Meaningful Use
Security Risk Analysis
Requirements

TIM CAMPBELL
MU OUTREACH AND EDUCATION CONSULTANT
NATIONAL INDIAN REC-CRIHB
SACRAMENTO, CALIFORNIA

EMMANUEL YENNEYEMB, CAC
K’IMA:W MEDICAL CENTER, HOOPA, CA

STEVE WILSON
ACCOUNT MANAGER
INFOGARD LABORATORIES
SAN LUIS OBISPO, CA
PRESENTATION OBJECTIVES

- ACA Relevancy
- CMS EHR Incentive Program Requirement
- How to Meet This Requirement
- Lessons Learned – Tribal Perspective
What is a Security Risk Analysis
ACA Relevancy

- Improving quality of patient care
- Lower costs of Health Care
- Fully integrated Electronic Health Record
- Less data entry errors, increased efficiencies
- Less duplication / double data entry
- Protects electronic patient information
- Meaningful Use requires sharing patient data in secured environment
Existing Security Requirements

Basis for protecting Patient Health Information

- Organizational Compliance
- HIPAA Security & Privacy rule requirements
  - 1. Security Awareness and Training §164.308(a)(5)
  - 2. Facility Access Controls §164.310(a)(1)
  - 4. Security management plan
- Staff Training / Annual IHS ISSA requirement
- IT system policies and procedures
- Implied trust by patients in your system
Data Breach Statistics

Since September 2009

- Over 20,000,000 individuals were affected by unauthorized access to ePHI
- Over 1.3 million people affected by Hacking or other IT related Incidents.
- Over 7 million people affected due to loss of media containing unprotected data
- Over 8 million people affected due to theft of electronic systems, devices and storage media containing unprotected data
SECURITY RISK ANALYSIS OBJECTIVE

- “Protect electronic health information created or maintained by certified EHR technology through the implementation of appropriate technical capabilities”

- “Conduct or review a documented security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.”
Why conduct Security Risk review?

- CMS Summit Panel Emphasizes Health IT Privacy, Security
  Last week at a CMS panel, several health IT experts stressed the importance of maintaining the privacy and security of patient data. A CMS Office of Civil Rights official said that health providers should perform risk analyses and develop mitigation strategies for addressing privacy and security risks, among other strategies. Clinical Innovation & Technology – IT Healthbeat 8/5/2013
Steps to conducting review

- Assemble a multi-disciplinary Team
- Review existing Health I/T systems
  - Physical Safeguards
  - Human Safeguards
  - Technical Safeguards
- Conduct review to HIPAA standards
- Identify Risks and Vulnerabilities to system
- Score risks – High / Medium / Low
- Develop plan to mitigate risks to acceptable level
# How to Evaluate a Risk

Risk = Impact * Likelihood

<table>
<thead>
<tr>
<th>Impact</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Critical</td>
</tr>
</tbody>
</table>

**Goal** = Understanding the probability of a threat occurrence being caused by a vulnerability and how to classify Low, Medium, High, Critical
Risk Analysis Workflow

- Incorporating an organization team review systems to identify “threats and vulnerabilities”
- Draft mitigation plan to address moderate to severe threats to acceptable level
- Conduct ongoing risk management program
- Continued education and training to all members of organizations
- Spread the word – Protect ALL Patient Health Information
Risk Management Team Example

- Facility Compliance Officer
- Security Officer Privacy Officer
- Information Technology Manager/Director
- Medical Records Manager
- Quality Control / Legal
- Clinic Administrator / Tribal Leadership
- Process to review / update policies
- Staff training plan
Most common barriers to MU

- Low E-Rx Measures?
- Incomplete Security Risk Analysis?
- Low Clinical Summary Measures?
- Awaiting system upgrades (Software & Equipment)

REC Services can help!
HIPAA Penalties

- HITECH Act mandates HHS conduct periodic privacy and security audits of HIPAA covered entities.
- OCR formally investigates HIPAA breaches via on site audits
- Maximum fines for HIPAA related breaches $1.5 million per organization
Meeting MU Requirements

Complete analysis by end of EHR report period in 2013
Attest Yes for each Eligible Provider
Keep copy of analysis in audit file
Treat Analysis as living document
Annual update analysis under each Stage
Clinic Limitations / Barriers

- Where do I begin?
- No formal risk management process in place
- Casual monitoring of Health IT system use
- “That’s the way we have always done it!”
- Limited time - assigned staff wears many hats
- Historical Institutional knowledge gets the job done, vs. policy spelling out who does what and how
- Bias viewpoint when reviewing own systems
Barriers & Best Practices

- Computer access – Policies & Procedures
  - Authorized / acceptable uses
  - Onsite uses computer resources
  - Monitoring Security Logs; policies update
  - Management Report results / frequency

- Re-connecting to the network – Policies / Controls
  - Remote off site network access – authorized uses
  - Unauthorized network connections (i.e. cell/iPads charging)
  - Secured data ports / wireless protocols in public areas
Lessons Learned

- Team approach to conduct risk analysis
- Review/update policies and procedures
- Enhance security awareness staff training
- Maintain patient’s TRUST in the system
- Need to know basis for staff access patient info
- Understand HIPAA breach requirements
- Protect and secure ALL Patient information
Tribal Perspective - Solutions

- **Start with Network Layout of Health I/T System**
  - Authorized users / workstation locations
  - Tracking matrix – software updates / equipment
  - Equipment replacement plan – back up servers

- **Staff – Security awareness training**
  - User profiles / EHR keys / P&P P Disaster Recovery Plan

- **Data Restoration Components**
  - Generator – back up power / Policy for down time
  - Data back ups – system restoration if needed
Preparing for Stage 2 MU

- Effective January 1, 2014
- Most sites will not reach until 2015
- Install re-certified EHR for Stage 2 measures
- Requires consideration of encryption/security of data at rest.
- NIST specified technology to render ePHI unusable, unreadable, or indecipherable to unauthorized individuals by encryption or destruction.
REC Support to Achieve Measure

1. Created in 2009 support Eligible Providers & MU
2. NIHB-REC services at no cost through 12/2013
3. Conduct on site Security Risk Assessments
5. Review & comment on existing Security Risk Analyses
Important Components of Stage 1 MU in 2013

- Meaningful Use Reports: 13 Core Measures, 5 Menu Set Measures, and 6 Clinical Quality Measures
- Privacy and Security Risk Analysis is one of the Core Measures
Presenter Contacts

- Tim Campbell, MU Outreach and Education Consultant
  National Indian Regional Extension Center
  Phone: (707) 889-3009
  E-mail tim.campbell@ihs.gov

- Steve Wilson
  Infogard Laboratories
  Phone (805) 783-0810
  E-mail: swilson@infogard.com

- Emmanuel Yenneyemb, CAC
  K’ima:w Medical Center, Hoopa, CA
  Phone: (530) 625-4261
  E-mail emmanuel.yennyemb@kimaw.org

E-mail General Questions: rec@crihb.net

www.crihb.org/rec
THANK YOU!