Strategies for Hardware Enabled Security

Safeguarding Health Information: Building Assurance through HIPAA Security

David Houlding, MSc, CISSP
Healthcare Security & Privacy
Intel Healthcare IT Program Office

Outline

1. Healthcare Trends Driving Risk
2. Regulatory Security and Breach Notification Requirements
3. Breach Trends and Costs
4. Practical Strategies for Identifying Security & Privacy Needs in Healthcare
5. The Role of Hardware Enabled Security

A **proactive, preventative** approach is the best approach to security & privacy. What are your **future** needs?

Healthcare Trends
Driving Increased Security & Privacy Risk

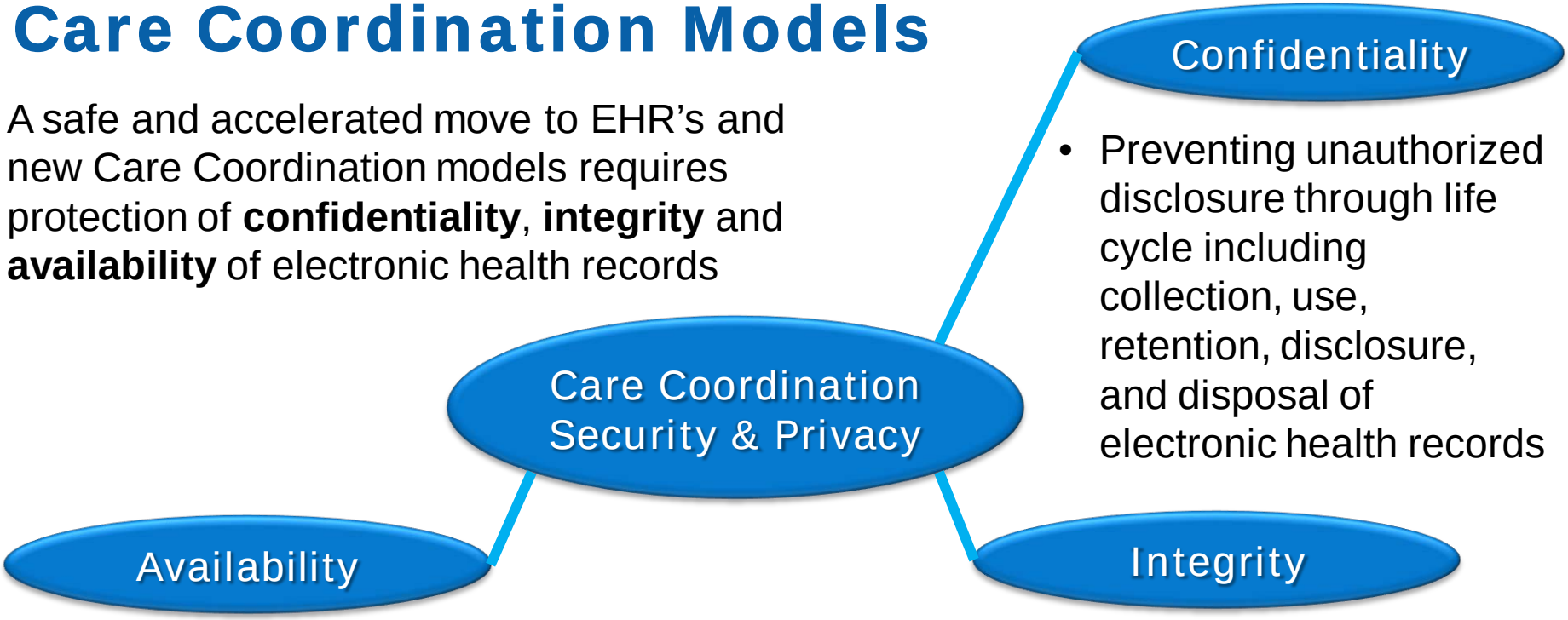
- Digitization of workflows
- Caregiver mobility is increasing
- Health information exchange
- New models of care are emerging
- Cloud computing changing the security perimeter
- Bring your own device is a growing trend
  - Increasing endpoint diversity
- Increasing use of PHR's
- Social media
- Complexity of new regulations

Security & Privacy in New Care Coordination Models

- IT density (new actors, venues, devices) increasing
  - Risk (probability) of security incidents increases
- New users to electronic health records
  - Administrative controls urgently needed including policy, procedures, security awareness training, auditing
- New workflows using electronic health records
  - New patterns of collection, use, retention, disclosure, disposal
  - New vulnerabilities, and threats; Threat Analysis Modeling required
- Multiple security & privacy policies across healthcare organizations
- Cross state / national border data flows, with different applicable regulations

Security & Privacy in New Care Coordination Models

A safe and accelerated move to EHR's and new Care Coordination models requires protection of **confidentiality**, **integrity** and **availability** of electronic health records



- Preventing unauthorized disclosure through life cycle including collection, use, retention, disclosure, and disposal of electronic health records

- Cloud and mobile technologies improve availability, and bring new security & privacy challenges
- Wireless coverage, performance for care coordination when & where required
- What if network goes down?
- What about remote care?

