

# Healthcare Information at Risk: The Consumerization of Mobile Devices



## Converging Trends in Healthcare

The consumerization of mobile devices, also known as bring your own device (BYOD), is a major trend affecting healthcare. This involves healthcare workers using their personal mobile devices, such as smart phones and tablets, to access applications that enable them to deliver care whenever and wherever it is needed. Concurrent are the broader trends of increasing caregiver mobility and the use of cloud computing—whether in the form of electronic health record (EHR) software as a service (SaaS), an enterprise private cloud, or other healthcare cloud offerings.

## Delivering the Benefits of Consumerization and Cloud Computing

These trends deliver benefits that help improve quality and efficiency while reducing the cost of patient care. They also improve the user experience for healthcare workers and increase flexibility, productivity, and job satisfaction. Using their preferred personal mobile devices, healthcare workers can efficiently coordinate patient care when and where needed. For the healthcare organization, embracing consumerization can reduce costs and improve talent acquisition and retention. Cloud computing delivers improved agility and scalability while further reducing costs. For example, cloud computing in the form of managed EHR SaaS enables rapid

startup and seamless scalability, allowing healthcare organizations to focus on patient care rather than IT, avoid upfront server capital costs, and use a pay-as-you-go model, with seamless scalability in cloud computing capacity as business needs grow.

## Recognizing Security Risks

However, these trends also present significant new information privacy and security risks that must be addressed before healthcare organizations can safely embrace and benefit from them. Because mobile computing provides anytime, anywhere access to sensitive data, and cloud computing moves the sensitive data into the cloud, they blur traditional security perimeters—including buildings in the physical sense and firewalls and networks in the logical sense.

Cloud computing moves sensitive data out of the healthcare organization and into the data centers of cloud providers, which could be located in multiple regions around the world and subject to a variety of local regulations. Mobile devices increase the risks of loss and theft, unauthorized access, and use of unsecured wireless services. Personal mobile devices are less manageable than corporate devices, and healthcare organizations struggle with tasks such as conducting inventory, applying policy, verifying safeguards, patching, auditing, remediation, and secure data wipes. Unmanaged devices

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

# Healthcare Information at Risk: The Consumerization of Mobile Devices

**Table 1. Ponemon 2010 Study of Five Countries: Cost of a Data Breach**

<b>Country</b>	<b>Total Cost of a Data Breach in Millions of U.S. Dollars</b>
United States	6.75
Germany	3.44
United Kingdom	2.57
France	2.53
Australia	1.83

are less secure than corporate-provisioned devices. Personal devices compound this risk, as healthcare workers also use them for personal apps, social media, e-mail, and Web browsing activities that bring higher risk of malware infection and accidental security incidents (such as e-mailing sensitive data over an unsecured personal e-mail service).

Mobile apps for healthcare, developed by software suppliers with a well-established security development life cycle, carry a relatively low risk of exposing vulnerabilities. However personal apps, such as games, are often created by “two guys in a garage,” with scant attention to privacy and security. Personal apps often cost as little as USD 0.99, and app developers are increasingly motivated to make up for this low price by harvesting sensitive data, profiling end user behavior, and selling it for secondary purposes such as behavior profiling for advertising.<sup>1</sup> When these personal apps run on consumer mobile devices that healthcare workers also use to access healthcare services and sensitive data, the confidentiality, integrity, and availability of healthcare data is put at risk.

Healthcare workers’ top priority is delivering great patient care, but when security controls perceived as cumbersome get in the way, it is human nature to develop workarounds that circumvent or disable those controls. Innovations in mobile devices and apps provide many opportunities for this, including services ranging from unsecured personal e-mail and social media to file transfer services and even USB flash drives. These alternatives not only move sensitive data outside the control and security of the healthcare organization, but have also been associated with numerous high-profile security breaches. For these reasons, healthcare organizations need to embrace consumerization in a secure manner rather than take a hardline stance of saying “no” to healthcare workers.

## Avoiding the Cost of Breaches

Concurrent with these trends and associated risks, the business impact of security incidents has grown to a staggering level, as shown in Table 1, and is trending upward globally.

