What You Don’t Know About Privacy & Security Can Hurt You

Introduction:
Nancie McAnaug, MSW
Center for Health Policy
MO HIT Assistance Center

Presenter:
Cora Butler, JD RN
Director of Commercial Operations
Primaris
Before we begin...

- Phone lines are now muted

- Find this or any previous webinar, go to http://www.EHRhelp.missouri.edu click on Webinars
MO HIT Assistance Center

Missouri’s Federally-designated Regional Extension Center

- University of Missouri:
  - Department of Health Management and Informatics
  - Center for Health Policy
  - Department of Family and Community Medicine
  - Missouri School of Journalism

- Partners:
  - EHR Pathway
  - Hospital Industry Data Institute (Critical Access Hospitals)
  - Missouri Primary Care Association
  - Missouri Telehealth Network
  - Primaris
What is our role?

- For providers who do not have a certified EHR system - We help you choose and implement one in your office

- For providers who already have a system - We help eligible providers meet the Medicare or Medicaid criteria for incentive payments
MO HIT Assistance Center
Now Serves Large Practices & Specialists

- Contact MO HIT Assistance Center for details and pricing
CME & AOA Credit
Now Available

- Instructions provided after today’s presentation
Disclosures

- The Office of Continuing Education, School of Medicine, University of Missouri is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

- The Office of Continuing Education, School of Medicine, University of Missouri designates this live Internet educational activity for a maximum of one AMA PRA Category 1 Credit™. Physicians should only claim the credit commensurate with the extent of their participation in the activity.

The learning objectives of this live Internet educational activity are:

- Choose an appropriate electronic health record for the practice, create a change team, redesign practice workflow and successfully implement transition to electronic records.
- Appropriately track quality measures in electronic health records and to create accurate reports of quality indicators; physicians will understand how to use indicators to improve patient outcomes.
- Identify potential privacy and security issues in individual practices that are utilizing electronic health records and provide tools for practices to use to assess their security measures to see if they are appropriate.
- Measure and track the way individual practices are reporting on the meaningful use requirements in the federal HIT Tech Act; understand additional clinical reporting requirements contained in meaningful use phases two and three.
- Appropriately design and implement patient portals for patients to access their health care information and learn how to better take care of their health conditions.

- The planning members and presenter for this activity have no commercial relationships to disclose.
Disclosures

This regional extension center is funded through an award from the Office of the National Coordinator for Health Information Technology, Department of Health and Human Services Award Number 90RC0039/01

Cerner and the University of Missouri Health System have an independent strategic alliance to provide unique support for the Tiger Institute for Health Innovation, a collaborative venture to promote innovative health care solutions to drive down cost and dramatically increase quality of care for the state of Missouri. The Missouri Health Information Technology Assistance Center at the University of Missouri, however, is vendor neutral in its support of the adoption and implementation of EMRs by health care providers in Missouri as they move toward meaningful use.
What You Don't Know About Privacy and Security Can Hurt You

Cora M. Butler, JD, RN, CHC
Director, Business Development & Commercial Contract Administration

Notice: Primaris is not acting in any capacity as the Federally designated Quality Improvement Organization (QIO) for Missouri during this presentation. Data used in this presentation was not obtained under the QIO contract Primaris holds with the Centers for Medicare & Medicaid Services (CMS). This presentation is not sanctioned or endorsed by CMS. The content of the webinars is based on material available in the public domain. The presentation is intended for educational purposes only. Primaris is not responsible for, and expressly disclaims all liability for, damages of any kind arising out of use, reference to, or reliance on any information contained herein. All presentation slides are the property of Primaris. No part of the presentation may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Primaris.
Presentation Goals

At the conclusion of this portion of the presentation, participants will be able to:

1. Identify the general requirements of the Risk Management Process contemplated by the HIPAA Security Regulations.

2. Identify the three categories of safeguards required by the HIPAA Security Regulations.

3. Discuss Required versus Addressable Implementation Standards.

4. Identify the factors that may be taken into account by a Covered Entity when determining the most appropriate approach to meeting the requirements of the HIPAA Security Regulations.