- Accuracy, completeness of PHI, and keeping up-to-date
- Multiple new contributors of information including patients, family caregivers and clinicians
- Versioning, context metadata, non-repudiation requirements

Security & Privacy Challenges in Mobile Computing

Managing diversity of mobile devices

Rapid change, new vulnerabilities

BYOD, high risk personal activities / apps

Less secure mobile locations and wireless

Regulatory compliance and breaches

Regulatory Protections for Health Information

- **Healthcare Organizations**
  - Covered Entities
    eg Health Plans,
    Clearinghouses, Providers
  - Business Associates
  - PHR Vendors

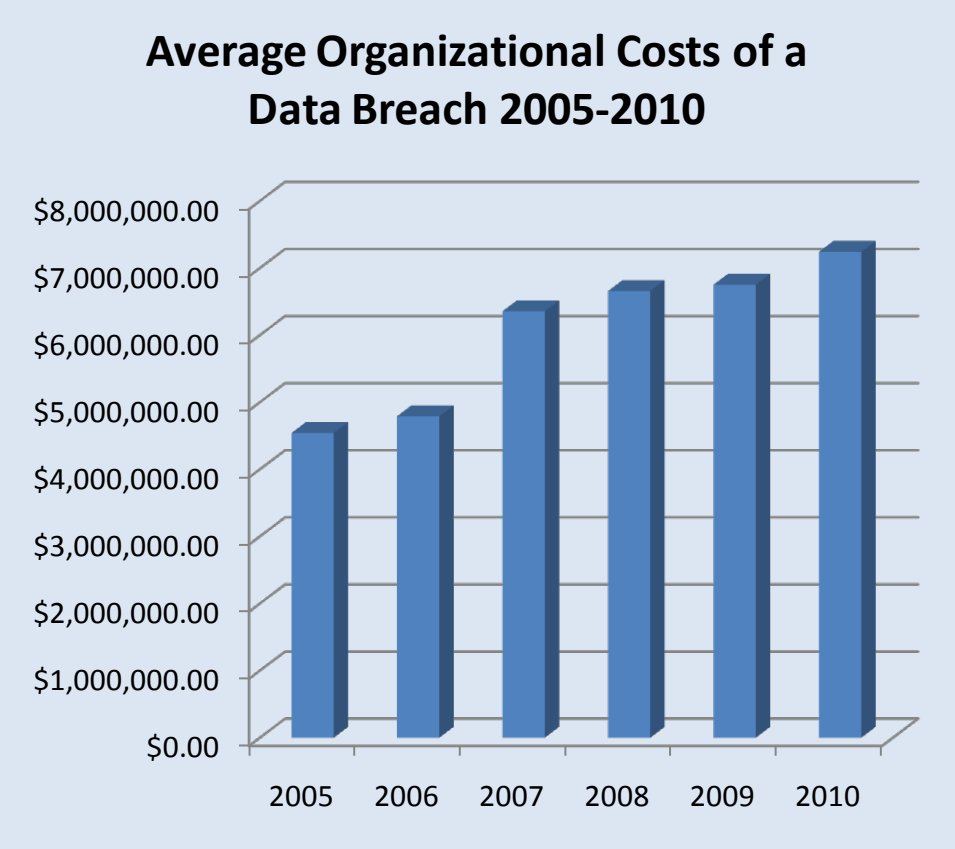
- **Regional Extent**
  - National eg HIPAA and HITECH Act (US)
  - State / Province eg SB 1386 (California)

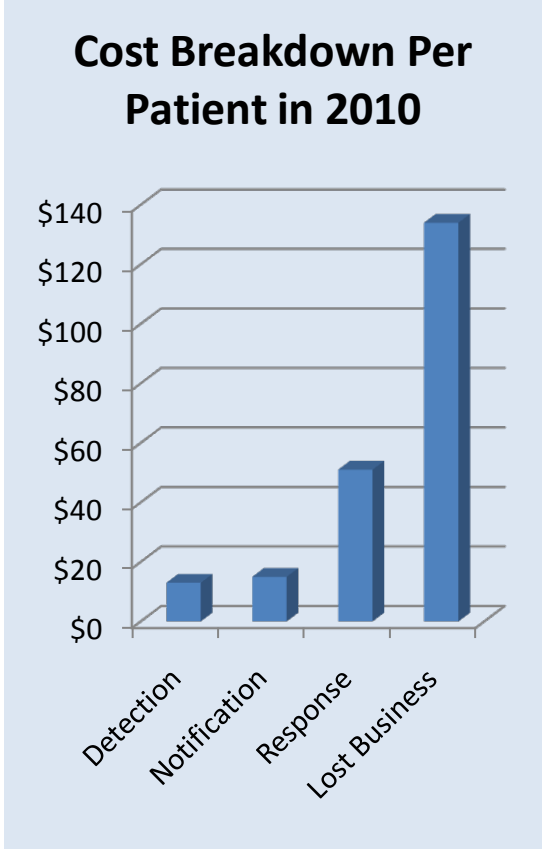
Regulatory Requirements for Notification of Breaches

