# Meaningful Use Risk Analysis

<table>
<thead>
<tr>
<th>Impact</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unencrypted laptop ePHI</td>
<td>Lack of auditing on EHR systems</td>
<td>Missing security patches on web server hosting patient information</td>
</tr>
<tr>
<td></td>
<td>Unsecured wireless network in doctor’s office</td>
<td>Outdated anti-virus software</td>
<td>External hard drives not being backed up</td>
</tr>
<tr>
<td></td>
<td>Sales presentation on USB thumb drive</td>
<td>Web server backup tape not stored in a secured location</td>
<td>Weak password on internal document server</td>
</tr>
</tbody>
</table>
Who are we

EHR 2.0 Mission: To assist healthcare organizations develop and implement practices to secure IT systems and comply with HIPAA/HITECH regulations.

- **Education**
- **Consulting**
- **Toolkit (Tools, Best Practices & Checklist)**

**Goal:** To make compliance an enjoyable and painless experience
Webinar Objective

Understand and Perform Meaningful Use Risk Analysis that satisfies CMS incentive and attestation requirement.
Glossary

1. HHS, CMS:

2. NIST:

3. Threats and Vulnerabilities:

4. Findings:

5. Risk Analysis:
The American Recovery and Reinvestment Act of 2009 and HITECH

Federal Spending for ARRA includes federal tax cuts, expansion of unemployment benefits and other social welfare provisions, and domestic spending in education, health care, and infrastructure, including the energy sector.
HITECH Act

The Health Information Technology for Economic and Clinical Health (“HITECH”) provisions of the American Recovery and Reinvestment Act of 2009 (“ARRA”, also referred to as the “Stimulus Bill”) codify and expand on many of the requirements contained in the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and its regulations to protect the privacy and security of protected health information (“PHI”).
HITECH modifications to HIPAA including:

- Creating incentives for developing a meaningful use of electronic health records
- Changing the liability and responsibilities of Business Associates
- Redefining what a breach is
- Creating stricter notification standards
- Tightening enforcement
- Raising the penalties for a violation
- Creating new code and transaction sets (HIPAA 5010, ICD10)
## CMS Meaningful Use Incentives

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Medicare</td>
<td>Medicaid</td>
<td>Medicare</td>
<td>Medicaid</td>
<td>Medicare</td>
<td>Medicaid</td>
</tr>
<tr>
<td>2011</td>
<td>$18,000</td>
<td>$21,250</td>
<td>$18,000</td>
<td>$21,250</td>
<td>$18,000</td>
<td>$21,250</td>
</tr>
<tr>
<td>2012</td>
<td>$12,000</td>
<td>$8,500</td>
<td>$12,000</td>
<td>$8,500</td>
<td>$15,000</td>
<td>$21,250</td>
</tr>
<tr>
<td>2013</td>
<td>$8,000</td>
<td>$8,500</td>
<td>$8,000</td>
<td>$8,500</td>
<td>$12,000</td>
<td>$21,250</td>
</tr>
<tr>
<td>2014</td>
<td>$4,000</td>
<td>$8,500</td>
<td>$8,000</td>
<td>$8,500</td>
<td>$8,000</td>
<td>$8,500</td>
</tr>
<tr>
<td>2015</td>
<td>$2,000</td>
<td>$8,500</td>
<td>$4,000</td>
<td>$8,500</td>
<td>$8,000</td>
<td>$8,500</td>
</tr>
<tr>
<td>2016</td>
<td>$8,500</td>
<td>$2,000</td>
<td>$4,000</td>
<td>$8,500</td>
<td>$4,000</td>
<td>$8,500</td>
</tr>
<tr>
<td>2017</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
</tr>
<tr>
<td>2018</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
</tr>
<tr>
<td>2019</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
</tr>
<tr>
<td>2020</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
</tr>
<tr>
<td>2021</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
<td>$8,500</td>
</tr>
<tr>
<td>Total</td>
<td>$44,000</td>
<td>$63,750</td>
<td>$44,000</td>
<td>$39,000</td>
<td>$24,000</td>
<td>$63,750</td>
</tr>
<tr>
<td></td>
<td>$63,750</td>
<td>$63,750</td>
<td>$63,750</td>
<td>$63,750</td>
<td>$63,750</td>
<td>$63,750</td>
</tr>
</tbody>
</table>

For Eligible Professionals
For Eligible Professionals

Eligible Professional
Meaningful Use Core Measures
Measure 15 of 15
Stage 1
Date issued: November 7, 2010

<table>
<thead>
<tr>
<th>Protect Electronic Health Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objective</strong></td>
</tr>
<tr>
<td>Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.</td>
</tr>
<tr>
<td><strong>Measure</strong></td>
</tr>
<tr>
<td>Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.</td>
</tr>
<tr>
<td><strong>Exclusion</strong></td>
</tr>
<tr>
<td>No exclusion.</td>
</tr>
</tbody>
</table>
For Eligible Hospital & CAH

Eligible Hospital and Critical Access Hospital
Meaningful Use Core Measures
Measure 14 of 14
Stage 1
Date issued: November 7, 2010

Protect Electronic Health Information

Objective
Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.

