SOLUTION BRIEF
Hardware-based Security Solutions
Healthcare Information Security

Healthcare Information at Risk – Encryption is Not a Panacea

David Houlding, MSc, CISSP, CIPP
Healthcare Privacy and Security Lead Architect
Healthcare IT Program Office
Intel Corporation

Healthcare Information and Breaches

Moving to electronic patient records will greatly contribute to improving the quality and reducing the cost of patient care. However the frequency of breaches has reached a level that threatens to impede or derail this migration.

No organization is immune to breaches. According to the U.S. Department of Health and Human Services, breaches are occurring every 4 to 5 days to all types and sizes of healthcare organizations, from private practices to hospitals, and across all geographical areas.[1] Types of electronic health record breaches range from loss or theft of electronic devices and improper device disposal, to unauthorized access and the use of unsecured e-mail with sensitive information. Such breaches can be prevented by using encryption together with other security measures to ensure that the data remains encrypted to all but those authorized to access it.

When considering healthcare information breaches it is common to take an organization-centric view. However breaches can lead to real harm to patients, including severe financial damages as well as psychological stress. These consequences and their effects should be included when evaluating the overall impacts of a breach, driven by the healthcare organization's goals and principles to improve the quality of patient care and "do no harm."

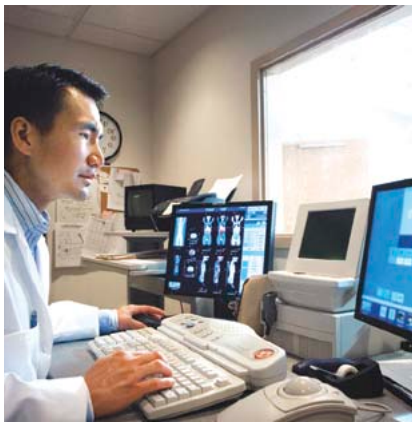
This document discusses encryption, presenting its key role as a safeguard of sensitive information, while also recognizing its vulnerabilities and the residual risk after encryption to healthcare organizations. We'll share a practical, multilayered approach that can help healthcare organizations achieve a more robust privacy and security practice. This approach uses encryption along with other administrative, physical, and technical controls to mitigate the risk of security incidents such as breaches and to better protect the confidentiality, integrity, and availability of sensitive information. We'll also discuss the importance of system performance for increasing user compliance, and we'll describe several hardware-accelerated security technologies from Intel that improve security while maintaining performance.

Healthcare Trends and the Impact of Security Breaches

In managing security and privacy risks, it's important to consider both the probability of security breaches as well as the business impact. Several growing trends are driving the increased probability of security breaches in healthcare organizations, such as:

- **Caregiver mobility.** Increasing caregiver mobility results in higher risk exposure, including loss or theft of sensitive information, the use of unsecured wireless systems for network access, and unauthorized access to data. Storing sensitive data on mobile client devices also expands the number of duplicate copies, further increasing risk of privacy and security breaches.

Healthcare Information at Risk – Encryption is Not a Panacea



The current business impact of healthcare organization privacy and security breaches in 2010 averaged over $7M U.S. dollars (USD) per breach event—about $214 per patient record breached.

- **Consumerization of IT.** More employee-owned devices are being used in healthcare organizations, and these devices often lack security controls such as encryption and enterprise manageability features for inventory, patching, and remediation to recover them from malware infections. With malware targeted for mobile devices growing rapidly, personal mobile devices are at risk of malware infection from personal applications, social media, web browsing, and e-mail. For example, Google Android malware grew 400% from June 2010 to January 2011, and 61% of detected malware infections came from spyware.[2] This presents a direct threat to the confidentiality of sensitive healthcare data either stored on or accessed using mobile devices. Since these devices are typically configured for personal use, including unsecured e-mail, this adds further risk of accidental breaches of sensitive information e-mailed from a personal device without encryption.
- **Cloud Computing.** Many healthcare organizations still take a perimeter-based approach to security, with firewalls and buildings providing logical and physical security perimeters. Accessing healthcare applications and sensitive data from cloud providers' data centers breaks this perimeter approach and places part of the responsibility for privacy and security upon the cloud providers. This adds new privacy and security risks and possible regulatory impact risks because healthcare organizations lack direct control over privacy and security of their sensitive data in the cloud and struggle to ensure confidentiality, integrity, and availability in a shared, virtualized environment.

