Peek-A-Boo: EHR Access and Compliance

HCCA Compliance Institute
Orlando, FL
April 10, 2011

Miriam Murray, Sava Senior Care
Andrea McElroy, Aurora Health Care

This is a medical record, can I show it to her?
Audience Poll...

- Participants from acute care?
- Participants from post-acute care?
- Participants from an integrated health system?
- Participants who have or are implementing an electronic health record?

Today’s Objectives

- Understand challenges facing compliance implementation and access to electronic health record systems
- Monitor appropriate usage and actions taken for non-compliance
- Benefits of electronic health record access by alternative care settings (SNF, ALF, etc)
The Magic of the EHR

Benefits Across Care Settings

- Standardizes the information passing between care settings.
- Reduces risk of inaccurate information
- Decreases response time between care settings
- Verifies role-based access to specific personnel in each care setting
- Builds relationships between care settings
The Magic of the EHR

- Coordination among our provider departments
  - Admissions
  - Nursing
  - Radiology
  - Laboratory
  - Pharmacy
  - Therapy Services
  - Care Management/Social Services

Privacy/Security Magic of the EHR

- Automated and Secured Access
  Authentication
- Data Integrity
- Auditable
  - Access
  - Data changes
**Torn from the Headlines**

- **April, 2010**: DOJ reports first person (a physician) sentenced to 4 months prison for accessing records of co-workers and celebrities without a valid reason.

- **June, 2010**: Five CA hospitals fined a total of $675,000 by CA Dept. of Health for failing to prevent employees from viewing private patient data of 204 patients. Largest individual hospital fine...$250,000. [SC Magazine](#)

- **November, 2010**: Seacoast Radiology notifies New Hampshire AG and 231,400 individuals (January, 2011) of unauthorized third party access to a patient billing server that was not encrypted. The access occurred through an internet connection that was hacked into by a group of video gamers playing “Call of Duty”. While there is no evidence to suggest information was accessed the possibility could not be excluded.

- **January, 2011**: University Medical Center of Tucson fires 3 employees and releases contracted registered nurse for snooping in electronic medical record of Rep. Gabrielle Gifford.
Challenges to Implementation

- Documentation and signature requirements
  - Templates
  - Copy/carry forward content
  - Data Integrity
- Scope of Practice
- Order-sets
- Special security requirements
- Role-based access
- Access Monitoring/Auditing

EHR - Approaches to Access

- Pre-established system roles
  - Physician
  - Admission clerk
- User-defined role
- Combination
**EHR - Why Monitor? Why Audit?**

To ensure patient privacy
- Policy enforcement
- Compliance with HIPAA Privacy Rule
- Compliance with HIPAA Security Rule
- OIG Elements of a Compliance Plan

**HIPAA Privacy Rule**

Safeguards 164.530(c)(1)(ii)
A CE must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards.

Sanctions: 164.530(e)(1)
A CE must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies of the CE or the requirements of this subpart.
HIPAA Security Rule

General Rules 164.306(a)(4)
CE’s must…ensure compliance with this subpart by its workforce.

Technical Safeguards 164.312(b)
*Standard: Audit Controls.* Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Challenges to Assuring Compliance

- Organizational size
- Education
- Notion of “Entitlement”
- What is a reasonable sample when auditing?
- Access Control
How can we assess Compliance?

- Complete a “Self-Assessment” of company confidentiality protections
  - Ensure policies and procedures on privacy/security of company confidential and protected health information (PHI)
  - Controls that support policies on confidentiality are in place
    - Who has access
    - What level of access
    - Safeguards in place for unauthorized access, improper destruction, improper release
  - Review for potential circumventions to controls
  - Method – Observation, Interview, Document Review

Sample Self-Assessment Questions

- What health information is viewable in public areas (including ability to “shoulder surf”)?
- What process is used to obtain release of information.
- What process is used to ensure that employees, vendors, etc. sign a confidentiality statement?
- What process is followed when there is a suspicion of a violation of confidentiality?
Small Group Scenario #1

Using Scenario #1 work with your group to come to consensus on the following:

1. Develop your own self-assessment questions to rate the entity’s apparent level of assurance on a scale of 1 (excellent) to 5 (poor).
2. Assign a risk weight to each of the responses based on the scenario. Risk ratings 1 (low), 2 (medium), 3 (high).
3. Multiply the two scores to determine areas of focus to improve compliance
4. Any additional self-assessment questions that come to mind?