- Precipitates the most damage and cost for organizations
- Increasingly required by regulations
  - Threshold influencing who needs to be notified eg HITECH (500 patients)
  - Requires notification of various stakeholders eg patients, government officials and the media
  - Defined window of time or annually

Avoiding breaches and the associated damage and cost is a key goal of organizations

Breaches Cost Healthcare Organizations

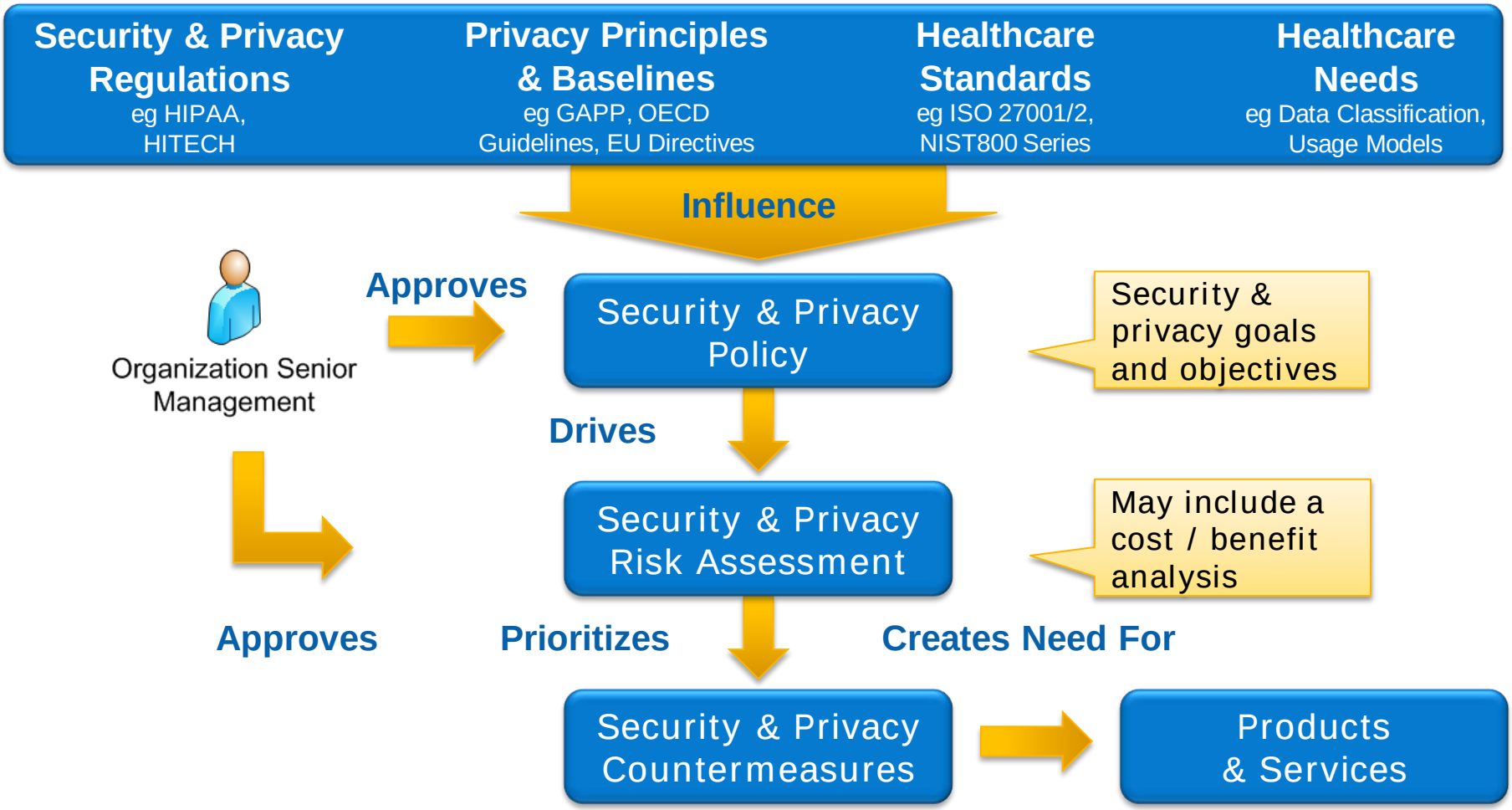




Ponemon Institute – 2010 Annual Study: U.S. Cost of a Data Breach

Risk is increasing. Notification is required by regulations. Breaches are expensive. Costs are growing.

Identifying Security & Privacy Needs



Protecting the Confidentiality of PHI

Healthcare Regulations
HIPAA Privacy Rule: requires protection of all *"individually identifiable health information" held or transmitted*

Influences

Healthcare Organization Security & Privacy Policy
-Confidentiality of sensitive data shall be protected at rest and in transit.