The current business impact of privacy and security breaches can be devastating for healthcare organizations, averaging over $7M U.S. dollars (USD) per breach event in 2010 according to the *Ponemon Institute 2010 Annual Study on the U.S. Cost of a Data Breach*[3]. This breaks down to an average $214 per patient record breached. The largest component of this cost, Loss of Business at 63%, is precipitated by breach notification, now required by laws and regulations at the national level, such as the HITECH Act in the U.S., and at the state level, for example California SB 1386. The Ponemon Institute study shows that these costs are consistently trending upward, and similar trends are evident in other nations around the world. Many other nations either already have or are planning to implement similar breach notification laws and regulations.

Breaches are Changing Healthcare Organizations

The traditional approach to security is reactive: paying scant attention to privacy and security, waiting for a breach to occur, and then reacting to it with the application of a "silver bullet" technical security control. Unfortunately, the impact of even a single breach can be so damaging that a reactive approach is simply not an option for healthcare organizations. The magnitude of the impact of breaches is raising security out of the IT silo into a much broader concern with direct involvement from senior management and spanning departments across the organization, including finance, legal, privacy, human resources, operations, public relations, IT, and security. The threat of breaches is increasingly motivating healthcare organizations to take a more proactive, preventative approach to avoid breaches.

Is Encryption Alone Enough Protection?

While encryption is essential, there is also risk of relying too much on encryption alone for privacy and security. Regulations for notifying affected individuals when a breach occurs are typically the paramount privacy and security concern in healthcare organizations. For example, the HITECH Act Breach Notification Rule[4] states that loss, theft, or unauthorized access of sensitive information in the U.S. is not considered a breach if the information is unusable, unreadable, or indecipherable to unauthorized individuals.

Encryption is recognized as a technique that renders sensitive information unusable, which then ensures no unauthorized access and ensures a non-breach event under the HITECH Act. This may lead to a false sense of security in the organization with encryption-only safeguards in place.

Like most security controls, encryption has vulnerabilities. As long as a reasonably secure encryption cipher or algorithm is used, such as the Advanced Encryption Standard (AES), these vulnerabilities are typically not from technical weaknesses in the encryption cipher. Vulnerabilities with encryption are most often due to issues with implementation, both by management and users, including:

- **Inactive encryption.** Users may not activate encryption due to performance or other concerns. This risk is especially applicable to full disk encryption where activation can significantly slow down the performance of the PC or mobile device, degrading usability of applications and compromising the productivity of the caregiver. Performance impact with encryption is typically most significant in endpoint devices with limited compute power, such as smartphones and tablets, which are increasingly used within healthcare organizations to access healthcare applications and sensitive data.
- **Poor password management.** Users may choose weak passwords they can easily remember, delay changing passwords, share passwords, or use the same password they have used in an online service that may have been breached. This enables an attacker to easily guess or acquire the encryption password from another less-secure source. Recognizing password risks, healthcare organizations have increased password sophistication and cycling frequency rules. However, this often results in users forgetting passwords and burdening the IT Support Desk for help, or worse, writing their passwords down and storing them in close proximity to encrypted devices used to access healthcare applications and sensitive information.
- **Remaining logged in.** Users may not log out from healthcare applications, or may put devices on standby where encryption pre-boot authentication is not required, thereby increasing the risk of unauthorized access to sensitive information. This risk is especially prevalent with mobile devices used in unsecured public settings. Even thin clients without any sensitive data stored locally on the client are vulnerable to unauthorized access and breach with this type of risk.
- **Malware.** Malware in the form of key loggers already residing on endpoint devices can capture encryption passwords, regardless of password length or complexity.
- **Weak link.** Encryption is only as strong as the weakest link. If even a single repository or flow of sensitive data within a healthcare organization remains unencrypted, this creates a weak link, subjecting sensitive information to risk of breach. Unfortunately many breaches involve late discovery of undocumented, and therefore unprotected, repositories or flows of sensitive data. For example, a weak link in the flow of data is created when healthcare personnel create process workarounds by extracting sensitive data from a secure, encrypted database and entering it into spreadsheets stored on their unsecure, unencrypted devices. When securing sensitive data, healthcare organizations need to consider all stages in the lifecycle of the data through collection, use, disclosure, retention, and disposal.
- **Device loss or theft.** In the event of loss or theft of a device, the organization loses control of the device and the data stored on it. Not only is it critical that encryption is in place on the device, but enforceable policies with audit and compliance controls must be in place to satisfy the requirement that it can be proven that encryption was active on that specific device.
- **Rogue employees.** Previously trusted employees, perhaps terminated under undesirable circumstances, may be prone to retaliation and yet still have access to sensitive data. This risk is especially true of users working remotely from the healthcare organization offices and using endpoint devices that can store sensitive data.