## Complying with Regulations and Breach Notification Rules

Regulations such as the HITECH Act<sup>2</sup> at the national level, as well as state-level regulations such as California SB 1386<sup>3</sup> increasingly include notification rules that compel disclosure of breaches. Healthcare organizations can incur significant losses, for example from lost business. Breach notification rules are increasingly incorporated into regulations at the national, state, province, or territory levels—in the United States and around the world.<sup>4</sup>

How can healthcare organizations embrace the consumerization of mobile devices and related trends when they introduce such significant privacy and security risks?

## Applying Best Practices for Information Security

Healthcare organizations increasingly take a preventative approach to avoid security incidents such as breaches and their potentially devastating impacts. This involves analyzing trends affecting the healthcare organization, identifying associated privacy and security risks, and mitigating those risks to an acceptable level by applying safeguards proactively before a security incident occurs. The foundation of the privacy and security practice in the healthcare organization is the policy. Policy must accurately and completely cover consumerization of mobile devices and related trends to provide a solid foundation on which to build a robust privacy and security practice. However, this is a significant task, given that these trends are so new and push the envelope on multiple fronts—including business, human resources, legal, and IT.

Regular risk assessments provide a practical tool and best practice for managing risks and evolving the privacy and security practices of the healthcare organization to track the rapidly changing threat landscape. With sensational security headlines in the news every day, healthcare organizations face a disparity between perceived and real risks. It is clear that there are deficiencies in healthcare privacy and security in general, but the nature of the deficiencies doesn't always align with news headlines. For example, insider threats are often underestimated. Risk assessments enable an objective, prioritized approach that guides the allocation of limited funds for privacy and security in a way that reduces the most business risk. They also provide a measured approach that avoids privacy and security becoming a budgetary black hole for healthcare organizations that are increasingly under pressure to reduce costs. Risk assessments are increasingly required by regulations and standards including ISO 27001/2 for Information Security Management Systems and Techniques. Focusing on the value of the healthcare data<sup>5</sup> and the threat agents driving risk<sup>6</sup> during the assessment process enables more consistent, objective prioritization of risks—focusing on real risks and avoiding hypothetical distractions. New tools such as

the Intel® Anti-Theft Laptop Risk Tool<sup>7</sup> help to quickly assess risk, cost, and the return on investment (ROI) associated with specific risks and safeguards.

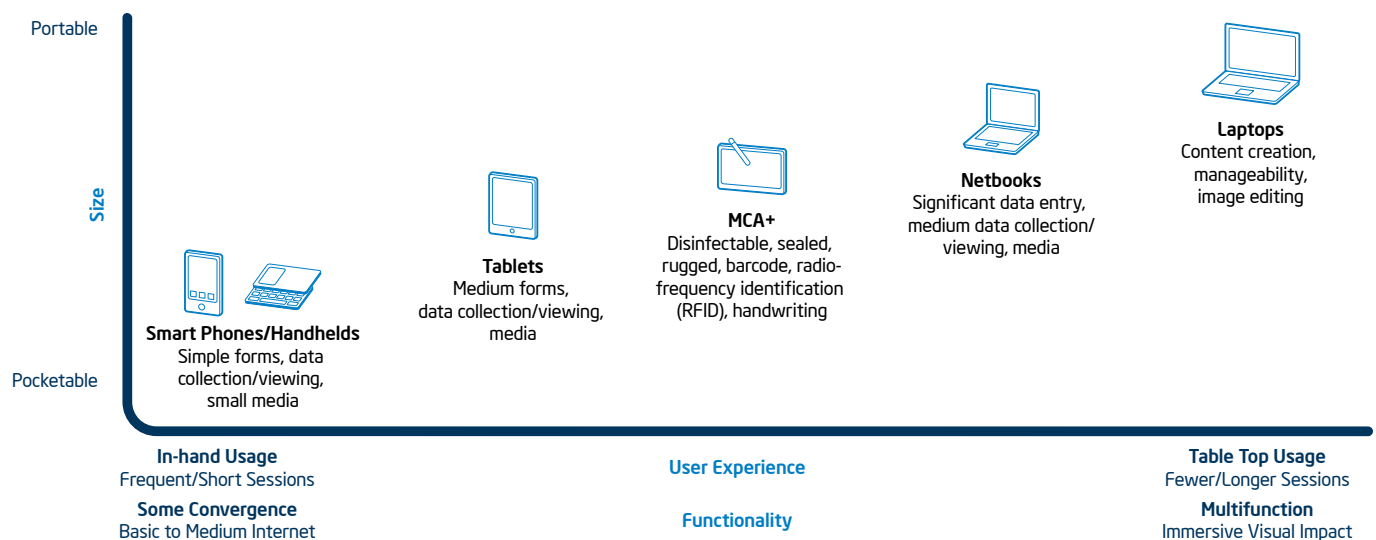
### Employing the Healthcare Compute Continuum to Improve Patient Care

