Healthcare IT Security in the Era of Meaningful Use & Heightened Enforcement

Presented by:
Mac McMillan
CEO CynergisTek, Inc.
Chair, HIMSS Privacy & Security Policy Task Force

May 11, 2012
Today’s Faculty

- Co Founder & CEO CynergisTek, Inc.
- Chair, HIMSS P&S Policy Task Force
- Chair, HIMSS P&S Steering Committee
- Chair, HIMSS P&S Infosecurity Workgroup
- HIT Exchange Editorial Advisory Board
- HCPro Editorial Advisory Board
- Director of Security, DoD Agency
- Excellence in Government Fellow
- US Marine Intelligence Officer, Retired

Mac McMillan
CEO CynergisTek, Inc.
Agenda

• Volunteering
• Why Data Security is Important
• OCR’s New Random Audits
• “New Rules” Regulatory Update
• Enforcement’s New Face
• Questions/Discussion
The Privacy and Security Work at HIMSS
HIMSS Privacy & Security Committee

- One of fifteen HIMSS Committees, members approved by HIMSS Board

Workgroups and Task Forces

- Broad industry representation

Collaboration with other Associations

HIMSS Analytics, mHIMSS, HIMSS Outreach

Annual Conference and Regional Events
<table>
<thead>
<tr>
<th>Regulatory Activity</th>
<th>Anticipated Final Rule Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Plan Identifier/ICD-10 Delay</td>
<td>August/September 2012</td>
</tr>
<tr>
<td>Electronic Funds Transfer Standard</td>
<td>January 2014</td>
</tr>
<tr>
<td>Meaningful Use Stage 2</td>
<td>August/September 2012</td>
</tr>
<tr>
<td>Standards &amp; Certification Criteria for MU 2</td>
<td>August/September</td>
</tr>
<tr>
<td>Nationwide Health Information Network</td>
<td>TBD</td>
</tr>
<tr>
<td>Operating Rules for Electronic Funds Transfer and Electronic Transfers</td>
<td>TBD</td>
</tr>
<tr>
<td>Compliance Certification and Audit Program for Health Plan</td>
<td>TBD</td>
</tr>
<tr>
<td>Accounting for Disclosure</td>
<td>Late 2012</td>
</tr>
<tr>
<td>Omnibus Rule – Pending Changes from ARRA</td>
<td>Summer 2012</td>
</tr>
<tr>
<td>Final Breach Notification Rule</td>
<td>Summer 2012</td>
</tr>
<tr>
<td>Final Enforcement Rule</td>
<td>Summer 2012</td>
</tr>
</tbody>
</table>
Why Is Data Security An Issue?
Why Data Security Is Important

• People **choose** to disclose their most intimate information in order to get healthy
• Physicians **earn** their trust by guaranteeing privacy
• Privacy is assured by properly **protecting** systems and information
• Breaches undermine patient **confidence**
• No Confidence and people avoid treatment, lie or omit information, opt-out, and potentially **get sicker**
• Privacy and security are integral to **care**
What’s Changing?

• Pervasiveness of information being made available electronically has made healthcare a target of cybercriminals. (1 in 6 attacks in 2009 were HC, greatest growth in attacks in 2010 in HC, repeated again in 2011)

• In general, healthcare faces bigger risks going forward than the financial or retail sectors because the information that we have is more valuable and there is expected to be greater access.

• Cybercrime in Healthcare is in its infancy, but only because health information sharing is in its infancy, it will grow with the opportunity.
2011 healthcare assumes number one position in total number of breaches, and fifth in overall identities exposed.

The total number of breaches reported in healthcare exceeds 55,000 including those less than 500 records.
OCR: Causes of Breach

- 24% Paper Records
- 22% Laptops
- 16% Desktops
- 15% Portable Devices
- 11% Network
- 2% Email
- 2% EMR
- 8% Other

Source: Leon Rodriguez, 20th HIPAA Summit
• In 2011 and 2012 DefCon & BlackHat both featured presentations demonstrating the vulnerability of medical systems and devices.