Clearly it is not sufficient for a healthcare organization simply to require encryption in their privacy and security policy and make the encryption technology available. Even with encryption in place, these vulnerabilities add up to significant residual risk that is

Encryption Vulnerabilities

- **Inactive encryption.** Users may deactivate encryption due to performance concerns.
- **Poor password management.** Users may choose weak passwords, delay changing passwords, share passwords, or use the same password that they are using elsewhere.
- **Remaining logged in.** Users may not log out from secure applications.
- **Malware.** Key loggers may capture encryption passwords.
- **Weak link.** Security depends on protection across all repositories and flows of sensitive data.
- **Device loss or theft.** In the event of loss or theft of a device, the organization loses control of the device and the data stored on it.
- **Rogue employees.** Undesirable actions from previously trusted employees.

Vulnerabilities with encryption are most often due to issues with implementation, both by management and users.

Figure 1. Qualitative Risk Assessment Prioritization Matrix

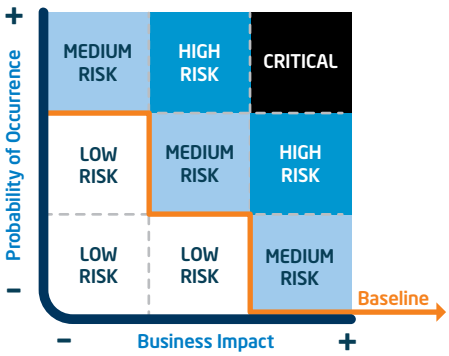


Figure 2. Protecting the Confidentiality of Sensitive Healthcare Information

intolerable for organizations needing a high level of assurance that sensitive data is secure. Further, mitigation of the residual risk requires a holistic, multi-layered approach in which encryption is a key security control that works together with other administrative, physical, and technical controls.

Risk Assessment and Identifying Controls to Mitigate Risks

A best known method to identify privacy and security controls for mitigating risks uses a top-down approach.[5] In this approach, the privacy and security policy for the organization is influenced by applicable regulations, privacy principles, and standards coupled with business needs—such as the inventory, classification, and the use cases for sensitive data. The resulting policy is reviewed and approved by senior management. Once established, the policy provides the foundation of the privacy and security practice in the healthcare organization.

Risk assessments are a key part of any approach to privacy and security and are increasingly required by regulations, such as HIPAA and the HITECH Act Meaningful Use Core Objective, to protect electronic health information. Performing risk assessments can deliver much more value than simply checking off a regulatory requirement. They provide a practical and valuable tool that enables a healthcare organization to allocate limited available budget in a way that reduces the most business risk and has the most positive impact to the organization's privacy and security posture. Risk assessments also provide a measured approach to privacy and security by indicating the threshold, or baseline, of acceptable risk. This enables the organization to determine when risks have been sufficiently mitigated and if remaining residual risks are at an acceptable level.

A best practice for risk assessments is to keep them as simple as possible. There are two fundamentally different types of risk assessments:

- **Quantitative risk assessments** assign monetary values to business impacts. This task can be difficult and time consuming in practice. For example, how does one quantify, in monetary terms, the damage to the reputation of a healthcare organization resulting from a breach?
- **Qualitative risk assessments** are suitable for most healthcare organizations. This simpler alternative prioritizes risks based on low, medium, and high assignments to business impacts and probabilities of occurrence. It then assigns to each risk an overall priority value from low to critical (see Figure 1).

Qualitative risk assessments involve using a prioritization matrix based on the risk probabilities of occurrence and business impacts, then applying mitigation controls starting with the critical-impact risks and finishing with those with medium impacts. This enables an organization to allocate the limited budget available for privacy and security in a way that reduces the most risk.