Scenario #1

Health System X has developed a mobile clinic for homeless individuals living in a metro area. Caregivers will provide general medical care for minor illness and injury, rehabilitation services, medication administration, immunizations, health counseling, etc. Documentation will be completed on a dedicated laptop which the caregiver uses “on the street”, using an electronic documentation system. Information will be uploaded via public wi-fi to the parent company. At times there is a need for exchange of information between law enforcement and the care team. Additionally, patients are provided with printed information such as an exercise program, medication side effects, etc.
Group Discussion 1

- What self assessment questions were asked?
- What weaknesses were identified?
- What are the next steps to address the weaknesses?
  - Change in policies?
  - Change in access control?
  - Additional training needs?

Scenario #2

The activity director of a residential facility for multiply handicapped individuals wants to take several complex need individuals on a day long excursion to a summer festival. Because of the length of the event, the director and the volunteers going along will need to access medical information regarding medications, the need for monitoring vital signs, diet information, etc. This is a one time event involving family so the facility does not request the family volunteers to sign any waiver or confidentiality statement.
Group Discussion 2

- What self assessment questions were asked?
- What weaknesses were identified?
- What are the next steps to address the weaknesses?
  - Change in policies?
  - Change in access control?
  - Additional training needs?

Challenges to Access Control

- Infinite “temporary access”
- Infamous “inherited access”
- Un-denied “shared access”
- Failure of “revoke and re-establish access”
- “Sneaky access”
Rooting Out Access Problems

- Observe, Interview, Audit
- Inquire about complaints and review resolution
- Determining if access behavior warrants investigation
  - Data Mining vs. finding the needle in a haystack

Scenario #3

You are the Compliance and Privacy professional at a hospital trauma center in a small community. You hear a news media report that the Mayor’s wife has been shot and taken to your hospital. The charge nurse on duty at the time of arrival of the wife has already spoken to the media.
Group Discussion #3

- What concerns do you have?
- What actions, if any would you take?
- What benefits can come from taking action?

Scenario #4

A physician is using his access to the hospital system for a research project he is conducting. His office staff is using the physician's username and password to access the hospital records as well for the services the physician performs at the hospital for billing purposes.
Group Discussion #4

- What concerns do you have?
- What actions would you take?
- Corrective actions for the organization to implement
- Other thoughts???

Monitoring/Auditing

- Create reports to help in monitoring access and system changes
  - Brainstorm conditions
  - Test for accuracy
  - Test for false positives
  - Identify opportunities to further limit
  - Re-test for false positives
What are the audit trails or reports available in your EHR(s)?

- Do the audit trails vary by system?
- Can you access all the audit trails?
  - If not, how do you audit access?
- What type of information is available from audit reports?
- Can you obtain a report of users and their positions?
- Can the audit trail tell you who (what patient) was accessed?
- Can the audit trail tell you what changes were made to the record?

Auditing and Monitoring of Access

Who do you look at?
- Users
- Vendors

What do you look for?
- Employees
- Persons of Interest

How often do you look?
Monitoring/Auditing

- Something is better than nothing
- Use technology to minimize human resource requirements
- Be creative
- Track and trend to identify educational needs

Questions?
Thank You!!!

Contact Information:

Miriam Murray
678-443-7134
MBMurray@SavaSC.com

Andrea McElroy
414-299-1714
Andrea.McElroy@aurora.org

References

Protecting Confidentiality, 2001, Joint Commission on accreditation of Healthcare Organizations

Copy Functionality Toolkit, 2008, American Health Information Management Association

Compliance Pitfalls to Avoid When Implementing EHR Systems, 2-Part Series, October, 2010, SINAIKO Healthcare Consulting for HCCA