer after a breach has occurred—patients also have to bear the burden. PHI records are a gold mine for hackers. Chock full of information—like credit card numbers and Social Security numbers—that could be used to turn a profit, PHI is valued at 20 to 50 times more than credit card information in the cybercrime black market. Breaches put patients at risk of identity theft, credit card fraud, insurance fraud, and much more. In addition, patients may experience disappointment in their healthcare providers and decide to seek out other medical facilities as an alternative. The Ponemon Institute's *2014 Cost of Data Breach Study: United States* report indicates that healthcare has had an abnormally high churn rate of 5.3%, as compared to retail, for example, which has had a churn rate of 1.4%.[13]

Risk Mitigation Recommendations

Physicians and other practitioners are well aware of the benefits of prevention as a strategy to maintain good health. The same principle applies to the cyberworld in a clinical or hospital setting. Preventative strategies and practices will reduce the probability of a breach and assist with the ongoing effort to maintain regulatory compliance. The **HealthIT.gov website** provides tips for securing valuable patient data, such as strong passwords for all devices (including servers), antivirus software, setting proper access permissions, limiting physical access to computers and devices, as well as network access, safeguarding mobile devices, and proper planning and user education.[14] The implementation of additional technologies and policies can further strengthen your organization's security posture. Here is an example checklist. The actual checklist for your organization will depend on your risk assessment.

- Mandatory encryption/OPAL drives for all portable devices.
- Encryption of all backups.
- VPN for all remote access.
- Digital rights management solutions.
- Establishment of a Bring Your Own Device (BYOD) policy.
- Internal security audits.
- Scheduling regular risk assessments to address deficiencies and monitor effectiveness of existing safeguards.
- Business Associate Agreements and assessment of the data security of third-party partners and associates.
- Security incident response plans.
- Securing paper records.
- Proper disposal for paper and electronic devices that are no longer in use.

"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
Healthcare Privacy and Security Lead
Intel

The Best of Both Worlds: Usability and Security

After reviewing this checklist, you may be inclined to think that such security measures will rob you of the efficiency and flexibility you have come to rely on to give your patients the best possible care. But you don't necessarily have to rethink your tools and workflow—nor give anything up to keep PHI secure. There are ways that enable a harmonious coexistence between usability and security. Intel Security and McAfee provide usable, robust security solutions with vertical integration of security software and security hardware. Here are some examples:

- **Fast, transparent encryption:** Intel AES-NI technology accelerates encryption at the processor level. Usability is unimpeded while valuable patient information is fully protected both at rest and in transit.
- **Data loss prevention solutions:** Intel AES-NI technology works hand in hand with McAfee® Data Loss Prevention (McAfee DLP), which has a variety of tools that help users become more data-aware. It can discover unsecured healthcare data both at rest and in transit, and automatically encrypt it. McAfee DLP notifies employees of noncompliant actions and, in that sense, offers on-the-job training in security best practices.
- **Centralized security management:** With McAfee ePO™ Deep Command, IT can remotely manage security on Intel® vPro™ Active Management Technology (AMT)-enabled PCs and fixed-function devices, including Ultrabooks, laptops, and intelligent systems—even when these devices are powered off. Security updates can be applied off hours, and if there is a security problem, remediation can be done quickly without impinging on your need to get your job done effectively.

- **Mobile security management solutions:** McAfee Enterprise Mobility Management (McAfee EMM™) allows health professionals to use BYOD and corporate-issued smartphones and tablets (Apple and Android) with confidence and without workflow disruption. McAfee EMM provides antivirus capabilities, reputation scanning for apps, and remote wiping and locking of devices should they get lost or stolen. Security and provisioning are managed centrally by IT, which provides control without interference.

The chart below provides some additional details on how Intel Security and McAfee products can help your organization facilitate security while preserving and even enhancing usability. Hospital administrators, IT, and senior healthcare practitioners will find it helpful to familiarize themselves with these solutions and capabilities as they strategize programs and policies that support quality healthcare, enable usable solutions, and maintain the privacy of patient healthcare records.