The mobile client continuum, shown in Figure 1, includes a myriad of mobile devices—from smart phones to tablets and laptops—that healthcare workers use to access healthcare applications and sensitive data. Healthcare workers use different devices for different use cases, with some complex use cases involving multiple mobile devices. For example, a doctor may receive an alert about a patient emergency on a smart phone when outside the clinic, use a tablet to do rounds in the clinic, and consult with specialists in a video conference using a laptop. Successful selection of mobile devices requires attention to criteria such as consumption and creation of content, online and offline access, sanitization and ruggedization needs, software and peripherals availability, and so forth. Intel has defined a new category of mainstream thin and light mobile computers, called Ultrabook™, to play key role in the continuum of mobile devices, together with smart phones, tablets, netbooks, laptops and other connected devices that use Intel® Atom™ and Intel® Core™ processors.<sup>8</sup>

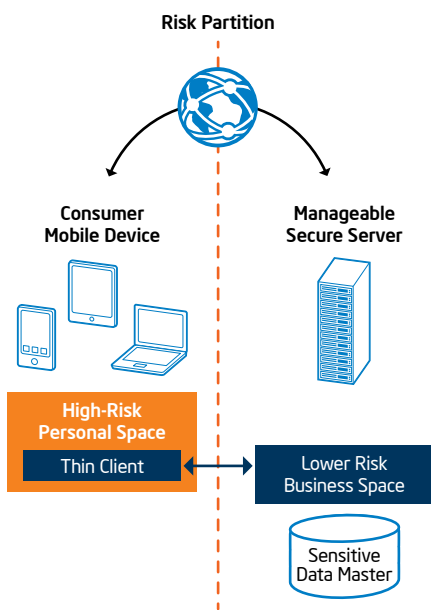


Healthcare workers' top priority is delivering great patient care, but when security controls perceived as cumbersome get in the way, it is human nature to develop workarounds that circumvent or disable those controls.

Figure 1. The Mobile Client Continuum.



# Healthcare Information at Risk: The Consumerization of Mobile Devices



**Figure 2.** Managing Risk with a Thin-client Compute Model.

The continuum of mobile devices offers multiple form factors, operating systems, and versions, and devices can be personally or organization-owned. This diversity is likely to increase in the future due to rapid change and a higher refresh rate in consumer devices, as well as increasingly smaller types of medical and healthcare devices proliferating at the lower end of the continuum. With the growth of care coordination and health information exchange, healthcare is becoming increasingly collaborative and will include new technologies such as multi-way video conferencing. Care coordination also promises to deliver increased patient engagement, and the diversity of mobile devices with which patients participate in their healthcare will only further increase the complexity of the client continuum that healthcare organizations must securely support.

## Using Compute Models to Manage Risk

Different use cases and workflows will use different compute models. For example, a powerful rich-client compute model enables local-client compute capabilities in rural care settings with limited or no network coverage. Rich clients in areas with good network coverage also improve the end user experience with performance-sensitive real-time collaboration tasks such as multi-way video conferencing. On the other hand, thin-client compute models may be used on consumer mobile devices where there is 100-percent network coverage, and enable “follow me sessions” while storing sensitive data on centrally managed and secured servers. A range of possible compute models has emerged between the extremes of rich- and thin-client, and they are discussed briefly below from a risk management standpoint.