As shown in the qualitative risk assessment prioritization matrix in Figure 1, the risk baseline indicates a policy that all medium, high, and critical priority risks shall be mitigated to low. In practice this means that security controls are applied to mitigate a given risk until the residual risk is low. When the residual risk is low, the healthcare organization is done mitigating that risk and can then apply its remaining resources allocated to privacy and security to mitigate other risks. Without a measured approach like this, there is risk of over-securing in some areas and under-securing in others, which can result in a weak link or vulnerability that can lead to security incidents such as breaches.

Without a risk assessment and baselines of acceptable risk that enable a measured approach, privacy and security risks may create a budgetary black hole for the healthcare organization.

An example of this top-down approach for mitigating risks is shown Figure 2. The HIPAA healthcare regulation influenced the addition of a data-protection rule to the healthcare organization's security and privacy policy. This led to identifying the loss or theft of a laptop as a risk, as it would jeopardize the confidentiality of the data. The probability of loss or theft of a laptop

containing unprotected patient records may be assessed as high, especially for a healthcare organization with many mobile caregivers. Similarly, the business impact may be assessed as high, especially where each laptop stores many patient records, rather than only the records the caregivers need for the patients they will visit on a given day.

In the qualitative risk assessment prioritization matrix shown in Figure 1, we see that this puts the overall priority of this risk as critical, requiring mitigation. A key mitigation for this risk is full disk encryption (FDE), and implementing this in a way that maintains adequate performance requires the use of hardware-accelerated encryption. However, due to vulnerabilities of encryption, FDE alone is likely insufficient to adequately mitigate this risk. Further administrative, physical, or technical controls must be applied to mitigate this to a low residual risk and assure the healthcare organization and its patients that their data is safe.

Robust Security with a Multi-Layered, Defense-in-Depth Approach

A defense-in-depth security strategy places multiple layers of controls in place which work together to mitigate risk. Table 1 shows the technical, administrative, and physical controls that provide robust defense-in-depth security to mitigate the risk of breach of sensitive data.

Controls are applied singly or in combination to mitigate risk:

Multiple technical controls. Secure wipe or "poison pill" technology such as Intel® Anti-theft technology may be applied as an additional layer of security to work in conjunction with encryption to mitigate residual risk. In this control, a command is sent to a mobile device when it is reported as lost or stolen, resulting in lockdown or securely wiping the mobile device in order to protect the sensitive data on it.

Administrative and technical controls. Risk assessments include the probability of a risk as well as its business impact. The business impact to the healthcare organization is proportional to the number of patient records with sensitive information that are compromised. For example, there is a big difference in terms of business impact between a breach of 10 patient records a caregiver accesses on a given day, versus 10,000 records for all the patients of the healthcare organization. An effective data minimization policy that reduces the scope of sensitive data at risk is a great example of an administrative control that works together with the encryption technical control to protect the confidentiality of the patient records. With data minimization, the mobile caregiver only has the minimal set of patient records stored on their mobile device that are needed for the patients that will be seen that day, and the confidentiality of the limited sensitive data at risk on the mobile device is protected with encryption.

Technical and physical controls. If encryption fails due to intentional deactivation or another one of the issues discussed previously, physical controls that ensure secure storage, use, and transport of the laptop containing the sensitive data provide additional layers that allow the healthcare organization to avoid security incidents such as breaches.

Increased Backend Server Security Needs

Mass migration to electronic health records driven by meaningful use regulations, new types of higher resolution imagery and video, and genomics is causing a growing surge of sensitive data on the servers of healthcare organizations. This challenge is further compounded by migration to thin client compute models such as Virtual Desktop Interface (VDI) that move the sensitive data and processing off the client and onto the backend servers. This trend is being accelerated by the consumerization of IT where healthcare workers access healthcare applications and sensitive data from their personal mobile devices which are typically not adequately secure. In many cases, these devices are viewed as unmanageable by the healthcare organization, causing it to mitigate risk by moving healthcare applications and sensitive information onto more manageable and secure backend servers, and enabling only thin client access from personal mobile devices.