5. Discuss the types of documentation to be maintained by Covered Entity to demonstrate compliance.
HIPAA Security Regulations (45 CFR Part 160, 162, 164(a) and 164(c)) apply to Covered Entities that transmit or maintain ePHI (Protected Health Information in an electronic form).

Requires implementation of Security Management (Risk Management) “sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level” (164.308(a)(1)(ii)(B))
Security Management Standards

- **Administrative**
  - Designated Security Officer
  - Periodic Risk Assessment and Risk Mitigation
  - Workforce Training and Education

- **Physical**
  - Protecting facility and other places where patient data is accessed
    - Building Alarm Systems, Locked Offices, Screen Savers

- **Technical**
  - Technical controls that help ensure the integrity, confidentiality and availability of PHI
    - Strong, secure passwords; backed up data; virus scans; data encryption

- **Organizational Requirements**
  - Breach notification policies and Business Associate Agreements
Security Management Process

- The first standard under Administrative Safeguards section is the Security Management Process. This standard requires covered entities to:

  - "Implement policies and procedures to prevent, detect, contain and correct security violations."

- The purpose of this standard is to establish the administrative processes and procedures that a covered entity will use to implement the security program in its environment. There are four implementation specifications in the Security Management Process standard.

  1. Risk Analysis (Required)
  2. Risk Management (Required)
  3. Sanction Policy (Required)
  4. Information System Activity Review (Required)
Risk Analysis

A periodic technical and non-technical evaluation:

- Based initially on the standards implemented under the security final rule;
- Based subsequently in response to environmental or operational changes affecting the security of electronic protected health information; and
- Establishes the extent to which an entity’s security policies and procedures meet the rule.
- Documentation of compliance must be maintained. At a minimum:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HIPAA Standard-Implementation Feature</td>
<td>Organizational Policy that Addresses</td>
<td>Procedures that Address</td>
<td>Current Environment</td>
</tr>
</tbody>
</table>
Screening Questions
Security Program

Roles & Responsibilities

- Has your organization formally appointed a central point of contact for security coordination?
  - If so, who, and what is their position within the organization?
  - Responsibilities clearly documented?
    - Job Descriptions
    - Information Security Policy
Screening Questions
Security Program

External Parties

- Do you work with third parties, such as IT service providers, that have access to your patient's information?
  - Does your organization have Business Associate agreements in place with these third parties?
    - REC
    - IT Vendor
  - EHR Vendor
  - Attorneys, Billing Company

- What controls does your organization have in place to monitor and assess flow of information to third parties?

Workflows to track data movement
Screening Questions
Security Policy

Information Security Policy & Procedures

- Do you have documented information security policies and procedures?
  - Do you have a formal information classification procedure? Please describe it. In particular, how would patient data be categorized?
  - Have formal acceptable use rules been established for assets (hardware and software)?
  - Do you have formal processes in place for security policy maintenance and deviation?
Screening Questions
Risk Management & Compliance

Risk Assessment

- Do you have a process that addresses: the identification and measurement of potential risks, mitigating controls, and the acceptance or transfer of the remaining risk after mitigation steps have been applied?

Compliance with Legal Requirements - Identification of applicable legislation

- Does a process exist to identify new laws and regulations with IT security implications?

- Newsletters
- Webinars
- Associations
Screening Questions
Training & Awareness

During Employment – Training, Education & Awareness

– Have your employees been provided formal information security training?
– Have policies been communicated to your employees?
– Are periodic security reminders provided?

– New Employee Orientation
– Yearly Training
– Posters in Public Areas
– Email Reminders
Screening Questions
Personnel Security

- Background Checks
  - Does your organization perform background checks to examine and assess an employee’s or contractor’s work and criminal history?
    - Credential Verification
    - Criminal History
    - References
Screening Questions
Personnel Security

Prior to Employment - Terms and Conditions of Employment?

- Are your employees required to sign a non-disclosure agreement? If so, are employees required to sign the non-disclosure agreement annually?

