Crowe Horwath

The Unique Alternative to the Big Four®

HIPAA/HITECH Security and Privacy

A Practical Approach

Presented by:

Raj Chaudhary, PE, CGEIT
Partner, Crowe Horwath LLP

Chris Reffkin, CISSP
Manager, Crowe Horwath LLP

www.crowehorwath.com/hipaa

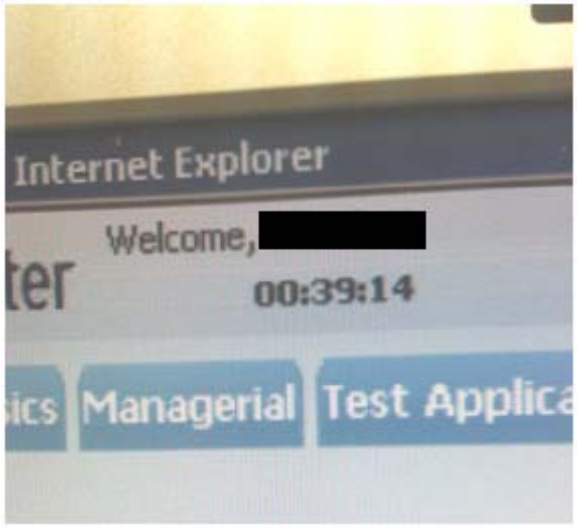
Learning Objectives and Agenda

- Introduction
- Holistic View of HIPAA
- A Picture is Worth a Thousand Words…
- Overall 5-Step Approach to HIPAA Compliance
- Top 5 HIPAA Security and Privacy Gaps
- Meaningful Use/CMS Incentives/EHR Certification
- Approach to EHR Certification and Compliance (Security)
- Top 5 Considerations for Self EHR Certification (Security)
- Q&A

Holistic View of HIPAA

- There is more than just EHRs with PHI…

A Picture is Worth a Thousand Words…



Workstation in the On Call room had been left logged in for 40 minutes and was discovered unattended.

Unlocked and unattended file cabinets with PHI.

Labs left unattended and unlocked.

Overall 5-Step Approach to HIPAA Compliance

- Security
  1. Policy Gap Analysis
  2. Application Inventory (50-70 Apps w/PHI) and Risk Rating
  3. Gap Analysis
     a) Top x # (6-10) High-Risk-Applications Application Control Gap Analysis
     b) Entity Level Controls Gap Analysis
  4. Survey Based Gap Analysis of Remaining Applications

- Privacy
  1. Policy Gap Analysis
  2. Agree on privacy survey participants with CMO
  3. Conduct privacy survey of selected departments
  4. Update Gap Analysis from Step 1 with Results of Survey