Measure
Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

Exclusion
No exclusion.
HIPAA Titles - Overview

HIPAA
Health Insurance Portability and Accountability Act

Title I
- Health care Access, Portability and Renewability
- Preventing Healthcare Fraud and Abuse
- Medical Liability Reform

Title II
- Administrative Simplification
- Electronic Data Interchange
- Privacy
- Transactions
- Identifiers
- Code sets

Title III
- Tax Related Health Provision

Title IV
- Group Health Plan requirement

Title V
- Group Offsets

Security
- Security Standards: General Rules
- Administrative Safeguard
- Physical Safeguard
- Technical Safeguard
- Organizational Requirements
- Policies and Procedures and Documentation Requirements
HIPAA Security Rule

HIPAA Title II Administrative Simplification

- Security Standards: General Rules (§164.306)
- Administrative Safeguards (§164.308)
- Physical Safeguards (§164.310)
- Technical Safeguards (§164.312)
- Organizational Requirements (§164.314)
- Policies and Procedures and Documentation Requirements (§164.316)

- Security management process
  - Assigned Security Responsibility
  - Workforce Security
  - Information Access Management
  - Security Awareness and Training
  - Security Incident Procedures
  - Contingency Plan
    - Evaluation

- BA Contracts and other arrangements
- Facility Access Control
  - Workstation Use
  - Workstation Security
  - Device and Media Control
- Access Control
  - Audit Controls
    - Integrity
    - Person or entity authentication
    - Transmission Security
Information Security Model

Confidentiality
Limiting information access and disclosure to authorized users (the right people)

Integrity
Trustworthiness of information resources (no inappropriate changes)

Availability
Availability of information resources (at the right time)
# ePHI – 18 Elements

<table>
<thead>
<tr>
<th>Elements</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Max Bialystock</td>
</tr>
<tr>
<td>Address</td>
<td>1355 Seasonal Lane (all geographic subdivisions smaller than state, including street address, city, county, or ZIP code)</td>
</tr>
<tr>
<td>Dates related to an individual</td>
<td>Birth, death, admission, discharge</td>
</tr>
<tr>
<td>Telephone numbers</td>
<td>212 555 1234, home, office, mobile etc.,</td>
</tr>
<tr>
<td>Fax number</td>
<td>212 555 1234</td>
</tr>
<tr>
<td>Email address</td>
<td><a href="mailto:LeonT@Hotmail.com">LeonT@Hotmail.com</a>, personal, official</td>
</tr>
<tr>
<td>Social Security number</td>
<td>239-68-9807</td>
</tr>
<tr>
<td>Medical record number</td>
<td>189-88876</td>
</tr>
<tr>
<td>Health plan beneficiary number</td>
<td>123-ir-2222-98</td>
</tr>
<tr>
<td>Account number</td>
<td>3333389</td>
</tr>
<tr>
<td>Certificate/license number</td>
<td>3908763 NY</td>
</tr>
<tr>
<td>Any vehicle or other device serial number</td>
<td>SZV4016</td>
</tr>
<tr>
<td>Device identifiers or serial numbers</td>
<td>Unique Medical Devices</td>
</tr>
<tr>
<td>Web URL</td>
<td><a href="http://www.rickymartin.com">www.rickymartin.com</a></td>
</tr>
<tr>
<td>Internet Protocol (IP) address numbers</td>
<td>19.180.240.15</td>
</tr>
<tr>
<td>Finger or voice prints</td>
<td>finger.jpg</td>
</tr>
<tr>
<td>Photographic images</td>
<td>mypicture.jpg</td>
</tr>
<tr>
<td>Any other characteristic that could uniquely identify the individual</td>
<td></td>
</tr>
</tbody>
</table>
HIPAA Security – Administrative safeguard (§164.308)

a(1) Security Management Process
Implement policies and procedures to prevent, detect, contain, and correct security violations.

(A) Risk analysis (Required)
Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

(B) Risk management (Required)
Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).

