**WHITE PAPER**
**Intel Hardware-Based Security Solutions**
Healthcare

# Health Information at Risk: Successful Strategies for Healthcare Security and Privacy



**David Houlding, MSc, CISSP**
Healthcare Security and Privacy
Healthcare IT Program Office
Intel Corporation

## RISING RISKS, GREATER THREATS, LIMITED BUDGETS

Improving the quality and reducing the cost of patient care depends on digitizing healthcare workflows and moving to electronic patient records. These records are a type of sensitive information, also referred to as electronic Protected Health Information (ePHI). Sensitive information in electronic form presents new vulnerabilities compared to paper-based equivalents. The security and privacy risks associated with sensitive information are increased by several growing trends in healthcare, including clinician mobility and wireless networking, health information exchange, cloud computing, "bring your own computer," and the use of Personal Health Records (PHRs). The sophistication of malware and security threats is increasing. Compounding these challenges are the limited budgets that healthcare organizations typically have available to mitigate risk, coupled with the rising consequences of failure to safeguard sensitive information.

This whitepaper describes an industry-standard approach that healthcare organizations can use to assess risks and identify security and privacy needs. We also share a multi-layered, defense-in-depth strategy that can help healthcare organizations mitigate risks throughout the threat lifecycle to protect the confidentiality, integrity, and availability of sensitive information. With this foundation in place, we discuss specific security and privacy needs for healthcare organizations and describe several Intel® technologies that can help address these needs:

- Mitigating loss or theft of sensitive information
- Protecting sensitive information at rest, in transit and in use
- Protecting access to sensitive information with strong authentication
- Improving security and privacy policy compliance

## Table of Contents



## Identifying Security and Privacy Needs in a Healthcare Organization

In today's world of vital electronic information and malicious threats, healthcare organizations are finding that a reactive, bottom-up, technology-centric approach to determining security and privacy requirements is not adequate to protect the organization and its patients. To avoid breaches of sensitive information and other types of security incidents, healthcare organizations must take a proactive, preventive approach with attention to future security and privacy needs. To apply the limited funds available in a way that maximizes the reduction of business risk, healthcare organizations should use a top-down approach based on risk assessment, and should mitigate risk through a combination of administrative, physical, and technical security controls.

As Figure 1 shows, the widely recognized best known method for determining an organization's security and privacy requirements for such an approach is driven by applicable regulations; standards such as the International Standards Organization's ISO 27001 and ISO 27002 for Information Systems Management Security and Security Techniques[1]; and principles such as the American Institute of CPA's Generally Accepted Privacy Principles (GAPP),[2] Organization for Economic Co-operation and Development (OECD) Guidelines,[3] or European Union (EU) Directives.[4] Healthcare needs including the classification of data and usage models are also a key driver that influences security and privacy within a healthcare organization.

Policy is the foundation of a healthcare organization's security and privacy practice, and should be reviewed and approved by the organization's senior management. Security and privacy risk assessments may be done based on the policy, and involves modeling risks. A risk is a function of the probability of a threat agent exploiting a vulnerability, and the resulting business impact. Risks modeled in the assessment may be prioritized based on probability and business impact. They may be compared to baselines of acceptable risk set in the policy. Risks that exceed baselines may be mitigated in priority order by applying security and privacy countermeasures, also referred to as controls or safeguards. Mitigating risks in priority order enables healthcare organizations to apply their limited budget to mitigate the maximum business risk.