			Benefit			
Security Capability	**Intel Security Solution**	**Other Considerations**	**Breach Avoidance**	**Regulatory Compliance**	**Improve Usability and Efficiency**	**Simplify IT Processes**
Data Loss Prevention	**McAfee DLP** (for endpoints and the network) with **Intel AES-NI**	• Hardware-accelerated, high-performance encryption. • Employees are empowered to self-remediate in the event of noncompliant action. • DLP helps manage "data in flight," preventing unauthorized distribution of data to printers, network, and removable media.	■	■	■	
Encryption	**McAfee Complete Endpoint Protection** with **Intel AES-NI and Intel Secure Key**	• High-performance encryption via the Advanced Encryption Standard with New Instructions is dedicated to accelerating encryption for "data at rest." • Hardens encryption to thwart advanced cybercrime threats. • Prevents cold boot attacks.	■	■	■	■
Solid State Drives with Encryption	**Intel SSD**	McAfee Drive Encryption automatically determines if the drive on the endpoint is self-encrypting or not. If so, software encryption will not be configured, and the drive will still be managed securely.	■	■	■	
Centralized Management of Security	**McAfee ePO with Deep Command and Intel vPro AMT**	• Remotely manages security on Intel vPro-based PCs, laptops, and tablets. • Security updates and remediation can be done off hours so workflow is uninterrupted.	■	■	■	■
Mobile Provisioning and Security	**McAfee Enterprise Mobility Management**	• Enables secure BYOD for Mac and Android devices. • Remote lock and wipe for lost or stolen devices.	■	■	■	■
Visibility Across All Devices and Automated Updates	**McAfee ePolicy Orchestrator®**	• Reduces IT management headaches. • Protects users without interfering with their workflow. • Ensures compliance across the entire organization.	■	■	■	■

Security Capability	Intel Security Solution	Other Considerations	Benefit			
			Breach Avoidance	Regulatory Compliance	Improve Usability and Efficiency	Simplify IT Processes
Hardening Against Cold Boot Attacks and Five Pre-Boot Authentication Options	**McAfee Drive Encryption**	• Ensures encryption keys are moved out of system memory when entering Connected Standby mode. • Helps to balance security with user access or location. For example, faster authentication is enabled in the clinic or hospital, and more security is enabled in public Wi-Fi hotspots, such as airports and coffee shops.	■	■	■	■
Secure Password Recovery	**McAfee Endpoint Assistant App**	• Associates smartphones with their laptops encrypted by McAfee Drive Encryption. • Enables users to access to their laptops 24/7 without calling the IT help desk.	■	■	■	■

Summary

Today, usability and security are vital in a clinical healthcare environment. Dedicated physicians and other practitioners are eagerly embracing new and potentially risky technologies that help them collect and share important patient data as they strive to deliver better, more efficient care. At the same time, healthcare organizations are faced with the dual pressures of a threat environment where breaches have become commonplace and strict regulatory mandates demand tougher security controls. With the help of integrated security solutions from Intel Security and McAfee, healthcare organizations can successfully unify usability and security to satisfy the needs of patients, practitioners, administrators, and IT.

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. **www.intelsecurity.com**.

1. **http://www.nuemd.com/news/2014/10/08/report-healthcare-sector-accounts-more-43-percent-data-breaches**
2. **http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/**
3. **http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis**
4. **http://www.intel.com/content/dam/www/public/us/en/documents/reports/curbing-healthcare-workarounds-report.pdf**
5. **http://www.emc.com/collateral/white-papers/h12105-cybercrime-healthcare-industry-rsa-wp.pdf**
6. **http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf**
7. **http://www.infoworld.com/article/2621954/security/we-re-doomed-to-insecurity-in-the-cloud-and-on-thin-clients.html**
8. **http://www.fool.com/investing/general/2014/07/09/who-stands-to-benefit-when-healthcare-wearables-ar.aspx**
9. **http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf**
10. **http://www.fiercehealthit.com/story/ocr-levies-2-million-hipaa-fines-stolen-laptops/2014-04-23**
11. **http://www.compliance.com/how-to-prepare-for-ocr-audit**
12. **http://www.databreachtoday.com/whitepapers/ponemon-institute-study-reputation-impact-data-breach-w-540**
13. **https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=gts-LITS-bus-conn-NA&S_PKG=ov23300**
14. **http://www.healthit.gov/providers-professionals/cybersecurity**

Disclaimer: This document does not constitute a legal summary, nor is it meant to provide legal advice about healthcare regulations. Detailed information about federal and state healthcare regulations is publicly available.

Intel® vPro™ Technology: Intel® vPro™ Technology requires setup and activation by a knowledgeable IT administrator. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. Learn more at: **http://www.intel.com/technology/vpro**.

Intel® Active Management Technology (Intel® AMT): Intel® AMT should be used by a knowledgeable IT administrator and requires enabled systems, software, activation, and connection to a corporate network. Intel AMT functionality on mobile systems may be limited in some situations. Your results will depend on your specific implementation. Learn more by visiting **Intel® Active Management Technology**.

Intel® Data Protection Technology: No computer system can be absolutely secure. Requires an enabled Intel® processor, system and software designed to use the technology. Check with your manufacturer or retailer. **Intel® Data Protection Technology with AES-NI and Secure Key**.

SSD Pro: No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® Solid State Drives may require additional software, hardware, services and/or an Internet connection. Results may vary depending upon configuration. Consult your system manufacturer for more details.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit, **http://www.intel.com/performance**.

61532wp_healthcare-dp_1214_ETMG