(C) Sanction policy (Required)
Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

(D) Information system activity review (Required)
Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
Infrastructure

- Computers
- Storage Devices
- Networking devices (Routers, Switches & Wireless)
- Medical Devices
- Scanners, fax and photocopiers
- VoIP
- Smart-phones, Tablets (ipad, PDAs)
- Cloud-based services

Any device that electronically stores or transmits information using a software program
Trends in Healthcare IT

- Informatics
- Collaboration
- Mobile Computing
- EHR HIE
Handheld Usage in Healthcare

- 25% usage with providers
- Another 21% expected to use
- 38% physicians use medical apps
- 70% think it is a high priority
- 1/3 use hand-held for accessing EMR/EHR

compTIA 2011 Survey
EMR and EHR systems

Figure 1. Percentage of office-based physicians with EMR/EHR systems: United States, 2001–2009, and preliminary 2010–2011

NOTES: EMR/EHR is electronic medical record/electronic health record. “Any EMR/EHR system” is a medical or health record system that is all or partially electronic (excluding systems solely for billing). Data for 2001–2007 are from the in-person National Ambulatory Medical Care Survey (NAMCS). Data for 2008–2009 are from combined files (in-person NAMCS and mail survey). Data for 2010–2011 are preliminary estimates (dashed lines) based on the mail survey only. Estimates through 2009 include additional physicians sampled from community health centers. Estimates of basic systems prior to 2006 could not be computed because some items were not collected in the survey. Data include nonfederal, office-based physicians and exclude radiologists, anesthesiologists, and pathologists.
SOURCE: CDC/NCHS, National Ambulatory Medical Care Survey.
Health Information Exchange (HIE)
Social Media

- How does your practice use it?
- How do your employees use it?
- Do you have policies?
Cloud-based services

- **Public Cloud**
  - EHR Applications
  - Private-label e-mail

- **Private Cloud**
  - Archiving of Images
  - File Sharing
  - On-line Backups

- **Hybrid**

Cloud Computing is taking all batch processing, and farming it out to a huge central or virtualized computers.

HIPAA regulations remain barriers to full cloud adoption.
Risk Assessment Methodology Flowchart (NIST)
### Risk Analysis - Example

<table>
<thead>
<tr>
<th>Risk Description /Threat and Potential Loss</th>
<th>Probability of Loss</th>
<th>Consequence</th>
<th>Risk Score</th>
<th>Risk Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePHI located on Desk top in an employees office is not routinely backed up.</td>
<td>4</td>
<td>4</td>
<td>16</td>
<td>High</td>
</tr>
</tbody>
</table>

Risk = Loss of PHI

(Identified in Gap Analysis)
# Sample Risk Analysis Template

<table>
<thead>
<tr>
<th>Impact</th>
<th>Likelihood</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High</td>
<td>Unencrypted laptop ePHI</td>
<td>Lack of auditing on EHR systems</td>
<td>Missing security patches on web server hosting patient information</td>
</tr>
<tr>
<td>Medium</td>
<td>Unsecured</td>
<td>Unsecured wireless network in doctor’s office</td>
<td>Outdated anti-virus software</td>
<td>External hard drives not being backed up</td>
</tr>
<tr>
<td>Low</td>
<td>Sales presentation on USB thumb drive</td>
<td>Web server backup tape not stored in a secured location</td>
<td>Weak password on internal document server</td>
<td></td>
</tr>
</tbody>
</table>
Risk Management - Steps

- Develop and implement a risk management plan
- Implement security measures
- Evaluate and maintain security measures
- Risk transfer, reduction, acceptance
Sanction Policy

Acceptable Use of PHI
- Minimum Necessary
- Sanction Exemptions

Disciplinary Actions

Sample sanction policy:
https://docs.google.com/document/d/1KSMZtdp9OAHILfTAKWdCkUR6jv6vI9mGIDYvv-5gQ1o/edit
Information System Security Review - Example

- Review of Security Incidents Response reports
- System user privileges grants and changes logs
- User-level system access logs, if available
- User level system activity logs, if available
- User level transaction log reports, if available
- Exception reports
- The required level of system activity logging and reporting capabilities, and the actual scope
Top 5 Recommendations

1. Ensure encryption on all protected health information in storage and transit. (at least de-identification)
2. Implement a mobile device security program.
3. Strengthen information security user awareness and training programs.
4. Ensure that business associate due diligence includes clearly written contract, a periodic review of implemented controls.
5. Minimize sensitive data capture, storage and sharing.
Meaningful Use Stage 2 and Stage 3 Security Requirements

- Security Risk Analysis with encryption assessment
- Secure Messaging for ambulatory practices
Effective Management of Security and Compliance