Drives

Healthcare Organization Security & Privacy Risk Assessment

Risk	Vulnerability	Threat	Probability	Impact
1	Laptop storing unprotected patient records	Breach through lost or stolen laptop	High	High

Is Mitigated By

Whole Disk Encryption

Is Implemented with Performance Using

AES-NI

Healthcare regulations are publicly available and this is not a legal summary or advice about regulations

Security & Privacy Risk Assessments

- Challenges
  - Limited budget to apply to security & privacy
  - Knowing when you are done
- Required by regulations and standards eg HIPAA, Meaningful Use core objectives, ISO27001 etc
- A practical, proven best practice to
  - Identify and prioritize risks, allocate funds
  - Provide a measured response to risks
- Done regularly, or with significant business changes
- Keep it simple

Qualitative Risk Assessment		Business Impact		
		Low	Medium	High
Probability of Occurrence	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Low	Low	Medium

Baseline

Is Encryption Alone Enough Protection?

- Encryption vulnerabilities
  - May not be activated, eg due to performance concerns
  - Weak choice of passwords
  - Same old password used
  - Poor key management, writing down passwords
  - Users may not logout, or may put mobile device on standby where pre-boot authentication is not required
  - Key loggers
  - Is it used pervasively at all points where PHI is at rest, in transit?

- Multi-layered approach
  - Administrative and physical controls in addition to technical controls
- Defense-in-depth approach
  - Combining encryption with other technical security controls, eg anti-theft technology for higher level of assurance PHI is secure

Protecting Confidentiality of PHI Using a Multi-Layered Approach

Technical Controls

- Disk encryption using Intel SSD with AES, or AES-NI

Administrative Controls

- Policy: Confidentiality of sensitive data shall be protected at rest and in transit. Data minimization. Good key management. Keys shall not be stored with locked devices.
- Security awareness training, and auditing

Physical Controls

- Secure storage, use and transportation of devices

Robust security depends on a multi-layered approach with administrative, physical and technical controls

Healthcare Security & Privacy Context

Healthcare Workers

Administrative Controls

Physical Controls

Technical Controls

Security Control Solution

- Services
- Software
- Hardware

Robust, High-Performance Hardware Enabled Security

Security & Privacy Risk Assessment

Identification of Security Controls Needed in Healthcare Org.

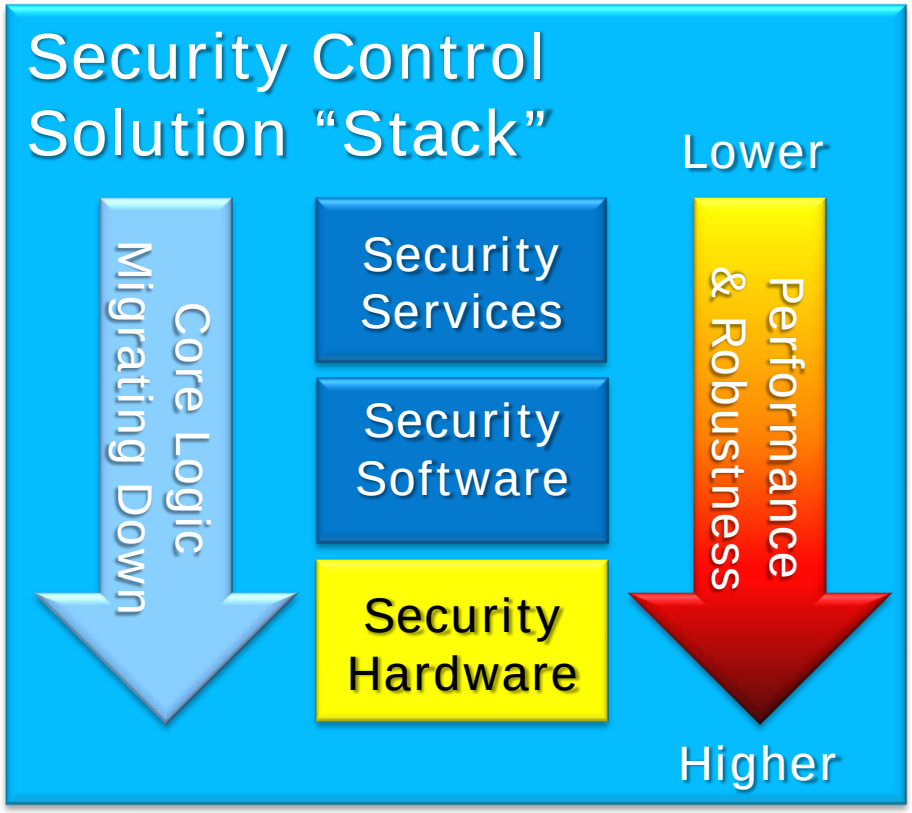
Security & Privacy Policy

Security & Privacy Foundation in Healthcare Org.