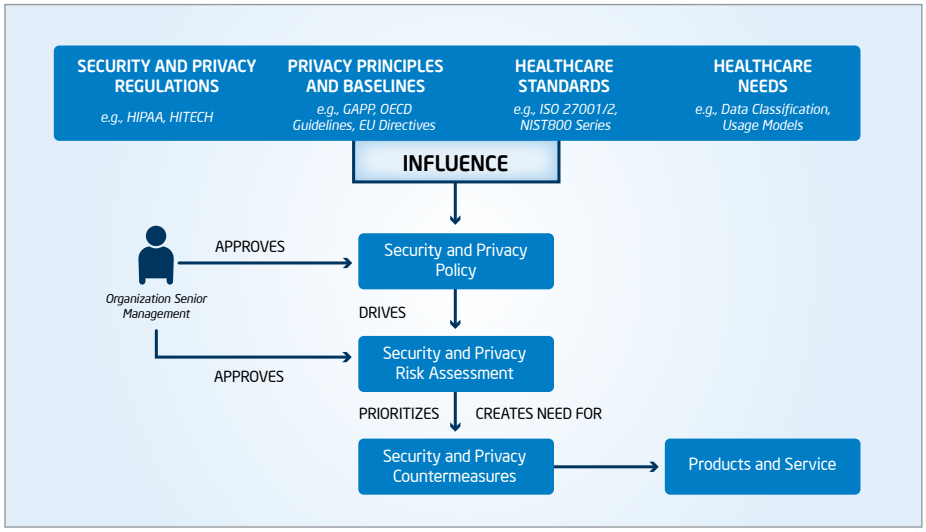


**Figure 1.** Identifying Security and Privacy Requirements in a Healthcare Organization.

When risks are mitigated to within acceptable baselines, then security and privacy is adequate by definition. This enables the healthcare organization to address security and privacy with a measured response and decide when the job is done.

Security and privacy countermeasures identified through this approach may be implemented using security products and services. Intel provides a broad suite of hardware-assisted security technologies including:

- Intel® AES-NI, with new instructions for robust, high-performance encryption based on the widely used Advanced Encryption Standard, to protect the confidentiality of sensitive information whether at rest, in transit, or in use[5]
- Intel® Anti-Theft Technology (Intel® AT) for mitigating loss or theft of sensitive information on PCs[6]
- Intel® Identity Protection Technology (Intel® IPT) for strong authentication to protect access to sensitive information, available in select 2nd generation Intel® Core™ processor-based PCs[7]
- Intel® Virtualization Technology (Intel® VT) for high performance secure virtual computing in the data center, the cloud, or the virtualized PC[8]
- Intel® Trusted Execution Technology (Intel® TXT) for protecting the confidentiality and integrity of healthcare systems and sensitive information on PCs and servers[9]
- Intel® Active Management Technology (Intel® AMT) for secure remote management of PCs to improve security and help enforce compliance with security and privacy policy

## Protecting Confidentiality, Integrity, and Availability

The need to protect confidentiality and avoid unauthorized disclosure is relatively well understood in healthcare, and is driven by the desire to avoid breaches of sensitive information. With breach notification now required by many regulations, the consequences of breaches are more serious than ever.

Encryption is an effective countermeasure that can help guard against data theft. However, users may disable their software-based encryption solutions because of concerns that encryption's performance requirements will slow the PC's responsiveness, affecting application usability and user productivity. Intel AES-NI provides hardware-assisted encryption that gives clinicians the protection of encryption while maintaining good performance, usability, and productivity. Intel AES-NI can be used to accelerate the performance of encryption by 3 to 10 times when compared to a completely software implementation of AES encryption.[10]

In healthcare, the confidentiality of sensitive information must be protected end-to-end while the data is stored, used, and exchanged. Intel AES-NI is a versatile solution that healthcare organizations can apply to a variety of encryption needs, in contrast to other point encryption acceleration solutions targeted at one specific area, such as self-encrypting disks or Secure Sockets Layer/Transport Layer Security (SSL/TLS) accelerators. Intel AES-NI may be used to encrypt information that is at rest on hard drives or removable storage devices, in transit (for example using SSL/TLS), or in use in applications or databases. This versatility supports robust protection of sensitive information end-to-end throughout healthcare systems.

In healthcare, the confidentiality of sensitive information must be protected end-to-end while the data is stored, used, and exchanged.

Policy is the foundation of a healthcare organization's security and privacy practice

As more sensitive information is consolidated in Enterprise Health Record (EHR) systems, the need to avoid breaches through unauthorized access to EHRs becomes increasingly critical. "What you know" username/password authentication is relatively weak. Increasing the complexity of passwords has had limited success in practice, since with increasing password complexity, users are more likely to write down passwords or forget them and burden the help desk. In addition, even strong and complex passwords are vulnerable to malware such as key loggers. Two-factor authentication involving an additional "what you have" hardware token provides strong authentication, but presents support and usability challenges with hardware tokens getting lost or damaged, or proving burdensome for users. Intel IPT enables strong two-factor "what you know and have" authentication, without these support and usability challenges; it combines a typical "what you know" password with a six-digit One-Time Password linked to the client computing platform.

