Healthcare Information at Risk: Practical Strategies to Avoid Breaches

Sam Pierre-Louis, CISSP-ISMP - - MDAnderson Cancer Center
David Houlding, CISSP, CIPP - - Intel
David S. Finn, CISA, CISM, CRISC - - Symantec
HITECH is Changing the Landscape

• HITECH provides significant financial support to adopt Electronic Record system - reimbursement incentives for “meaningful use”.

• Many significant changes to regulatory and compliance requirements:
  – Data Breach Notification for breach of unencrypted information: penalties, patient notification, self-reporting to media and State HHS (>500 records).
  – Expansion of HIPAA applicability (e.g. now includes Business Associates)
  – Increased fines for HIPAA violations
  – Increased legal exposure (criminal and civil penalties, State AG can sue)
  – “Meaningful Use” Requirements:
    • Maintenance of audit logs
    • Data encryption preferred
    • Recording of PHI disclosures
    • Security risk analysis
    • Implement security updates
    • Increasing integration with outside parties (patients, care providers, payors, state registries, health agencies labs, pharmacies) increases risk.
Security and IT has changed

Security

• Intelligent devices with embedded and downloadable software
• The Threat Landscape
• More automation, more data, more access

• Resulting in:
  – More dependency on highly complex IT systems and infrastructures
  – Highly valuable data

How we deliver IT

• Mobile
• Anytime, any where, any device
• Separation between IT infrastructure and consumer devices is fading
  – Infrastructures as well as data are merging
• Cloud for internal IT service delivery and delivery of IT services
• Legislation & Regulation are raising the Security & Privacy bar
Elements of a Risk Analysis

• Scope of the Analysis
• Data Collection
• Identify & Document Potential Threats and Vulnerabilities
• Assess Current Security measures
• Determine the Likelihood of Threat Occurrence
• Determine Potential Impact of Threat Occurrence
• Determine the Level of Risk
• Finalize Documentation
• Periodic Review and Updates
The Information-Centric Model

It’s about the data.

It’s about the data.

Policy  Compliance  Identity  Remediation  Reporting

Classification  Threats  Encryption  Ownership  Discovery

Infrastructure Security  Endpoint Management  Backup and Archiving  Storage Management  Availability

Physical  Virtual  Cloud

Healthcare Information at Risk: Practical Strategies to Avoid Breaches
Components of a Comprehensive Security and Risk Management Program

- Threats & Vulnerability Management
  - Industry Threat Monitoring
  - Vendor patches
- Identification of PHI in motion and at rest
  - Identification of critical assets
  - Protecting transmission of PHI
- Security Event Monitoring
  - Infrastructure
  - Application
- Network Vulnerability Scanning
- Endpoint Protection and Management
  - Antivirus/Antispam
  - IPS
  - Patch Management
  - Standard Builds
- Backup and Disaster Recovery
- Executive Reporting
Data Protection Extends Beyond the Enterprise

Increasing Connectivity and IT Proliferation

- Accessibility for all Departments and external Care / Service Providers
  - Increasing use of mobile technology / roaming users
    - Patient, Visitor, and Contractor Access
  - Mix of Devices - under IT Control and not under IT Control
    - Removable, high capacity Storage Devices

---

Enterprise

- Server
- Workstations
- Patients and Visitors
- Mobile Users
- Contractors
- Home PC
- Mobile Device
- Home Care Services
- Patient Access
- Sneakernet
- Remote Clinic
- Doctor's Office
Intel Laptop Anti-Theft Risk Estimator

- Quick assessment of your organizations risk of laptop loss or theft, and breach
- View estimated costs, and savings from implementing various safeguards
  - Encryption, Anti-Theft, Backup / Recovery
  - Based on research by Ponemon Institute

Risk Estimator Website

- Interactive
- PDF / PPT reports to share with stakeholders
- Useful resources
Privacy & Security Risk Assessments

• Challenges
  • Inconsistent risk prioritization
  • Too many risks
  • Only a regulatory checkbox

• Define threat agents for each risk in assessment
  • Intel Threat Agent Library has 22 threat agents with attributes
  • Approach is also used by the U.S. Dept. of Homeland Security

• More objective, consistent
  Focus on real risks, avoiding hypothetical distractions

• Justification of risks and expense on mitigations

Do you know what threats you face?
The Value of Healthcare Data

• Street cost for a stolen record
  - Medical:$50 vs SSN:$1

• Payout for identity theft
  - Medical:$20,000 vs Regular: $2,000

• Medical records can be exploited 4x longer
  - Credit cards can be cancelled, medical records can’t