Termination or Change in Employment

- Do you have a formal process to manage the termination and/or transfer of employees?
  - All Equipment is Returned
  - User ID's Disabled in EHR and Windows
  - Badges and/or Keys Returned:
Screening Questions
Physical Security

Secure Areas

- Do you have effective physical access controls in place that prevent unauthorized access to facilities and a facility security plan?
  - Are there plans in place to handle/manage contingent events or circumstances?
  - Is there a facility security plan?
  - How are physical access controls authorized?
  - Are there policies and procedures to document repairs and modifications to physical components of the facility that are related to security?
Screening Questions
Network Security

Application and Information Access Control - Sensitive System Isolation

- Describe your network configuration. Has your IT vendor provided information regarding how your EHR system is protected?
  - Are systems and networks that host, process and or transfer sensitive information ‘protected’ from other systems and or networks?
  - Are internal and external networks separated by firewalls with access policies and rules?
Screening Questions
Network Security

Application and Information Access Control - Sensitive System Isolation (continued)

- Is there a standard approach for protecting network devices to prevent unauthorized access/ network related attacks and data-theft?
  - Firewall between public and private networks
  - Internal VLAN
  - Firewall Separation
  - Separate WLAN Network
  - Secure Patient Portal
Screening Questions
Network Security

Encryption

- Is sensitive information transferred to external recipients?
- If so, are controls in place to protect sensitive information when transferred?
  - Secure VPN Connection with EHR and/or IT Vendors or Email Encryption
Screening Questions
Network Security

Vulnerability Assessment
- How often do you perform periodic vulnerability scans on your information technology systems, networks and supporting security systems?
  - Internal Assessments
  - Third party Assessments
  - Automated Assessments

Monitoring
- Are third party connections to your network monitored and reviewed to confirm authorized access and appropriate usage?
  - VPN Logs
  - Server Event Logs
  - EHR logging
  - Automated Alerts
  - Regular Review of Logs or Reports
Screening Questions
Logical Access

Identity & Access Management
- Do you have a formal access authorization process based on 'least privilege' and need to know?
  - Role-based permissions
  - Limited access based on specific responsibilities
  - Network access request form
- How are systems and applications configured to restrict access only to authorized individuals?
  - Use of unique ID's and passwords.
    - Minimum Password Length
    - Complexity
    - History
    - Change/Lockout
Screening Questions
Logical Access

Identity & Access Management (continued)

- Is there a list maintained of authorized users with access to operating systems?
  - Active Directory user lists, within EHR application
  - Excel spreadsheet of users, HR file.
- Does a list of 'accepted mobile devices' exist based on testing?
  - Are accepted mobile devices tested prior to production use?
Screening Questions
Logical Access

Identity & Access Management (continued)

- Is sensitive information removed from, or encrypted within, documents and or websites before it is distributed?
  - Use of Patient Portal for distribution
  - De-identifying of sensitive information prior to being distributed
Screening Questions

Logical Access

Identity & Access Management (continued)

- Is software installation restricted for desktops, laptops and servers?
  - Restricted User access to workstations, Group Policy enforcement, Administrative privileges on servers limited?
  - Automatic logoff of workstations?
  - EHR system?
- Is access to source application code restricted? If so, how?
- Is a list of authorized users maintained?
Screening Questions
Logical Access

Identity Management

- Are user IDs for your system uniquely identifiable?
  - Any shared accounts at all?
    - Hard coded into applications
    - Someone is sick or unavailable
    - Emergency access to sensitive information
Screening Questions
Logical Access

Entitlement Reviews

- Do you have a process to review user accounts and related access?
  - Manual process of reviewing Human Resource records to user accounts in Active Directory and EHR
Screening Questions
Operations Management

Antivirus
- Has antivirus software been deployed and installed on your computers and supporting systems?
  - Product Installed
  - Centrally Managed
  - Updated Daily

Security Monitoring
- Are systems and networks monitored for security events? If so, please describe this monitoring.
  - Server and networking equipment logs monitored regularly.
    - Servers
    - Routers
    - Switches
    - Wireless AP's
Screening Questions
Operations Management