When considering risk mitigation using compute models, healthcare organizations must be concerned with maintaining the confidentiality of sensitive information as well as with protecting the availability and integrity of sensitive information. Urgent patient care is critically dependent on availability, the timely and reliable access to electronic patient records. Similarly, evidence-based medicine is dependent on the integrity of electronic patient records, ensuring they are accurate, complete, and up to date, and a suitable basis upon which to make important decisions about patient care.

Thin-client compute models, such as terminal services or virtual desktop interface (VDI), partition relatively high-risk consumer mobile client devices from the healthcare applications and sensitive data that are stored on centrally managed and secured servers, as show in Figure 2. However, thin-client compute models are not a panacea and are not suitable for all use cases. Unsuitable use cases include instances when healthcare workers are delivering patient care in settings that don’t have reliable or performant network coverage, or are participating in a multi-way video conference, which requires performance-intensive real-time collaboration. Although many mobile device types, including smart phones and tablets, offer compelling usability features, using a mobile device with a small touchscreen to access applications designed for a large screen, keyboard, and mouse can be a major usability challenge for healthcare workers. Thin-client compute models can also bring significant network, storage, and server CPU build-out costs.

Reverse seamless technology<sup>9</sup> promises to deliver a key extension to VDI that enables healthcare workers to seamlessly run local

applications on mobile devices. This includes real-time, performance-sensitive applications such as video conferencing, or applications that use local peripherals attached to the mobile device. This extension enables local applications to utilize full client compute capabilities while minimizing server load and required build-out, delivering an improved user experience, and improving the availability of healthcare services.

Alternative compute models that provide increased availability of healthcare applications and sensitive data, even offline or outside of network coverage, use a risk partition on the client side, as shown in Figure 3. Examples of this type of compute model include application virtualization, virtual containers, or sandboxing technologies that each conceptually provide a manageable secure “compartment” for healthcare applications and sensitive data, including the ability to cache limited sensitive data on the consumer mobile device to enable local computing. Using this type of compute model, healthcare workers might sync the client with the EHR SaaS cloud and cache 10 records in a secure business space on the mobile device for the patients they will visit that day in a rural setting without network coverage. The healthcare organization can manage this business space, and it can be strongly secured with a multi-layered, defense-in-depth approach that includes technical controls such as encryption with Intel® Advanced Encryption Standard—New Instructions (Intel® AES-NI),<sup>10</sup> solid-state drives (SSDs) with Advanced Encryption Standard (AES),<sup>11</sup> and Intel® Anti-Theft Technology.<sup>12</sup> Intel® Virtualization Technology<sup>13</sup> and Intel® Trusted Execution Technology<sup>14</sup> enable faster and safer virtual containers, for example with Citrix XenClient XT<sup>15</sup>. Additional administrative and physical controls, such as a policy to minimize

the amount of sensitive information stored on the mobile device and secure use, transport, and storage of the device, help ensure robust privacy and security.

### Using HTML5

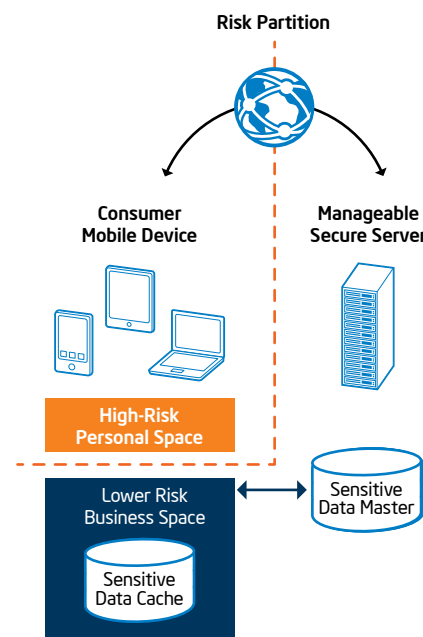
As the diversity of the compute continuum grows, the practicality of providing custom software apps for every mobile device type, version, and OS will diminish. New options such as HTML5, which enable write-once, run-anywhere across different types of mobile devices, whether online or offline, will grow.

