RBAC and HIPAA Security

Uday O. Ali Pabrai, CHSS, SCNA
Chief Executive, HIPAA Academy
Session Objective

• Challenges
• HIPAA Requirements
• Seven Steps to HIPAA Security
• Access Control
• RBAC
  – Information Access Control Security Policy
  – RBAC System Characteristics
  – Developing a RBAC Solution
  – Getting Started
  – Implementation Challenges
Challenges

• Increasing demand for moving mission critical applications on-line
  – This requires access to PHI based on the user’s function

• Identities of authorized users and transactions are constantly changing
  – Organizations require a solution that supports robust authorization capabilities

• Number of users and applications is increasing within most organizations
  – Requires a scaleable solution to manage authorized access
Privacy’s Minimum Necessary

• HIPAA Privacy Rule requires that the covered entity must identify:
  – Who needs access to PHI
  – What type of access and if there are to be any restrictions associated with such access

• Central aspect of the Privacy Rule is the principle of “minimum necessary” use and disclosure
Security’s Access Control

• The Final Security Rule requires these standards to be implemented:
  – **Information Access Management**
    • Access Authorization
    • Access Establishment and Modification
  – **Access Control**
    • Unique User Identification
    • Emergency Access Procedure
    • Automatic Logoff
    • Encryption and Decryption
Seven Steps to HIPAA Security

The Seven Steps to HIPAA Security Compliance

1. Security Responsibility
2. Risk Analysis
4. Remediate
5. Secure Third Parties
6. Training
7. Evaluate

- Confidentiality
- Integrity
- Availability

Vital Assets

e-PHI

HIPAA Shield
Access Control

- Access control, also referred to as authorization, refers to:
  - What the user can do
  - What the user can access

- Access control enables businesses to restrict individual access to resources
  - Allowing access only by privileged entities with a business need to access

- Defense-in-depth:
  - Authentication
  - Access control
Types of Access Control

- Role Based Access Control (RBAC)
- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Context Based Access Control
• **What is RBAC?**
  RBAC allows disclosures to authorized users while preventing disclosures to unauthorized users

• **Stems from:**
  – Minimum Necessary Standard for HIPAA Privacy
  – Access Control Standard in Security Rule
Why RBAC?

• Using RBAC has several advantages compared to other access control mechanisms
  – Simplifies access definitions, auditing and administration of security access rights
  – The delegation of access rights does not occur at the discretion of any user (even the security administrator)
  – Users are given only the access privileges necessary to perform their duties or role
  – Updates can be done to roles instead of updating privileges for every user on an individual basis
Security Policy

• First develop the Information Access Control Security Policy
• Objective of policy
  – The confidentiality and integrity of information assets stored within systems must be protected
  – Only authorized users must have access to specific defined, documented and approved systems and applications
• Clearly articulate RBAC requirements
Getting Started with RBAC

• **Step 1:** Define all roles within the organization

• **Step 2:** Next step is to do a complete inventory of all active applications

• **Step 3:** Identify the RBAC solution to meet objectives

• *Carefully plan the implementation to ensure successful operation!*
RBAC System Characteristics

The characteristics of an RBAC system are:

- “Roles” map to organization structure
- Each “role assigned minimum access privileges
- Each employee then assigned one or more roles that determine their level of access
RBAC Solution Requirements

• Any RBAC product solution must support requirements such as:
  – Scalability
  – Inheritance
  – Multiple roles
  – Types of access
  – Auditing and logging
  – System administration
  – Customization
Implementation Challenges

• RBAC policies and procedures must be clear, complete and rigorously followed

• Specifically:
  – Lay out the procedures for access requests
  – Establish an approval policy for modification to procedures
  – Establish an approval policy for user ID requests

• Establish a firm timeline for RBAC implementation
Thank You!

For more information, contact:
- Bob Matthews
  - 877.899.9974 x20
- Scott Louden
  - 877.899.9974 x22
- Uday O. Ali Pabrai
  - Pabrai@HIPAAAcademy.Net

For FREE PDF on RBAC and HIPAA Security, Email Your Testimonial To: Scott.Phillips@HIPAAAcademy.Net