Source: RSA Report on Cybercrime and the Healthcare Industry

Medical records are valuable and versatile to a cyber-criminal, who are strongly motivated to steal them.
Mobile and Cloud Break the Traditional Security Perimeter

• Many organizations still rely on a traditional perimeter approach
  • Physical – eg buildings
  • Logical – eg firewalls

• Hard shell, soft inside approach to security
• Mobile devices give anytime, anywhere access
• Sensitive data is moving into the cloud

Embracing mobile and cloud safely requires securing the sensitive data directly, at rest and in transit.
Is Encryption Alone Enough Protection?

- Inactive eg due to performance
- Weak, old, reused, or shared passwords
- Writing down passwords
- Users may not logout
- Key loggers capture passwords
- Is all sensitive data encrypted, at all points at rest and in transit?
- Can you prove that encryption was active on a lost / stolen device?

Whitepaper: Healthcare Information At Risk – Encryption is Not a Panacea

Robust security requires a multi-layered, defense-in-depth approach with encryption and other safeguards is required
Performance, User Experience and Compliance Challenges

- Users are motivated to disable or circumvent security controls that get in the way: compliance issues = risk eg breaches
- Security controls are much needed to mitigate risk on mobile devices and in the cloud

- Security control performance challenges
  - Limited compute power of mobile devices
  - Surging healthcare data in the cloud

Hardware Enabled Security protects healthcare data on mobile devices and the cloud, with high performance
Healthcare Security & Privacy Context

Security & Privacy Risk Assessment
Identification of Security Controls Needed in Healthcare Org.

Security & Privacy Policy

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

Healthcare Information at Risk: Practical Strategies to Avoid Breaches
Even if the encryption passphrase is obtained, the data is protected by this second level of lockdown security.

1. Stolen or Compromised Laptop with Intel® AT
2. Central IT service is alerted to the problem by a phone call and they remotely disable the laptop*.
3. Disabled Laptop: Only a screen with the owner’s contact info will appear.

*Or, automated lockdown measures kick in.
Symantec VIP and Intel Identity Protection Technology Provide Strong Authentication

• The Challenge: Physicians don’t want to be burdened with carrying a hardware token or by inputting an additional security token.

The VIP and IPT Solution: Add 2-factor authentication to login. After PC registration OTP code appears and user inputs it to allow access to the account.

The Bottom Line: Strong 2-factor authentication without usability and support issues of separate hardware tokens
University of Texas MD Anderson Cancer Center

• For seven of the past nine years, including 2010, MD Anderson has ranked No. 1 in cancer care in the “America’s Best Hospitals” survey published by U.S. News & World Report

• 18,000 employees including 1,500 faculty

• Over 1,200 hospital based volunteers

• 7,000 trainees participated in education programs
UT-MDACC Technical Complexities

- Platform disparities
- Hundreds of applications
- Thousands of servers
- Several data centers
- Centralized IT – about 700 employees
- Distributed IT – about 300 employees
- Ongoing development of new applications
- Continual infrastructure build-out
- Internal software development, e.g. EMR

Healthcare Information at Risk: Practical Strategies to Avoid Breaches
Complexities of Information Security Regulations


• State – Texas Administrative Code

• University of Texas Policies – UTS Policy 165, University Identity Management Federation

• Payment Card Industry standard (PCI)

• Sarbanes-Oxley

• Etc.
How to Manage the Chaos?

Healthcare Information at Risk: Practical Strategies to Avoid Breaches
MD Anderson Unified Controls Matrix (Process Before Technology)

- Mapping of all Information Security regulations and some security best practices
- Enables 1 assessment to satisfy applicable regulations versus conducting a special assessment for each regulation
- Reduces the hundreds upon hundreds of regulatory control points to a smaller set
- Developed high level Policies for end users
- Developed Operations Manual for system administrators
- Developed Security Guidelines
- Developed System Security Checklist
- Developed Risk Assessment Questionnaires
Unified Controls Matrix Example

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td></td>
<td></td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td></td>
<td></td>
<td>d</td>
<td>d</td>
<td>d</td>
<td>d</td>
<td>d</td>
</tr>
<tr>
<td>e</td>
<td></td>
<td></td>
<td></td>
<td>e</td>
<td>e</td>
<td>e</td>
<td>e</td>
<td>e</td>
</tr>
<tr>
<td>f</td>
<td>f</td>
<td>f</td>
<td>f</td>
<td>f</td>
<td>f</td>
<td>f</td>
<td>f</td>
<td>f</td>
</tr>
</tbody>
</table>