With healthcare organizations digitizing critical workflows, protecting the integrity of the sensitive information and systems that process it is also critical. This includes ensuring that sensitive information and systems are complete, accurate, and up-to-date, and are modified only by authorized individuals. Intel TXT provides a trusted execution environment in which to run healthcare applications with sensitive data. It includes a verified launch capability to ensure the integrity of the execution environment, such as a virtual machine (VM), and to mitigate risks associated with the presence of malware or root kits. Intel TXT also provides hardware-enforced separation of VMs to prevent malware from compromising the integrity or confidentiality of healthcare applications with sensitive data running in adjacent VMs in a multi-tenant environment.

When a VM running a healthcare application shuts down, Intel TXT can scrub the memory to protect the confidentiality of sensitive information in memory. Security capabilities provided by Intel TXT are especially important in virtualized shared environments such as in cloud computing. In virtualized environments, Intel VT also provides additional protection of graphics and I/O. Intel TXT makes use of a hardware Trusted Platform Module (TPM), which also provides sealed storage that shields sensitive data from attack while stored or in use. This can help protect certificates used to authenticate clinicians.

As patient care becomes critically dependent on electronic patient records and workflows, healthcare organizations must also ensure that sensitive information is available to authorized individuals whenever they need it. Timely and reliable access thus becomes as important as protecting confidentiality and integrity. Healthcare organizations face a variety of threats to availability, some malicious such as denial of service attacks, and some accidental or environmental. A robust, holistic security and privacy practice can mitigate such risks through countermeasures such as intrusion detection and prevention systems, backup and recovery, and business continuity and disaster recovery planning.

## Robust Security Using a Multi-Layered Approach

Mitigating risk and providing robust security and privacy within a healthcare organization requires the use of administrative, physical, and technical controls (see Figure 2). For example, the encryption technical control is not as effective in practice without administrative controls, such as policy that emphasizes the importance of maintaining the confidentiality of sensitive information, training in security awareness, and auditing to enforce policy. Similarly, physical controls such as locks and secure perimeters are required to ensure secure use, transport, and storage of devices containing and processing sensitive information.

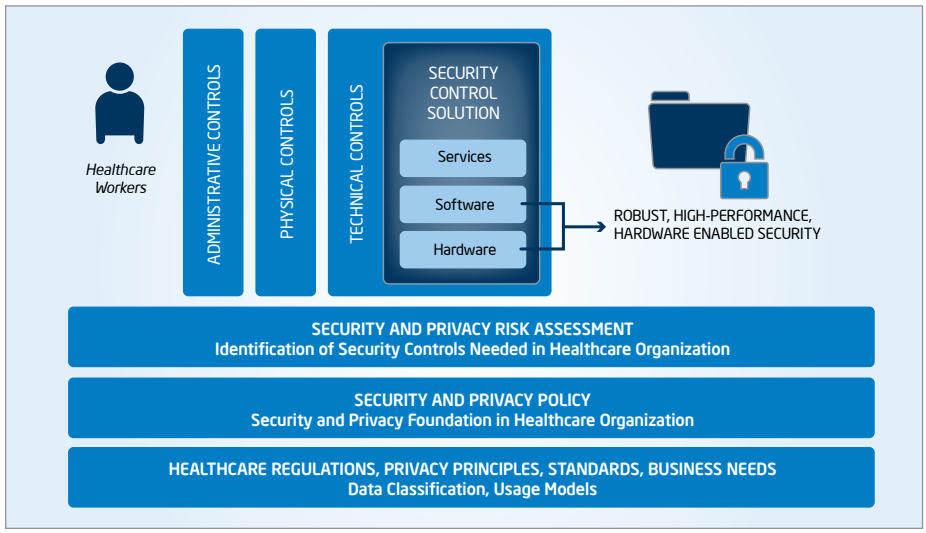


**Figure 2.** Layered approach to security and privacy.

## Robust, High-Performance Hardware-Assisted Security

For technical controls required to mitigate security and privacy risk, hardware-assisted security, used with enabled software, provides key advantages over software-only technical controls.

Attacks on healthcare organizations and systems are becoming increasingly sophisticated. Traditional software-only security controls can be circumvented and may be vulnerable to malicious change. Hardware-assisted security can help healthcare organizations harden these systems (Figure 3).


**Figure 3.** Hardware-assisted security.

A hardware trusted root element at the base of the security solution is immutable and not subject to vulnerabilities associated with malicious change, as is the case with software-only security solutions. This robustness can be transferred to higher elements of the security solution; for example, through a verified launch or the step-by-step boot chain of trust, as provided by Intel TXT. As we've seen, hardware-assisted security also encourages compliance by removing the performance penalty that previously may have led many users to disable software-based security solutions.