### Providing Centralized Patching and Management

The need for timely patching is increasingly critical for healthcare organizations due to the rapid escalation of attacks based on newfound software vulnerabilities and the use of social media by threat agents. The compute models previously described provide centralized patching and management, which helps ensure timely and efficient patching, minimizes the risk of security incidents, and avoids patch fatigue for end users. The healthcare compute continuum also includes devices provisioned and managed by the healthcare organization. Intel® Active Management Technology, a feature of Intel® vPro™ technology,<sup>16</sup> enables secure remote power on/off, inventory, patching, and remediation.

### Preventing Unauthorized Access

Unauthorized access to sensitive healthcare information using mobile devices is a key risk exacerbated by mobile devices that are at increased risk of loss, theft, or unauthorized use. This risk is effectively mitigated with the application of strong, two-factor authentication. This includes a biometric “what you are”



**Figure 3. Managing Risk with a Client-side Risk Partition**

## Healthcare Information at Risk: The Consumerization of Mobile Devices

Ideally, technical security controls are invisible to healthcare workers and only become apparent when necessary.



factor, such as a fingerprint, or a “what you have” factor such as a hardware-based token. Physically separate two-factor authentication hardware tokens are increasingly associated with usability, support, and cost issues. Intel® Identity Protection Technology (Intel® IPT)<sup>17</sup> provides strong two-factor authentication without these issues, where the “what you have” is the Intel IPT-capable mobile device.

### Addressing the Use of Unsecured Wireless Networks

Use of unsecured wireless networks is another key risk associated with consumer mobile devices. This risk is bound to grow as mobile devices increasingly support Wi-Fi\* connectivity. Mitigating snooping and “man in the middle” (MITM) risks can be addressed with the use of a virtual private network (VPN) from the mobile device, together with controls to mitigate risk of malware attacks through the VPN from a potentially infected mobile device.

### Securing Data

Mobile computing provides anytime, anywhere access to sensitive data inside the security perimeter. Cloud computing moves sensitive data outside this perimeter and into data centers operated by cloud providers. Embracing these trends safely requires securing the sensitive data itself, whether at rest on a mobile client or server, or in transit. This requires a thorough data inventory with a dual top-down and bottom-up approach, including the use of documentation, interviews, and data loss prevention (DLP) safe-

guards. This is particularly important to catch the ad hoc repositories and flows of sensitive data—for example on a USB flash drive or unsecured spreadsheet—that emerge when healthcare workers are under constant pressure to reduce costs and save time. Healthcare data should be classified according to its sensitivity, with classification being a function of content, the number records, and the value of the data to both the healthcare organization and potential threat agents.<sup>18</sup> Security needs to be holistic, both in terms of technical controls to secure the complete continuum of mobile devices and servers, together with administrative and physical controls to safeguard the healthcare organization as a whole.

### Making Security Invisible

Security measures must serve the delivery of patient care. Ideally, technical security controls are invisible to healthcare workers and only become apparent when necessary. This eliminates the need for healthcare workers to circumvent or disable security controls—which improves compliance and minimizes risk to healthcare organizations. This requires high-performance technical security controls to preserve the user experience, even on mobile devices with limited compute power and for back-end servers that are increasingly challenged with a surge in sensitive data to protect. Digitization as a result of the move to EHRs, health information exchange and data proliferation, retention requirements, and new data types such as high-resolution digital pathology and genomics all accelerate this surge.

## Understanding the Human Factor

Ultimately, healthcare workers can be the “weakest link” in the privacy and security practice of a healthcare organization. They are vulnerable to accidents, spear phishing attacks, and so forth. A robust security strategy combines maximally invisible security controls with regular and current security awareness training to help healthcare workers understand the rationale for safeguards, why the controls are needed to protect patients and the healthcare organization, and their roles and responsibilities. Strong audit and compliance controls are also needed to help compliance with privacy and security policy.