Healthcare Regulations, Privacy Principles, Standards, Business Needs (Data Classification, Usage Models)

Robust, High-Performance, Hardware-Enabled Security

- Increasing threat sophistication & performance demands, especially with defense-in-depth and mobile devices
- Robust hardware element at root of the solution stack
  - Immutable, not vulnerable to malicious changes
- Enables security with performance
  - Improves compliance
- Simplifies software above
- Combines robustness of hardware with flexibility of software
- Open platform, maximizing use of standards

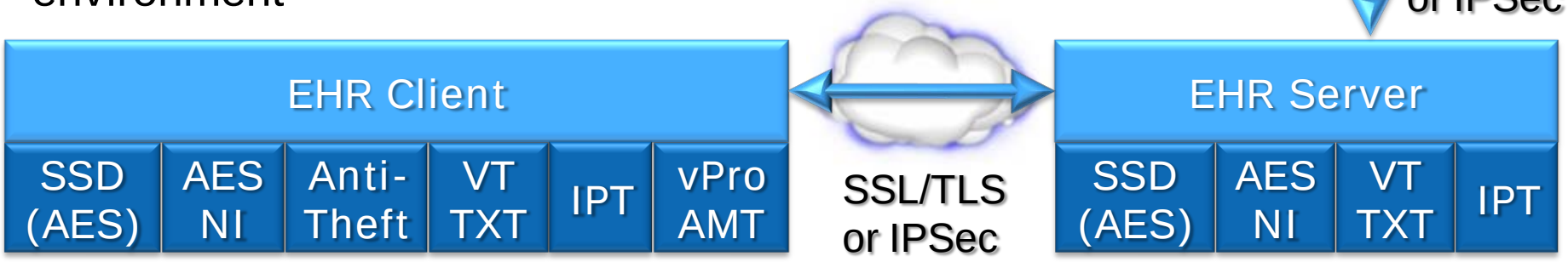


Intel AES-NI Software Ecosystem

Type	Product / Version	Availability
Secure Transactions (TLS/SSL)	Microsoft Windows Server 2008 R2	Now
	OpenSSL Patch	Now
	Red Hat Enterprise Linux 6	Beta 2 Now
	Fedora Linux 13	Now
Full Disk Encryption Software	Checkpoint Endpoint Security R73 FDE 7.4 HFA 1	Now
	McAfee Endpoint Encryption 6.0 with ePolicy Orchestrator 4.5	Now
	Microsoft BitLocker WS2008R2	Now
	PGP Universal 10.1	Now
	WinMagic SecureDoc	2011
	Dell Data Protection for Windows System	Now
Enterprise Applications	Oracle Berkeley DB 11.2.5.0.26	2010
	Oracle Database 11.2.0.2	2010
Virtualization	VMware ESX 4.0 U1 (supports AES-NI usage in the guest OS)	Now
	Citrix XenServer Midnight Rider 5.6 (supports AES-NI usage in the guest OS)	Now
	Oracle VM 3.0 beta (supports AES-NI usage in the guest OS)	Now
	Xen 4.0.1 (supports AES-NI usage in the guest OS)	Now
Tools / Libraries	Intel® Compiler, V11.0	Now
	Microsoft Visual Studio 2008 SP1	Now
	GNU Compiler Collection, GCC v4.4.0	Now
	Microsoft Crypto Next Generation, CNG WS2008R2	Now
	Intel® Integrated Performance Primitives crypto library V7.0	Beta Now
	Network Security Services, NSS 3.12.3	Now
	Solaris 10 Java Cryptographic Framework	Now

Intel Hardware Enabled Security Technologies for EHR's

- **SSD** (Solid State Drive) with AES: high performance, low power, robust, encrypted solid state drives
- **AES-NI** (Advanced Encryption Standard – New Instructions): high performance encryption of PHI at rest, in use, in transit
  IPT (Identity Protection Technology): strong 2-factor authentication
- **Anti-Theft**: mitigating loss or theft of client with PHI
- **vPro AMT** (Active Management Technology): improving manageability and compliance
- **VT/TXT** (Virtualization and Trusted Execution Technologies): protecting confidentiality and integrity in a virtualized / cloud environment



Summary

- Improving the quality and reducing the cost of patient care depends on moving to electronic health records
- Electronic health records have **new vulnerabilities** when compared to paper based equivalents
- Risk is exacerbated by several growing healthcare trends
- **Breaches and other security & privacy incidents are damaging and expensive**
- To avoid these a **proactive, preventative approach** to security & privacy is required
- Intel® delivers **robust, high-performance hardware based technologies** to meet the growing sophistication of threats and demands for performance
- Realizing the full benefits of these technologies in an end solution requires a **holistic, multi-layered and defense-in-depth approach**

Additional Resources

- Intel Healthcare IT Program Office
  - Healthcare Security & Privacy: David Houlding
    david.houlding@intel.com
- Mitigating Loss/Theft of PHI: Anti-theft
  http://www.intel.com/go/anti-theft
- Protecting PHI Confidentiality: AES-NI, SSD's
  http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/
  http://www.intel.com/design/flash/nand/320series/overview.htm
- Protecting PHI in Virtualization/Cloud: VT/TXT
  http://www.intel.com/go/virtualization
- Protecting Access to PHI: Identity Protection
  http://www.intel.com/technology/identityprotectiontechnology/index.htm
- Improving Compliance with Policy: vPro
  http://www.intel.com/technology/vpro