5. Common Step for Security and Privacy
   - Walk Through Observations
   - Picture is worth a thousand words

End Result: Risk Ranked Remediation Plan

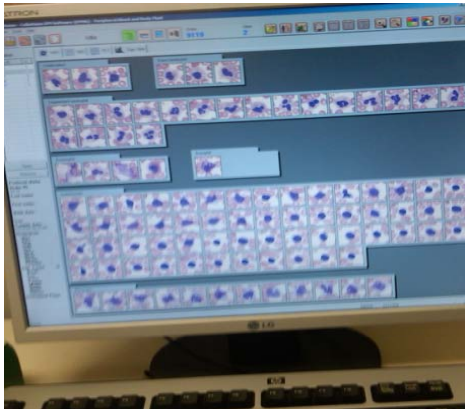
Top 5 HIPAA Security and Privacy Gaps

1. Safeguarding Data from Unauthorized Individuals/Physical Security

2. Vendor Management Function/Business Associate Processes

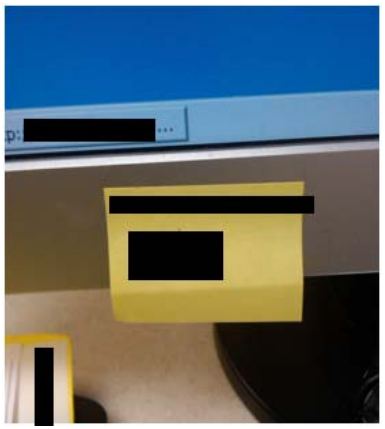
Top 5 HIPAA Security and Privacy Gaps

3. Entity Level IT Security Governance



4. Inadequate Application Logging and Monitoring

5. Weak Application Access Control Processes



Meaningful Use/CMS Incentives/EHR Certification

Meaningful Use -15 Core Objectives

NUMBER	DESCRIPTION	METRIC OR % OF PATIENTS
Core 1	Record Patient Demographics	>50% Structured Data
Core 2	Record Vital Signs/Chart Changes	>50% Structured Data
Core 3	Up-to-date List of Current Diagnosis	>80% - at least one entry
Core 4	Maintain Active Medication List	>80% - at least one entry
Core 5	Maintain Active Medication Allergy	>80% - at least one entry
Core 6	Record Smoking Status >13 Years Age	>50% Structured Data
Core 7 (Hosp.)	On Request E-Copy of Hospital Discharge	>50% Patients Discharged
Core 7 (Phys.)	Clinical Summary of Office Visit	>50% Patients Within 3 Days
Core 8	On Request Electronic Copy of Health Inf.	>50% Requesting Within 3 Days
Core 9	Generate/Transmit Permissible Prescriptions	>40% E-Transmit Certified EHR
Core 10	CPOE for Medication Orders	>30% At Least 1 Medication
Core 11	Implement Drug-Drug/Allergy Interaction	Functionality is Enabled
Core 12	E-Exchange of Clinical Information	1 Test of E-Exchange of HER
Core 13	Implement 1 Clinical Decision Support Rule	1 Rule Implemented
Core 14	Implement Security/Privacy of Patient Data	Review Security Risk Analysis Implement Security Updates Correct Security Deficiencies
Core 15	Report Clinical Quality Measures to CMS	

Approach to EHR Certification and Compliance (Security)

- Vendor Supplied/Certified EHR Technology
  - Upgrade to certified version
  - Verification of Vendor Certification

- In-House Developed EHR Technology
  - CCHIT EHR Alternative Certification for Hospitals (EACH) Program
  - Approved Test Procedures v1.1 (NIST)
    - 45 Certification Criteria to be tested
    - 8 of which are security-focused

Approach to EHR Certification and Compliance (Security)

- Security Focused Certification Criteria
  - Access Control
  - Emergency Access
  - Automatic Log-Off
  - Audit Log
  - Integrity
  - Authentication
  - General Encryption
  - Encryption when Exchanging Electronic Health Information

- Should look familiar in regards to your overall HIPAA Security and Privacy Compliance Program…

Approach to EHR Certification and Compliance (Security)

- The requirements for EHR Certification correlate to Standards and Implementation Specifications from the HIPAA Security Rule

Approved Test Procedures v 1.1	Certification Criteria / HIPAA (Standard or Imp. Spec.)	HIPAA/HITECH Reference
§170.302 (o)	Access Control	§164.312(a)(1)
§170.302 (p)	Emergency Access	§164.312(a)(2)(iii)
§170.302 (q)	Automatic Log-Off	§164.312(a)(2)(iii)
§170.302 (r)	Audit Log	§164.312(b)
§170.302 (s)	Integrity	§164.312(c)(1)
§170.302 (t)	Authentication	§164.312(d)
§170.302 (u)	General Encryption	§164.312(a)(2)(iv)
§170.302 (v)	Encryption when Exchanging Electronic Health Information	§164.312(e)(2)(ii)

Top 5 Considerations for Self EHR Certification (Security)

- Independence and Developers
  - Consider implications of in-house testing
  - "…the Tester remains in full control of the testing process, directly observes the test data being entered by the Vendor, and validates that the test data are entered correctly as specified in the test procedure. "

- Audit Logs
  - A developer/debug log is generally not the same as an audit log; specific requirements for log details are provided by certification criteria
  - Consider overall benefits to organization versus just meeting the requirements; a tool or utility may be useful in general to manage logging and monitoring of events

- Encryption
  - Balanced knowledge of HIPAA/Meaningful Use as well as technology required to fully understand in order to apply "common sense"

Top 5 Considerations for Self EHR Certification (Security)

- Integration with Overall HIPAA Compliance Efforts
  - Ensure all members of the HIPAA Compliance Committee and/or the HIPAA Security and Privacy Officers are collaborating on certification efforts
  - Verify direction of overall HIPAA compliance efforts align with certification efforts
    - Want to avoid designing a control for certification that contradicts efforts or not does not follow direction of overall HIPAA compliance program

- Ongoing Maintenance
  - Release version 2 of Approved Test Procedures anticipated April 2011

Q&A

For more information, contact or visit:

Raj Chaudhary

Direct: 312.899.7008

Mobile: 574.210.7005

Raj.Chaudhary@crowehorwath.com

Chris Reffkin

Direct: 317.208.2547

Mobile: 219.718.2860

Chris.Reffkin@crowehorwath.com

Or visit:

www.crowehorwath.com/hipaa