Media Handling

- Do procedures exist to protect documents, computer media, from unauthorized disclosure, modification, removal, and destruction?
- Is sensitive data encrypted when stored on laptop, desktop and server hard drives, flash drives, backup tapes, etc.?
- Data at Rest - Is data encrypted?
  - Backups
  - EHR server
  - Mobile devices
  - SD Cards
Screening Questions
Operations Management

Secure Disposal

- Are there security procedures for the decommissioning of IT equipment and IT storage devices which contain or process sensitive information?
  - use of Shred-IT
  - Retire-IT
  - Wiping
  - NIST 800-88

Segregation of Computing Environment

- Are development, test and production environments separated from operational IT environments to protect production applications from inadvertent changes or disruption?
Screening Questions
Operations Management

Segregation of Duties

- Are duties separated, where appropriate, to reduce the opportunity for unauthorized modification, unintentional modification or misuse of the organization's IT assets?
  - Front desk duties separated from accounting?
  - Nurse duties separated from Doctor's?
Screening Questions
Operations Management

Change Management

- Do formal change management procedures exist for networks, systems, desktops, software releases, deployments, and software vulnerability patching activities?
  - Changes to the EHR?
  - Changes to the workstations and servers?
  - Appropriate testing, notification, and approval?
Screening Questions
Incident Management

Process & Procedures

- How do you identify, respond to and mitigate suspected or known security incidents?
  - Incident Form filled out as a response to an incident
  - During the investigation of a security incident, is evidence properly collected and maintained?
  - Chain of custody and other computer forensic methodologies followed by internal and/or external parties?
Screening Questions
Incident Management

Process & Procedures (continued)

- Are incidents identified, investigated, and reported according to applicable legal requirements?
- How are incidents escalated and communicated?
  - Documented process for escalation to management and even outside authorities.
Screening Questions
Business Continuity Management

Disaster Recovery Plan & Backups

- Do you have a mechanism to back up critical IT systems and sensitive data? i.e. nightly, weekly, quarterly backups? Taken offsite?
  - Have you had to restore files after a systems outage?
- Does a Disaster Recovery plan exist for the organization and does it consider interruption to, or failure of, critical IT systems?
  - Are disaster recovery plans updated at least annually?
  - If not, has the backup and restoration process been tested?
People & Processes

Asset Management Category- Security Policy

- Threat-Vulnerability Statement
  - Management has not set a clear policy direction in line with business objectives or demonstrated support for, and commitment to information security.

- Recommended Control Measures
  - Information security policy, approved by management in accordance with business requirements and all relevant laws and regulations.

- Existing Control
  - No existing IS Security Policy in place
People & Processes

Asset Management Category- Personnel Security

- Threat-Vulnerability Statement
  - Background verification checks are carried out and management is aware of academic, professional, credit, or criminal backgrounds of most employees, contractors and third party computer system users.
- Recommended Control Measures
  - Background verification checks on all candidates for employment, contractors and third party computer system users are carried out in accordance with regulations and ethics, the classification of the information to be accessed, and the perceived risks.
  - Existing Control-References are verified for all employees

### Existing Control Effectiveness

<table>
<thead>
<tr>
<th>Existing Control Effectiveness</th>
<th>Exposure Potential</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partially Effective</td>
<td>Medium</td>
<td>Likely</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Existing Control Effectiveness</td>
<td>Exposure Potential</td>
<td>Likelihood</td>
<td>Impact</td>
<td>Risk Rating</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------</td>
<td>--------------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Not Effective</td>
<td>High</td>
<td>Not Likely</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

**Technology**

- **Asset Management Category- Training and Awareness**
  - **Threat-Vulnerability Statement**
    - Applications and technology solutions are not correctly and securely used since a training curriculum for employees has not been established.
  - **Recommended Control Measures**
    - A training curriculum for employees be established to educate and train users for correct and secure use of applications and technology solutions.
  - **Existing Control**
    - The use of technology regarding a training curriculum is not currently being utilized.
Findings & Remediation