• At RSA this year a presenter demonstrated how to hack an insulin monitor by intercepting the signal to the device and then causing a lethal dose of insulin to be released into the pancreas.

• A quarter of all hospitals reported an increase in breaches while 1/3 reported at least one case of Medical Identity theft.
OCR’s Audit Program
OCR Audit Program

• Requirement assigned to OCR in ARRA/HITECH
  • Conduct random audits of Covered Entities
• Used 2010 & 2011 to develop program
  • Determine pool of CEs and identify audit approach
  • Develop site selection process/organize CEs
  • Develop audit protocol
• Conduct 150 random audits by end of 2012
  • Number rounded down to 115
  • Will be notified in three waves
Audit Protocol Scope

- **Policies and Procedures**
  - Covers the HIPAA Privacy and Security Rules and the Breach Notification Interim Final Rule

- **Routine Operations**
  - Are policies implemented?
  - Do they address HIPAA adequately?
  - Are practices aligned?

- **Critical Weaknesses**
  - Focus on identifying weaknesses
<table>
<thead>
<tr>
<th>Category</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Plans</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Health care providers</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>Healthcare clearinghouses</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>5</strong></td>
<td><strong>6</strong></td>
<td><strong>3</strong></td>
<td><strong>6</strong></td>
<td><strong>20</strong></td>
</tr>
<tr>
<td>Health Plans</td>
<td>Providers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medicaid</td>
<td>Allopathic &amp; Osteopath Physicians</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCHIP</td>
<td>Hospitals</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Laboratories</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Health</td>
<td>Dental</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nursing &amp; Custodial Care Facilities</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health Insurance Issuer</td>
<td>Pharmacy</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Timeline of an Audit

- Notification letter from OCR
- Documentation due (10 business days from notice)
- Start of site visit (30 – 90 days from notice)
- Additional analysis and questions
- Draft audit report (20 – 30 days from end of site visit)
- Comments on draft audit report due (10 business days from draft audit report)
- Final audit report (30 days after comments)
Documentation Review: Can Include

- Demographic Information
- Policies & Procedures
- Key Person Information
- Organizational Chart
- Incident response plans
- Contingency plans
- System generated information
- Technical controls information
- Physical safeguards
- Notice of Privacy Practices
- Privacy documentation
- Training documentation
- Compliant handling and sanction policies
- Mitigation practices
- Policies and procedures regarding uses and disclosures
- Breach notification policies and procedures
Audit Reports

- Information about covered entity
- Methodology
- Findings
- Acknowledgment of best practices
- Overall conclusion
- Opportunity to dispute/appeal
Audit Findings

• Condition: Observed noncompliance and evidence
• Criteria: Citation of provision(s) potentially violated
• Cause: Reason the noncompliance exists
• Effect: Risk of resulting noncompliant status
• Recommendation
• Corrective action taken (if any)
Lessons Learned

• Readiness and organization are key
• Close the gap between policy, practice & documentation
• A prepared workforce performs better
• Audits are very broad in scope and very detailed in execution
• Risk analysis and policies are key
• Workforce training is important
• Deception is “very” bad
• Resolution is OCR’s and may be delayed
“New Rules” Regulatory Update
HITECH Recap

- Modified enforcement penalties/raised limits for fines
- Required HHS to accomplish rule making and publish guidance
- Introduced and defines “Willful Neglect”
- Required OCR to implement random compliance audits for covered entities
- Introduces the concept of Meaningful Use and sets criteria for certified EHRs
The Omnibus Rule: Modifications to HIPAA