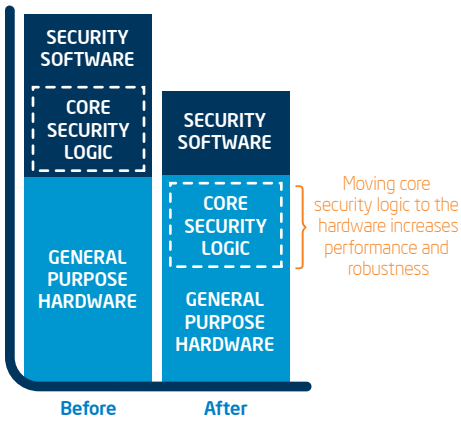
Table 1.
Technical, Administrative, and Physical Controls for Risk Mitigation

Technical Controls
▪ Encryption
▪ Secure Wipe or "Poison Pill" technology
Administrative Controls
▪ Policy, Procedures, Standards, Baselines, Guidelines
– Data minimization
– Protect sensitive data at rest, in use, and in transit throughout entire lifecycle
– Good key management
▪ Security Awareness Training
▪ Auditing and Compliance Enforcement
Physical Controls
▪ Secure storage, use, transport and disposal of sensitive data

Although more and more sensitive data is on the servers, many healthcare organizations have inadequately secured their backend servers.

If users perceive that security controls such as encryption slow them down, they may be motivated to avoid or disable these controls.

Figure 3. Trend toward Hardware-Enabled Security For Increased Performance and Robustness



Healthcare organizations typically prioritize the application of encryption to the repositories most at risk of loss or theft, such as those on mobile devices. However, encryption should be done on all repositories and flows of sensitive data, including those on servers. Although more and more sensitive data is on the servers, many healthcare organizations have given a disproportionate amount of attention to securing client devices and have inadequately secured their backend servers. While client devices are at higher risk of loss or theft than servers, loss or theft of a server can result in a much larger business impact since the magnitude of the business impact is proportional to the number of patient records breached.

Recent high-profile breaches involving the loss or theft of servers, such as the Health Net breach of March 2011[6], have shown that this presents a real risk to healthcare organizations. Mitigation of risks associated with breaches involving the loss or theft of servers requires robust security on backend servers with multiple controls including encryption. Maintaining good performance on these growing server repositories of sensitive data is increasingly a challenge that demands high performance technical security controls.

Performance Impacts Security Compliance

Performance is critical when considering technical security controls. Performance is much more than a "nice to have" in the sense that if users perceive that security controls such as encryption slow them down, they may be motivated to avoid or disable these controls. This is especially the case for users of mobile devices, which typically have less compute power than PCs, resulting in a higher performance impact by encryption or other technical controls. This presents compliance issues for healthcare organizations and can greatly increase the risk of breaches and other security incidents. This performance challenge is acute both on the client side for devices with limited compute power, and on backend servers struggling with the increased volume of sensitive data.

Hardware-enabled Security for Higher Performance and Robustness

To counter the growing sophistication of threats and meet future demands for high performance, healthcare organizations can benefit from hardware-enabled security. As shown in Figure 3, hardware-enabled security provides new instructions in silicon that both accelerate the security control and improve robustness by dropping the core processing to the hardware layer where it is less vulnerable, for example, to side channel attacks that can be a weakness of software-only encryption solutions.

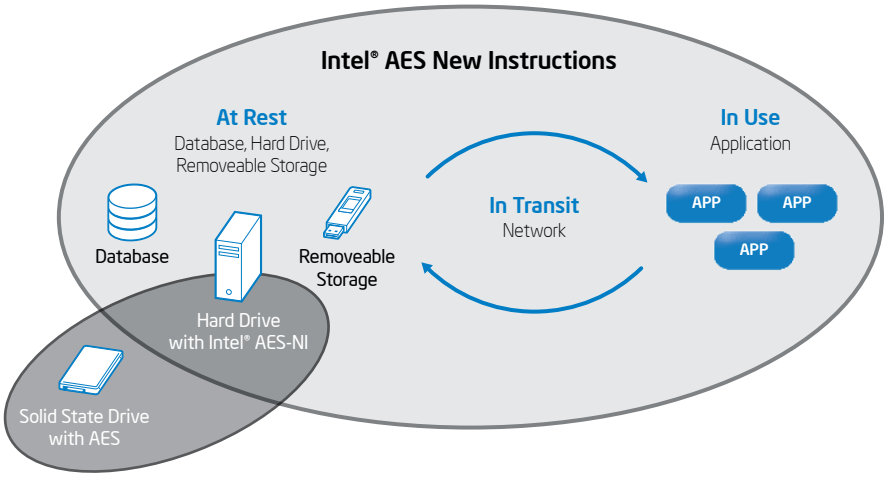
Hardware-enabled security technologies provided by Intel enable more robust, higher performance technical security controls. These technologies, such as Intel® Advanced Encryption Standard – New Instructions (Intel® AES-NI) and solid state drives (SSDs) with AES, maximize the use of standards such as AES and provide open platforms that the security software ecosystem can use for innovative new technical security controls.