High and Medium Risks Findings and Remediation

- Information around risks and related control options are not presented to management before management decisions are made.
  - Risk Rating-High
- Existing Control Measures Applied
  - No prior Risk Assessments conducted
  - REC helping to provide a foundation by utilizing this Security Risk Assessment tool as a starting point.
Findings & Remediation

- High and Medium Risks Findings and Remediation (continued)
  - Recommended Control Measures.
    - Risk Assessments are conducted to identify, quantify, prioritize and manage risks through acceptance and objectives.
    - Ensure the Risk Assessment is accurate with all the information that has been filled out as well as the risk ratings, that have also been completed based on the information provided.
Findings & Remediation

High and Medium Risks Findings and Remediation (continued)

- Recommended Control Measures.
  - After verifying accuracy of the information, the Medium and High Risk items from the Findings-Remediation tab should be addressed by making the necessary business decisions on whether to mitigate, transfer, or accept the risks. It is recommended to mitigate risks that are easy to address
  - It is important to continue the Risk Assessment process by assessing the additional risks to your facility.
ONC’s - Guide to Privacy and Security of Health Information - Tools

Guide to Privacy and Security of Health Information

Tools
- Security Risk Assessment Tool. This tool can be used to help your practice conduct a security risk assessment. Available at: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
- ONC’s 10 Best Practices for the Small Health Care Environment. This guide provides information to help smaller health care practices learn about security measures they may need to consider as they use health information technology. Available at: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
- ONC’s Cybersecurity Checklist. This checklist provides 10 simple best practices that should be taken to reduce the most important threats to the safety of EHRs. Available at: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
- HRSA Health IT Adoption Toolbox. HHS’ Health Resources and Services Administration (HRSA) compiled planning, implementation, and evaluation resources to help health centers, safety net providers, and ambulatory care providers implement health IT applications in their facilities to meet administrative, IT, and clinical quality objectives. The Health Information Technology Toolbox is available at: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Education & Training Materials
- HIPAA Privacy Rule Training Materials. To find educational materials to help you learn more about the HIPAA Privacy Rule, visit the OCR HIPAA Training Materials page.
- HIPAA Security Rule Training Materials. To find educational materials to help you learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic personal health information, visit the OCR Security Rule Guidance page.
- Uses & Disclosures: A Provider’s Privacy Guide. Uses and disclosures of health information, a two-page fact sheet about when protected health information can be used or shared without a patient’s express permission. Available at: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

What You Don't Know About Privacy and Security Can Hurt You

QUESTIONS?
MOHIT JumpStart Series
Online Community & Collaboration

Register at: www.bit.ly/MOHITREC
Referral code: JumpStart

• Connect with JumpStart Participants
• Access Presentation Materials, Tools, Information
• Q&A with Presenter
• Discussions, Knowledge Sharing
Your Phone Line is Now Open!

- Click on the “hand” on your computer to ask a question & press * 6 to unmute your phone.
To Receive CME Credit

1. Go to: [http://www.EHRhelp.missouri.edu](http://www.EHRhelp.missouri.edu)

1. Click on [Webinars](#) on our home page

1. Look for today’s Webinar title

2. Download pdf or complete online questionnaire

1. Submit or fax completed questionnaire to 573-882-5666 by: Friday, March 9, 2012
To Receive AOA Credit

1. Go to: http://www.EHRhelp.missouri.edu

1. Click on **Webinars** on our home page

1. Look for today’s Webinar title

2. Download pdf questionnaire by
3. **Friday March 9, 2012**
4. Mail or fax completed questionnaire to the American Osteopathic Association
Upcoming Advanced Webinar

New Time: 5:00 – 6:00 p.m.

July 12th
Transform Your Practice Through Social Learning

Mike Levinger
President, CEO and Founder
The HIT Community
June 21st

"Utilizing Your EHR"

Presenter:
Margalit Gur-Arie
EHR Pathway
For More Information:

- Website:  http://ehrhelp.missouri.edu
- E-Mail:  EHRhelp@missouri.edu
- Phone:  1-877-882-9933