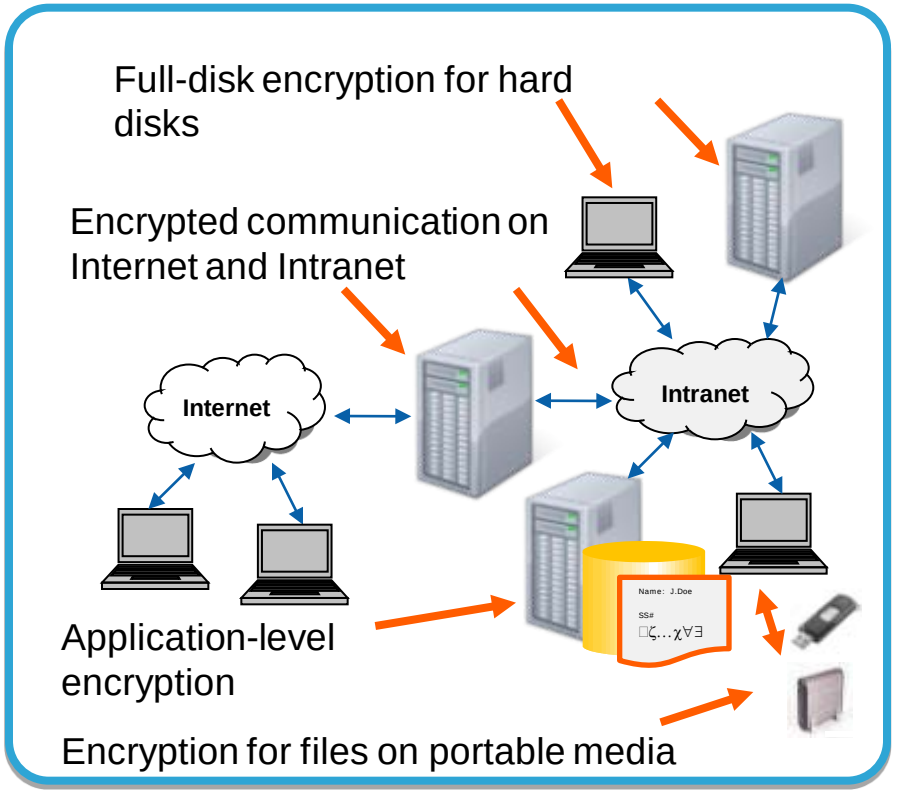
Legal Disclaimers

- **Intel® Anti-Theft Technology** (Intel® AT-p) 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. No system can provide absolute security under all conditions. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit http://www.intel.com/go/anti-theft
- **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: http://www.intel.com/technology/vpro
- Intel® Core™ vPro™ processor family includes **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 connection.
- **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 Intel® Core™ i5-600 Desktop Processor Series, Intel® Core™ i7-600 Mobile Processor Series, and Intel® Core™ i5-500 Mobile Processor Series. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/
- **Intel® Virtualization Technology** requires a computer system with an enabled Intel® processor, BIOS, 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 http://www.intel.com/go/virtualization
- **Intel® Identity Protection Technology:** No system can provide absolute security under all conditions. Requires an enabled chipset, BIOS, firmware and software and a website 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. For more information, visit http://ipt.intel.com/

BACKUP

Advanced Encryption Standard New Instructions (AES-NI)

- AES is currently the dominant block cipher, standardized by NIST in FIPS PUB 197
- Protects confidentiality of sensitive data at rest and in transit
- 6 new HW instructions
- HW acceleration: 3+ times
- More secure implementation of encryption
- Flexible in supporting all standard usage modes of AES
- Available in 2010 Intel Core and Xeon processors



Security in Self Encrypting Drives

- Confidentiality
  - AES 128 (Advanced Encryption Standard) hardware based encryption enables high performance full disk encryption
  - Enables improved compliance on clients and servers
  - Unlocked using a BIOS encryption key
- Integrity
  - New features to enhance data reliability and data safety
  - Anticipates power loss and prepares drive to avoid data loss
- Availability
  - Rugged and reliable, no moving parts
  - High performance read / write access
  - Low power consumption

Mitigating Loss or Theft of PHI with Intel® Anti-Theft Technology

Protections

- Hardware Based
- Works with/without Network connectivity (wired or wireless)
- Rendezvous timer
- Failed login threshold
- Poison pill
- Deterrent anti-theft label

Responses

- Centrally trigger PC to display recovery message
- Disable PC (prevent boot)
- Disable access to data by either:
  - Deleting essential cryptographic material stored in the hardware, or
  - Deleting user credentials