Find out where your business is weak

Determine the compliance and security needs & gaps

Put reasonable policies and business processes in place

Implement the right technologies & processes to help with enforcement

Re-evaluate on a periodic and consistent basis
## HIPAA Security Checklist

### Overview

<table>
<thead>
<tr>
<th>Security Management Process</th>
<th>Implementation</th>
<th>Requirement Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Analysis</td>
<td>Required</td>
<td>Policies and procedures to manage security violations</td>
<td>Penetration test, vulnerability assessment</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Required</td>
<td>Conduct vulnerability assessment</td>
<td>SIM/SEM, patch management, vulnerability management, asset management, helpdesk</td>
</tr>
<tr>
<td>Sanction Policy</td>
<td>Required</td>
<td>Implement security measures to reduce risk of security breaches</td>
<td>Security policy document management</td>
</tr>
<tr>
<td>Information System Activity Review</td>
<td>Required</td>
<td>Worker sanction for policies and procedures violations</td>
<td>Log aggregation, log analysis, security event management, host IDS</td>
</tr>
<tr>
<td>Assigned Security Responsibility</td>
<td>Required</td>
<td>Identify security official responsible for policies and procedures</td>
<td>Security policy document management</td>
</tr>
<tr>
<td>Workforce Security</td>
<td>Required</td>
<td>Implement policies and procedures to ensure appropriate PHI access</td>
<td>Mandatory, discretionary and role-based access control: ACL, native OS policy enforcement</td>
</tr>
<tr>
<td>Authorization and/or Supervision</td>
<td>Addressable</td>
<td>Authorization/supervision for PHI access</td>
<td>Mandatory, discretionary and role-based access control: ACL, native OS policy enforcement</td>
</tr>
<tr>
<td>Workforce Clearance Procedure</td>
<td>Addressable</td>
<td>Procedures to ensure appropriate PHI access</td>
<td>Mandatory, discretionary and role-based access control: ACL, native OS policy enforcement</td>
</tr>
<tr>
<td>Termination Procedures</td>
<td>Addressable</td>
<td>Procedures to terminate PHI access policy</td>
<td>Mandatory, discretionary and role-based access control: ACL, native OS policy enforcement</td>
</tr>
<tr>
<td>Information Access Management</td>
<td>Addressable</td>
<td>Procedures to terminate PHI access policy</td>
<td>Mandatory, discretionary and role-based access control: ACL, native OS policy enforcement</td>
</tr>
<tr>
<td>Isolation Health Clearinghouse Functions</td>
<td>Required</td>
<td>Policies and procedures to authorize access to PHI operations</td>
<td>Application proxy, firewall, mandatory UPN, SOCKS</td>
</tr>
<tr>
<td>Access Authorization</td>
<td>Addressable</td>
<td>Policies and procedures to authorize access to PHI</td>
<td>Mandatory, discretionary and role-based access control: ACL, native OS policy enforcement</td>
</tr>
<tr>
<td>Access Establishment and Modification</td>
<td>Addressable</td>
<td>Policies and procedures to separate PHI from other operations</td>
<td>Application proxy, firewall, mandatory UPN, SOCKS</td>
</tr>
<tr>
<td>Security Awareness Training</td>
<td>Addressable</td>
<td>Policies and procedures to authorize access to PHI</td>
<td>Mandatory, discretionary and role-based access control: ACL, native OS policy enforcement</td>
</tr>
<tr>
<td>Security Awareness Training</td>
<td>Required</td>
<td>Policies and procedures to grant access to PHI</td>
<td>Mandatory, discretionary and role-based access control: ACL, native OS policy enforcement</td>
</tr>
<tr>
<td>Training program for workers and managers</td>
<td>Required</td>
<td>Training program for workers and managers</td>
<td>Security policy document management</td>
</tr>
<tr>
<td>Penetration test, vulnerability assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIM/SEM, patch management, vulnerability management, asset management, helpdesk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security policy document management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log aggregation, log analysis, security event management, host IDS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Key Takeaways

- Risk Analysis is foundation for an effective security program
- ePHI elements drives risk analysis scope
- There is no silver bullet for risk management. It is a journey of continuous assessment and improvement
Additional Resources

- NIST - Risk Management Guide for Information Technology Systems SP800-30

- Small Practice Security Guide
How can you help us?

- Follow-us on social media
  - facebook.com/ehr20 (Like)
  - linkedin.com/company/ehr-2-0 (Follow us)
  - https://twitter.com/#!/EHR_20 (Follow)

- Next Webinar on Business Associate Assessment(3/21)

- http://ehr20.com/services/

We sincerely appreciate your referrals!
Thank you!!