Increased complexity brings increasing vulnerabilities. Hardware-assisted security moves core processing into the hardware where it is less prone to vulnerabilities such as side-channel leaks. This also simplifies and streamlines the software part of the security solution, reducing its vulnerabilities and improving the robustness of the overall security solution.
For the benefits of hardware-assisted security to be realized in the end security solution, software and services higher in the solution stack must recognize and be compatible with the hardware-assisted security. Setup and configuration procedures are also typically required to activate hardware-assisted security.

Intel security technologies provide robust, high-performance, hardware-assisted capabilities to enhance security.

Intel security technologies provide robust, high-performance, hardware-assisted capabilities to enhance security. These technologies maximize the use of standards; for example, AES-NI is based on the Advanced Encryption Standard that is standardized by the National Institute of Standards and Technology (NIST)[11] and is currently the dominant symmetric key block cipher. These hardware-assisted technologies also provide an open foundation for third-party software vendors and service providers to innovate and provide compatible software and services.

## Strengthening Security Using a Defense-in-Depth Approach

Of course, encryption is not a panacea for breaches. It may fail as a security safeguard due to vulnerabilities such as users' turning off encryption, using weak encryption passwords, or leaving a system in an unlocked state (such as a laptop left active or in standby mode that does not require pre-boot authentication). When such actions open the door to a serious and costly breach, many healthcare organizations require a higher level of assurance that sensitive information is secure. This can be achieved using a multilayer, defense-in-depth approach.

Intel Anti-Theft Technology can further mitigate risk of loss or theft of sensitive information on a laptop PC. Healthcare organizations can send a poison pill to a lost or stolen laptop to prevent the machine from booting and accessing sensitive information, mitigating risk of a breach of confidentiality. If a lost or stolen laptop is unreachable over the network, Intel AT protections can be initiated locally through a hardware rendezvous timer triggered when the laptop is late in contacting a central server. Similarly, consecutive failed login attempts reaching a threshold may also be used to initiate Intel AT protections locally on the laptop. Intel AT provides a robust additional layer of protection above encryption, and these two technical security control layers together provide a defense-in-depth protection of sensitive information on mobile laptops, with an increased level of assurance to healthcare organizations and patients that their data is safe.

## Mitigating Risk Throughout the Threat Lifecycle

Mitigating the security and privacy risk to healthcare organizations requires the use of countermeasures throughout the threat lifecycle, from prevention, through detection, response, and recovery.

A key goal in the security and privacy policies of healthcare organizations is to keep systems up to date. New vulnerabilities are constantly emerging, especially in software. Mitigating the risk of security incidents associated with these new vulnerabilities requires the timely application of security patches. When a new vulnerability surfaces in a zero-day attack, software vendors create and issue a patch, and healthcare organizations are then challenged to rapidly deploy this patch to their PC fleets, since any delay increases the window of attack based on the new vulnerability.

Typically patches can be rolled out to the majority of PCs in a fleet in an automated, timely manner. However, it is not uncommon for patching to fail for up to 20 percent of PCs in the fleet, for example, because PCs are powered down or inoperable. Any delay in applying security patches increases the window of opportunity for attacks based on the new vulnerabilities, and raises the risk of security incidents.

Intel® Core™ vPro™ processor-based PCs can be securely reached and patched by a remote central administrator over a wired or wireless network, even when the PC is powered off.[12] This enables IT technicians to achieve full patch saturation more quickly and efficiently, avoiding the cost and delay of deskside visits, and mitigating risk by minimizing the window of attack based on new vulnerabilities. This use of Intel® vPro™ technology is an example of a technical control applied at the prevention part of the threat lifecycle. If a PC does become infected with malware, Intel vPro technology can also be used during the recovery part of the threat lifecycle to more quickly and efficiently resolve the issue without costly and time-consuming deskside visits. This enables clinicians to more quickly resume use of their PC, while improving the productivity and reducing the cost of the IT support.