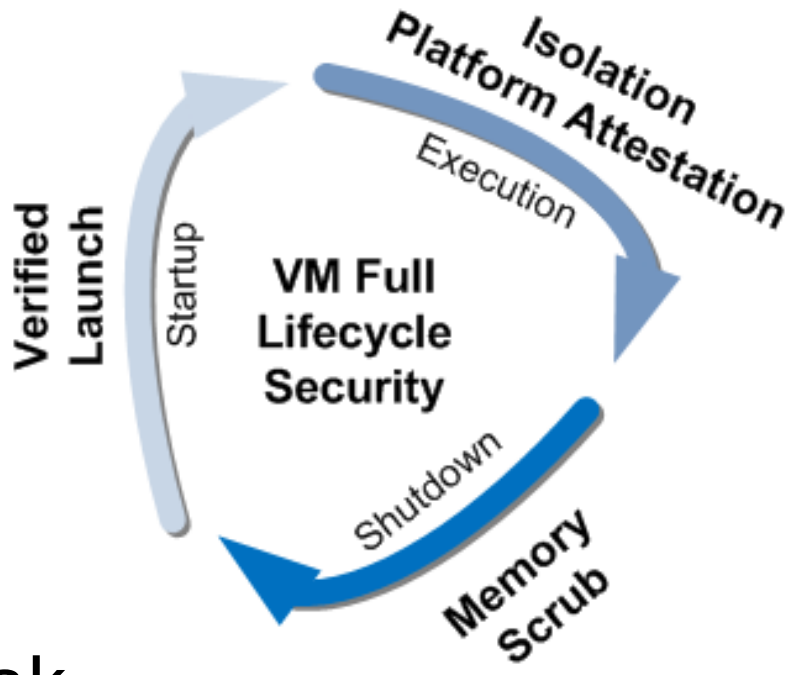
Recovery

- Recovery passphrase established at PC setup time to re-enable PC
- One time token generated centrally to re-enable PC

Leading Intel® Anti-Theft Technology Enabled Software Services: Computrace, LoJack and WinMagic

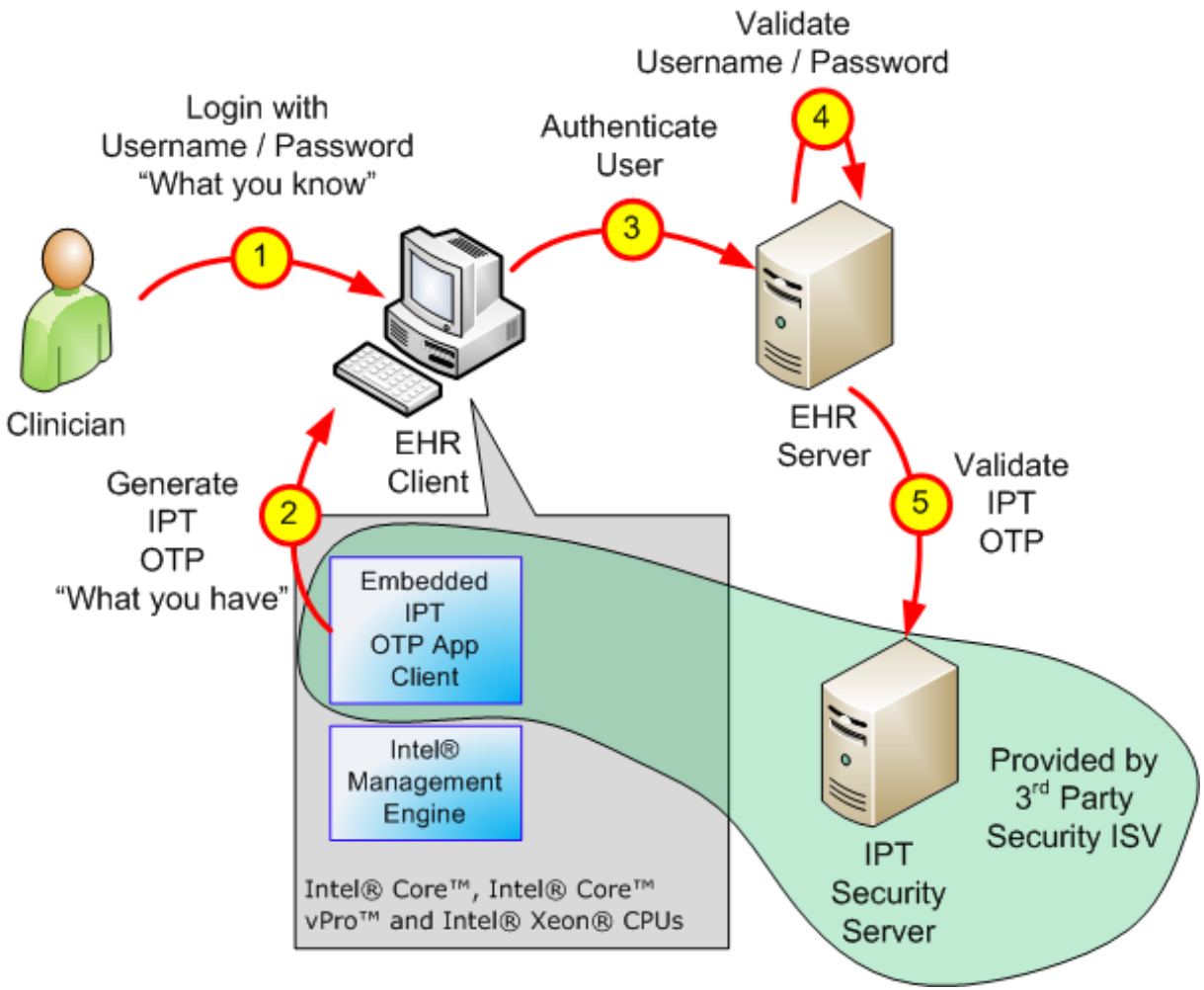
Healthcare and Virtualization Security

- VM full lifecycle security with Intel® Virtualization Technology and Trusted Execution Technologies
- Partitioning applications across VM's based on risk
  - Keep higher risk activities such as browsing away from most sensitive data eg PHI