Data Classification Guidelines & Ratings
Risk Assessment Methodology

- Information Security sets expectations by holding kickoff meetings with Application/System Owner or designee
- Application Owner completes self assessment
- Host, web and database self-scans using Information Security’s “Gold” templates
- Criticality Assessment
- Validation by Information Security Risk Analyst and additional technical checks
- Action Plan
- **Very** Formal Exception Process
- Third party “real” penetration testing
## Risk Quantification

### Residual Risk Rating Sheet

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Risk Item</th>
<th>Lowest</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Highest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability of occurrence</td>
<td>Factor 1</td>
<td>Description 1</td>
<td>Description 2</td>
<td>Description 3</td>
<td>Description 4</td>
<td>Description 5</td>
<td>Description 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Factor 2</td>
<td>Description 1</td>
<td>Description 2</td>
<td>Description 3</td>
<td>Description 4</td>
<td>Description 5</td>
<td>Description 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Factor 3</td>
<td>Description 1</td>
<td>Description 2</td>
<td>Description 3</td>
<td>Description 4</td>
<td>Description 5</td>
<td>Description 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Impact</td>
<td>Factor 1</td>
<td>Description 1</td>
<td>Description 2</td>
<td>Description 3</td>
<td>Description 4</td>
<td>Description 5</td>
<td>Description 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Factor 2</td>
<td>Description 1</td>
<td>Description 2</td>
<td>Description 3</td>
<td>Description 4</td>
<td>Description 5</td>
<td>Description 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Factor 3</td>
<td>Description 1</td>
<td>Description 2</td>
<td>Description 3</td>
<td>Description 4</td>
<td>Description 5</td>
<td>Description 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Factor 4</td>
<td>Description 1</td>
<td>Description 2</td>
<td>Description 3</td>
<td>Description 4</td>
<td>Description 5</td>
<td>Description 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Detection Controls</td>
<td>Description 1</td>
<td>Description 2</td>
<td>Description 3</td>
<td>Description 4</td>
<td>Description 5</td>
<td>Description 6</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Exception Process Flow

• Request by customers via formal request process
• Analysis by Risk Analyst
• Approval Process
  – Director of Information Security
  – CIO or Deputy CIO
  – Internal Audit Taskforce
  – Information Services Executive Team (ISET) Committee
• Response Process via formal response process
• Exception Tracking Annual Review
Dovetail Risk Assessments within Other Programs

- Change Management Process
- IT Governance Process
- IT Standards Work Group
- Technical Review Work Group
- Solutions Engineering Team
- Information Security Work Group
- Infrastructure Steering Committee
- Business Continuity Executive Steering Committee
- Information Security Compliance Committee
- Etc.
Sampling of Metrics Reporting

- Compliance Reports (HIPAA, TAC 202, etc.)
  - Shows compliance information of each application being risk assessed
- Service Delivery
  - Risk Assessment cycle time metrics for each step of the process
- Operations improvement Reports
  - Change Management Readiness Level for each application going through Change Management
  - Disaster Recovery reports
- “Wall of Shame” Reports
  - Non-compliance reports
Recap of MDACC Risk Management Program

• Unified Controls Matrix as the basis of security policies and guidance
• Risk Assessment Methodology married to Unified Controls Matrix
• Integrate Vulnerability Assessment into Risk Assessment Process
• Integrate Disaster Recovery into Risk Assessment Process
• Integrate Risk Assessment Process into other institutional programs, e.g. Institutional Change Management, Project Management, etc.
• Build relationships with other departments within the institution
• Effect cultural change within the institution
Strategy for Breach Avoidance

1. Sound Risk Management Processes
2. Sound Risk Management Processes
3. Sound Risk Management Processes
4. Leverage Technology to Facilitate Processes
5. Sound Risk Management Processes
Intel 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](http://www.intel.com/go/anti-theft)

- **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/](http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/)

- **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 any other damages resulting thereof. For more information, visit [http://ipt.intel.com/](http://ipt.intel.com/)
Thank you!

Sam Pierre-Louis, CISSP-ISMP - - MDAnderson Cancer Center
spierrelouis@mdanderson.org
David Houlding, CISSP, CIPP - - Intel
David.houlding@intel.com
David S. Finn, CISA, CISM, CRISC - - Symantec
David.finn@symantec.com