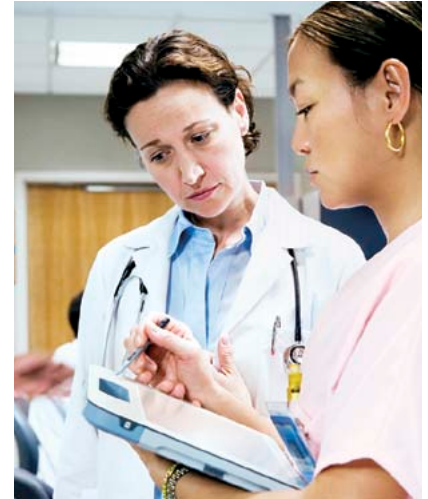
## Deploying a Detect and Respond Capability

A proactive, preventative approach will stop most security incidents but, in practice, not all. A good detect and respond capability is also required for robust privacy and security. Safeguards such as DLP can detect vulnerabilities such as unsecured sensitive data and respond by initiating cleanup or encryption of that data, while intrusion detection and prevention systems (IDPS) and security incident and event management (SIEM) can detect, prevent, and manage any security incidents and events.

## The Role of Hardware-assisted Security

While mobile devices increasingly support remote locate, lock, and wipe capabilities, and these safeguards provide a good starting point for securing the device, alone these capabilities are not sufficient. These controls have low computational demands and have achieved

higher use across mobile devices with limited compute power. For healthcare organizations to safely embrace mobile devices, and especially higher risk consumer mobile devices, additional strong security controls such as encryption, anti-malware, IDPS, DLP and mobile device management (MDM) are increasingly required. However, these controls have a higher computational cost and risk grinding mobile devices to a halt. Intel® hardware-assisted security technologies, such as Intel AES-NI, accelerate the performance of technical security controls, preserve healthcare workers’ user experience, remove the need to disable or circumvent safeguards, enable good compliance, and minimize risk to healthcare organizations. Intel® 22nm 3-D Tri-Gate Transistor Technology<sup>19</sup> will significantly increase the performance and reduce the power consumption of future processors that include hardware-assisted security technologies. This will pave the way for stronger security controls on both mobile devices and servers. Hardware-assisted security technologies also improve the robustness of technical security controls—Intel AES-NI, for example, executes core security logic at the hardware layer, where it is less vulnerable to side channel attacks. Hardware-assisted security also enables advanced security capabilities such as McAfee DeepSAFE\*<sup>20</sup> that may be used to detect, block, and remove increasingly sophisticated malware below the operating system, such as kernel mode rootkits used in advanced persistent threats (APTs). Intel hardware-assisted security technologies maximize use of standards, such as the AES in Intel AES-NI, and provide open, standards-based platforms on which security software suppliers can innovate strong technical security controls.



A robust security strategy combines maximally invisible security controls with regular and current security awareness training to help healthcare workers understand the rationale for safeguards, why the controls are needed to protect patients and the healthcare organization, and their roles and responsibilities.

# Healthcare Information at Risk: The Consumerization of Mobile Devices

## Conclusion

The consumerization of mobile devices and the related trends of mobile and cloud computing are blurring the traditional boundaries between personal and work life, and working onsite or offsite. While these trends promise compelling benefits, they also incur privacy and security risks. Managing these risks and avoiding security incidents, like breaches, requires a robust privacy and security policy; a proactive, preventative approach; and good detection and response capabilities. Healthcare organizations that embrace these trends in a secure manner will pave the way for future care coordination, integrated care delivery network models, and improved patient engagement.

## Best Practices Checklist for Implementing Mobile Devices

- Identify trends** that are relevant to your healthcare organization.
- Update your privacy and security policies**, procedures, standards and guidelines.
- Engage healthcare workers** who use mobile devices early in the process of device selection.
- Define healthcare use cases** and selection criteria for mobile devices.
- Jointly select the right device(s) and compute models** for each use case and task.
- Conduct regular risk assessments** to track the constantly evolving threat landscape.
- Implement security controls** prioritized in risk assessments.
- Conduct security awareness training**, and implement auditing and compliance controls.
- Detect and respond quickly to vulnerabilities**, including unsecured sensitive data detected by DLP, and security incidents such as breaches, to avoid or minimize business impact.
- Continually monitor safeguards** for effectiveness.