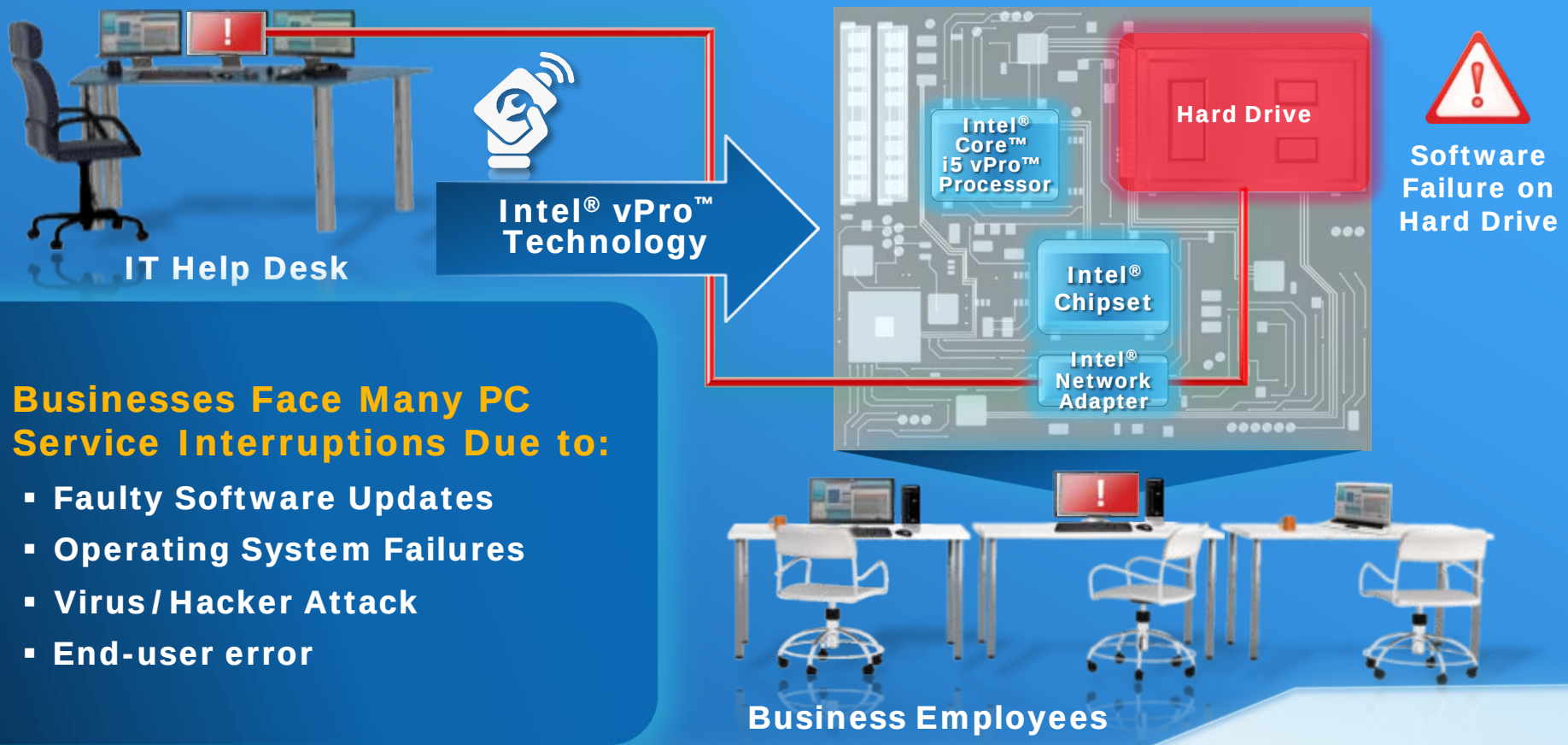
Intel Identity Protection Technology Login

- Strong 2-factor authentication without support challenges of separate hardware tokens
- Provisioning involves verifying the identity of the Clinician and placing an OTP serial number “hardware based cookie” on the EHR Client



2nd Gen Intel® Core™ vPro™ Processors

Remotely Diagnose and Repair Unresponsive PCs[7]



Businesses Face Many PC Service Interruptions Due to:

- Faulty Software Updates
- Operating System Failures
- Virus/Hacker Attack
- End-user error

Remotely diagnose, isolate, and repair an infected PC—even if its unresponsive

7 Intel® vPro™ Technology is sophisticated and requires setup and activation

Thank You