AES-NI is particularly well suited to protecting the confidentiality of data at all stages including at rest, in transit, and in use. A wide and growing range of mission critical software applications make use of Intel AES-NI, as can be seen from the AES-NI ecosystem[7]. For example, Oracle was able to deliver a 10x performance improvement in Transparent Data Encryption in Oracle* Database 11g R2 by using Intel AES-NI in an Intel® Xeon® 5600 series processor-based system[8].

The Intel® Solid State Drive 320 Series is a series of SSDs that include AES 128 encryption to protect the confidentiality of all data stored, or at rest, on the drives. Since all data stored on the SSDs is encrypted, it is not up to the user's discretion what constitutes sensitive data, mitigating risk of unencrypted sensitive data missed by a user.

As shown in Figure 4, Intel AES-NI helps with encryption in three contexts: when the data is used by a running application, when data is in transit, and when the data is at rest. Intel® Solid State Drive 320 Series helps with encryption of data at rest on a hard drive.

Figure 4. Protecting Confidentiality of Sensitive Information with Intel AES-NI and SSDs with AES



Beyond Security: Availability and Integrity

Intel's approach to security is that it is committed to protecting not only the confidentiality, but also the integrity and availability of sensitive healthcare data. Availability, or timely and reliable access, is particularly important as electronic health records become mission critical; inaccessibility of this information at a critical moment can adversely and severely impact the health of the patient.

Intel SSDs improve availability of healthcare applications. Because they have no moving parts, SSDs are more rugged than traditional storage devices, and they consume less power which enables longer battery life, extending access to healthcare applications and data from the mobile devices that are increasingly used by caregivers.

Data integrity–or ensuring sensitive healthcare information is accurate, complete, and up to date–is critical as healthcare organizations make evidence-based medical decisions using this sensitive information. Intel SSDs include measures to avoid corruption and protect the integrity of information stored on them in the event of a power loss.

Intel 22nm 3-D Tri-Gate Transistor Technology[9] will significantly increase performance and reduce the power consumption of future processors. Future processors will continue to include hardware-enabled security features, allowing powerful performance and robust technical security controls to provide the increased security needed by healthcare organizations to avoid breaches. They will enable mobile clients with limited compute power to run technical security controls, while leaving ample compute power on the clients to ensure good performance and usability of healthcare applications. These technologies also enable the use of strong security controls including encryption on servers in the cloud while maintaining expected performance, even under the building surge of sensitive data.

Healthcare Privacy and Security Checklist

Ensuring the privacy and security of sensitive healthcare information is a journey, not a destination. The threat landscape is constantly evolving and healthcare organizations must continually re-evaluate trends, associated risks, and the privacy and security controls needed to mitigate them. Healthcare organizations that follow this practice will adapt to a changing threat landscape with robust privacy and security and minimal risk, while those that don't will face the crippling consequences of security incidents such as breaches. Use the following checklist to strengthen and evolve your privacy and security practices:

Healthcare Privacy and Security Checklist

- ❑ **Build a privacy and security practice** using the industry standard proactive, preventative, holistic, and top-down approach.
- ❑ **Regularly evaluate** privacy and security policy, procedures, baselines, and guidelines in order to ensure they are up-to-date, comprehensive and accurate.
- ❑ **Conduct risk assessments** regularly and at key milestones. Recognize risk assessments as not just a regulatory requirement but also a practical tool and best practice, and infuse this rationale into the culture of the healthcare organization.
- ❑ **Implement privacy and security controls** identified in your risk assessments to mitigate risk within acceptable baselines. Be aware of dependencies between service, software, and hardware layers when implementing technical security control solutions.
- ❑ **Continually monitor and evaluate** the effectiveness of your privacy and security controls and practice, and make changes as needed to ensure risks are adequately mitigated.
- ❑ **Conduct privacy and security awareness training** regularly to improve compliance and mitigate risks associated with accidents and social engineering.