<sup>1</sup> Malicious Mobile Threats Report 2010/2011. Juniper Networks.

<sup>2</sup> [www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitech/enforcementiftr.html](http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitech/enforcementiftr.html)

<sup>3</sup> [http://info.sen.ca.gov/pub/01-02/bill/sen/sb\\_1351-1400/sb\\_1386\\_bill\\_20020926\\_chaptered.html](http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html)

<sup>4</sup> [www.ey.com/GL/en/Services/Advisory/IT-Risk-and-Assurance/Top-11-privacy-trends-for-2011---2--Breach-notification-requirements](http://www.ey.com/GL/en/Services/Advisory/IT-Risk-and-Assurance/Top-11-privacy-trends-for-2011---2--Breach-notification-requirements)

<sup>5</sup> Cybercrime in the Healthcare Industry. RSA. [www.healthcareinfosecurity.com/whitepapers.php?wp\\_id=338](http://www.healthcareinfosecurity.com/whitepapers.php?wp_id=338)

<sup>6</sup> Prioritizing Information Security Risks with Threat Agent Risk Assessment. Intel Corporation. [http://download.intel.com/it/pdf/Prioritizing\\_Info\\_Security\\_Risks\\_with\\_TARA.pdf](http://download.intel.com/it/pdf/Prioritizing_Info_Security_Risks_with_TARA.pdf)

<sup>7</sup> [www.intel.com/communities/ipp/anti-theft/launch.htm](http://www.intel.com/communities/ipp/anti-theft/launch.htm)

<sup>8</sup> [http://newsroom.intel.com/community/intel\\_newsroom/blog/2011/05/30/intels-maloney-talks-mobile-growth-industry-opportunities-at-computex](http://newsroom.intel.com/community/intel_newsroom/blog/2011/05/30/intels-maloney-talks-mobile-growth-industry-opportunities-at-computex)

<sup>9</sup> [www.reverseseamless.com](http://www.reverseseamless.com)

<sup>10</sup> 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 <http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni>. Also see: [www.intel.com/content/www/us/en/enterprise-security/enterprise-security-aes-ni-white-paper.html](http://www.intel.com/content/www/us/en/enterprise-security/enterprise-security-aes-ni-white-paper.html)

<sup>11</sup> [www.intel.com/content/www/us/en/solid-state-drives/solid-state-drives-320-series.html](http://www.intel.com/content/www/us/en/solid-state-drives/solid-state-drives-320-series.html)

<sup>12</sup> No system can provide absolute security under all conditions. Requires an enabled chipset, BIOS, firmware and software, and a subscription with a capable service provider. Consult your system manufacturer and service provider for availability and functionality. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit [www.intel.com/go/anti-theft](http://www.intel.com/go/anti-theft).

<sup>13</sup> Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, and virtual machine monitor (VMM). Functionality, performance, or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit [www.intel.com/go/virtualization](http://www.intel.com/go/virtualization).

<sup>14</sup> [www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/malware-reduction-general-technology.html](http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/malware-reduction-general-technology.html)

<sup>15</sup> <http://citrix.com/English/NE/news/news.asp?newsID=2311981>

<sup>16</sup> Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more, visit: [www.intel.com/technology/vpro](http://www.intel.com/technology/vpro).

<sup>17</sup> <http://ipt.intel.com>

<sup>18</sup> Cybercrime and the Healthcare Industry. RSA. [www.healthcareinfosecurity.com/whitepapers.php?wp\\_id=338](http://www.healthcareinfosecurity.com/whitepapers.php?wp_id=338)

<sup>19</sup> <http://newsroom.intel.com/docs/DOC-2032>


<sup>20</sup> [www.mcafee.com/us/solutions/mcafee-deepsafe.aspx](http://www.mcafee.com/us/solutions/mcafee-deepsafe.aspx)

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Copyright © 2011 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Atom, and Intel Core are trademarks of Intel Corporation in the U.S. and other countries.

\* Other names and brands may be claimed as the property of others.

Printed in USA 1011/DH/KC/LP/250

 Please Recycle

326193-001US