## Six Steps to Improve Healthcare Security and Privacy

Avoiding security incidents such as breaches requires a proactive, preventive, and forward-looking approach, so that security and privacy policy, risk assessments, and countermeasures are in place by the time a threat arrives. Building your organization's security and privacy capabilities is an incremental, iterative, and ongoing process. Start now with the following steps:

1. Build your healthcare organization's security and privacy practice upon the industry-standard top-down approach.
2. Establish and build out your security and privacy policy, incorporating applicable regulations, privacy principles, standards, and business needs in terms of data classification, usage models, and data processing needs. Address the requirements to maintain security and privacy as you collect, use, retain, disclose, and dispose of data.
3. Implement a security and privacy risk-assessment based approach to help you develop a well targeted and measured approach that makes the most of your limited security and privacy budget and maximizes the reduction of business risk.
4. Mitigate the risk of breaches and other security incidents with a robust, multi-layered, defense-in-depth approach that addresses the full threat lifecycle.
5. Use Intel hardware-assisted security technologies to improve the robustness and performance of your technical security control solutions.
6. Maximize the value of your security controls through a holistic implementation approach ensuring hardware, software, and service layers of the security control solution are compatible and work in harmony to mitigate the maximum business risk.

Intel® Core™ vPro™ processor-based PCs can be securely reached and patched by a remote central administrator over a wired or wireless network, even when the PC is powered off.

## Move Forward

Talk to your Intel representative, or visit Intel's Healthcare IT web sites:

**www.intel.com/healthcare**
**premierit.intel.com/healthcare**

Learn more about Intel security technologies. Visit:

**www.intel.com/technology/anti-theft**

**www.intel.com/technology/dataprotection**

**www.intel.com/technology/identityprotectiontechnology**

**www.intel.com/technology/malwarereduction**

**www.intel.com/technology/virtualization/technology.htm**

**www.intel.com/technology/vpro/**

[1] http://www.iso.org

[2] http://www.aicpa.org

[3] http://www.oecd.org

[4] http://eur-lex.europa.eu

[5] AES-NI is a set of instructions that consolidates mathematical operations used in the Advanced Encryption Standard (AES) algorithm. Enabling 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 Intel® Core™ i5-600 Desktop Processor Series, Intel® Core™ i7-600 Mobile Processor Series, and Intel® Core™ i5-500 Mobile Processor Series. For further availability of AES-NI enabled processors or systems, check with your reseller or system manufacturer. For more information, see http://softwarecommunity.intel.com/isn/downloads/intelavx/AES-Instructions-Set_WP.pdf.

[6] No computer system can provide absolute security under all conditions. Intel® Anti-Theft Technology (Intel® AT) requires the computer system to have an Intel AT-enabled chipset, BIOS, firmware release, software, and an Intel AT-capable service provider/ISV application and service subscription. The detection (triggers), response (actions), and recovery mechanisms only work after the Intel AT functionality has been activated and configured. Certain functionality may not be offered by some ISVs or service providers and may not be available in all countries. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof.

[7] No computer system can provide absolute security under all conditions. Intel IPT requires an enabled chipset, BIOS, firmware and software and a web site that uses an Intel® IPT Service Provider's Intel IPT solution. Consult your system manufacturer and Service Provider for availability and functionality. Intel assumes no liability for lost or stolen data and/or or any other damages resulting thereof.

[8] Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain computer system software enabled for it. Functionality, performance, or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

[9] No computer system can provide absolute security under all conditions. Intel Trusted Execution Technology (TXT) is a security technology that requires for operation a computer system with Intel® Virtualization Technology, an Intel Trusted Execution Technology-enabled Intel processor, chipset, BIOS, Authenticated Code Modules, and an Intel or other Intel® Trusted Execution Technology compatible measured virtual machine monitor. In addition, Intel Trusted Execution Technology requires the system to contain a TPM v1.2 as defined by the Trusted Computing Group and specific software for some uses. See http://www.intel.com/ for more information.

[10] Download the whitepaper, Breakthrough AES Performance with Intel AES New Instructions, at http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/

[11] FIPS Publication 197, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[12] Intel® vPro™ technology includes powerful Intel® Active Management Technology (Intel® AMT). Intel AMT requires the computer system to have an Intel® AMT-enabled chipset, network hardware, and software, as well as connection with a power source and a corporate network. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications or implementation of new business processes. With regard to laptops, Intel AMT may not be available or certain capabilities may be limited over a host OS-based virtual private network or when connecting wirelessly, on battery power, sleeping, hibernating, or powered off. For more information, see http://www.intel.com/technology/platform-technology/intel-amt/.



Printed in USA 0411/DH/HBD/PDF Please Recycle 325318-001US