- Creates new and revised privacy and security requirements (Sect. 13401/Sect. 13404) to be covered in the Omnibus Rule now at OMB:
  - Breach Notification
  - Business Associates
  - Marketing of PHI
  - Fundraising
  - No Sale of PHI
  - Patient Access/Disclosure Restrictions
  - Limited Data Set/Minimum Necessary
• Meaningful Use requires providers implement and demonstrate that they are using EHR technology in ways that can be measured.
• Security under MU is the same as security under the original HIPAA security rule, provide for confidentiality, availability and integrity of PHI.
• Attestation is different than compliance with HIPAA. Establishes eligibility to receive federal funding based on defined criteria.
• Both Stage I and Stage II are focused primarily on EHR adoption.
• Perform and/or update security risk analysis and address deficiencies (explanation of encryption practices)

• EP: Use secure electronic messaging to communicate with patients on relevant health information

• Record (log) actions related to health information, audit log status and encryption of end user devices

• Any encryption has to meet NIST specification and be approved by FIPS 140-2

• Synchronization of clocks must meet Network Timing Protocol (NTP) v3 or v4
• Authenticate users against unique identifiers and proscribed accesses
• Auditing by default, permit restricted access and monitor for tampering
• Permit an end user to create an audit report for a specific period of time and permit sorting by specific criteria
• Permit amendments or comments to a patient record while preserving the original record content
• Permit automatic logoff after a predetermined time
• Permit access to patient information, in time of emergency, by identified set of users

• Encryption of end user devices if PHI remains on the device after disconnecting from the EHR application by default

• Ensure integrity of patient information within the EHR and information exchanged by creating a message digest

• Optional – record disclosures made for treatment, payment and operations for purposes of accounting for disclosure
GINA NPRM

• GINA content:
  – Mandates modifications of the Privacy Rule to incorporate provisions specific to genetic information
  – Genetic information is protected health information
  – Prohibits the use or disclosure of genetic information for underwriting
• Advance Notice of Proposed Rulemaking: The Common Rule (Applies to Research Data)
  • Better calibrate level of review to level of risk
  • Improve informed consent
  • Implement data protection standards to protect against informational risk
  • May necessitate future changes to the HIPAA regulations to harmonize
  • Safeguards modeled on the HIPAA Security Rule
A New Sheriff Is In Town
• OCR is aggressively enforcing HIPAA Privacy and Security Rules
• Covered Entities and Business Associates should have demonstrable HIPAA Privacy and Security compliance programs
• A robust compliance program includes employee training, vigilant implementation of policies and procedures, regular internal audits, and a prompt action plan to respond to incidents
A New Era of Enforcement

• Fine of BlueCross BlueShield of Tennessee ushers in new era of “monetary enforcement” by the agency, in contrast to its long-standing approach of what OCR Director, Leon Rodriguez termed “handholding”.

• Following the Phoenix Cardiac Surgery resolution Rodriguez said, “We hope that healthcare providers pay careful attention to this resolution agreement and understand the HIPAA Privacy and Security Rules have been in place for many years, and OCR expects full compliance no matter the size of a covered entity.”
• HIPAA Privacy and Security enforcement are the responsibility of HHS/OCR:
  — Resolution of complaints (25% result in CAP)
  — Investigation of Breaches (50+% result in CAP)
  — Random audit program (115 by year-end)
• Meaningful Use attestation enforcement is the responsibility of HHS/CMS:
  — Audits/investigation by OIG (2012 Audit Plan)
• State Attorneys General may also bring enforcement actions.
• 400+ reports involving a breach of over 500 individuals
  – Theft and loss account for 65% of large breaches (about 70% of these incidents involve ePHI)
  – Laptops and other portable storage devices account for 37% of large breaches
  – Paper records are 24% of large breaches
• 50,000+ reports of breaches of under 500 individuals
• Raised concern in Congress latter 2011, audit report out due in 2013
Questions
Thank You

For more Information please check out the CynergisTek blog site.

www.cynergistek.com

Mac McMillan
Mac.McMillan@cynergistek.com
(512) 402-8555