Healthcare Information at Risk – Encryption is Not a Panacea

1. **Build a privacy and security practice** using the industry standard proactive, preventative, holistic, and top-down approach.
2. **Regularly evaluate** privacy and security policy, procedures, baselines, and guidelines in order to ensure they are up-to-date, comprehensive, and accurate, including:
   - Regulations impacting the organization, based on the countries, states, provinces, and territories in which the healthcare organization does business.
   - Privacy principles recognized by the organization's customer base.
   - Relevant standards such as ISO 27001/2 for Information Security Management Systems and Techniques.
   - Thorough inventory and classification of sensitive information repositories and workflows using a dual top-down and bottom-up approach. Use documentation and data loss prevention (DLP) to detect all sensitive data at rest and in transit, and then classify and secure accordingly with safeguards including encryption.
   - Account for all usage models of sensitive data, including new use cases associated with mobile computing, health information exchange, care coordination, social media, cloud computing, and consumerization of IT. Include all stages in the lifecycle of sensitive information from collection, use, and retention, to disclosure and disposal.
3. **Conduct risk assessments** regularly and at key milestones. Recognize risk assessments as not just a regulatory requirement but also a practical tool and best practice, and infuse this rationale into the culture of the healthcare organization.
   - Use a qualitative risk assessment prioritization matrix to take both a prioritized and measured approach to allocating limited budget to reduce the most business risk, and know when the job is done.
   - Keep risk assessments simple, using qualitative risk assessments wherever possible.
   - Use a holistic, multi-layered, and defense-in-depth approach to identify privacy and security controls required to mitigate risks, including administrative, physical, and technical controls working together to deliver robust security.
   - When identifying security controls to mitigate risk, be aware of the importance of performance for user experience and compliance, and the need for more robust technical security controls required to counter the rising sophistication of threats.
   - Use hardware-enabled security technologies from Intel to mitigate risk with high performance and more robust technical security control solutions.
4. **Implement privacy and security controls** identified in your risk assessments to mitigate risk within acceptable baselines. Be aware of dependencies between service, software, and hardware layers when implementing technical security control solutions.
5. **Continually monitor and evaluate** the effectiveness of your privacy and security controls and practice, and make changes as needed to ensure risks are adequately mitigated.
6. **Conduct privacy and security awareness training** regularly to improve compliance and mitigate risks associated with accidents and social engineering.

Summary

Privacy and security breaches occur with alarming frequency and represent a significant cost to healthcare organizations and risk of harm to patients in the U.S. and around the world. With today's rapid changes in how healthcare workers interact with patient data, it is critical that robust privacy and security controls are present to prevent breaches, and that compliance is enforced. Robust hardware-enabled security such as that provided by Intel AES-NI and Intel SSDs helps reduce the risk of breaches without significantly impacting system performance.

Learn more about Intel security technologies. Visit:

- **www.intel.com/technology/anti-theft**
- **www.intel.com/technology/dataprotection**
- **www.intel.com/design/flash/nand/320series/overview.htm**

[1] U.S. Department of Health and Human Services, "Breaches Affecting 500 or More Individuals," http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html
[2] Juniper Networks Malicious Mobile Threats Report 2010/2011, http://www.juniper.net/us/en/local/pdf/whitepapers/2000415-en.pdf
[3] http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf
[4] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html
[5] "Healthcare Information at Risk: Successful Strategies for Healthcare Security and Privacy," Intel Corporation, April 2011. http://premierit.intel.com/servlet/JiveServlet/download/6242-1-6046/Successful%20Strategies%20for%20Healthcare%20Security_Privacy.pdf
[6] http://www.dmhc.ca.gov/library/reports/news/pr031411.pdf
[7] http://www.intel.com/technology/security/downloads/AES-NI_ecosystem.pdf
[8] http://www.oracle.com/us/corporate/press/173758
[9] http://newsroom.intel.com/docs/DOC-2032

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. For availability of AES-NI enabled processors or systems, check with your reseller or system manufacturer.

Printed in USA 0711/DHOU/KC/LP/250 Please Recycle 325343-001US