Session Objectives

• Review terminology and the basic concepts of Identity and Access Management (IAM)
• Examine the challenges
• Discuss best practices
Terminology

• **Provisioning** is the process of coordinating the creation of user accounts

• **Access rights, privileges, and/or entitlements**
  – ... mean about the same thing; pick a term and be consistent
  – What data a user can access (permitted access)
  – What actions a user can take:
    • Read only
    • Write, edit, delete
Challenge – Onboarding

**User:** “I need access.”

**Help Desk:** “Fill out an access request form.”

**User:** “Where can I find the access request form?”

**Help Desk:** “It’s on the intranet.”

**User:** “But I don’t have network access.”

**Help Desk:** “Too bad. So sad.”
Manager: “I need access for a new employee.”
Help Desk: “When will the new employee start work?”
Manager: “They started yesterday.”
Help Desk: “It’ll take two days to set up all the access.”
Manager: “I need their access now. Otherwise, they will not be able to do their job.”
Help Desk: “When did you know they were starting?”
Access Control Steps

Basic steps in user identification and access control

Source: CISSP All-in-One Certification Exam Guide, by Shon Harris
User IDs

• User IDs are created on some set of rules
• However, when based upon a user’s name could cause issues in the future or when two users have similar names, for example, **Tom Walsh** and **Tim Walsh**; one is:
  
  twalsh@companyname.org

• The other ends up being:
  
  trwalsh@companyname.org

  - Or -

  twalsh1@companyname.org
Three methods of authentication:

1. **Something you know**
   - Password, PIN, mother’s maiden name, pass phrase

2. **Something you have**
   - Smart card, token, key, swipe card badge, mobile phone

3. **Something you are (biometric)**
   - Fingerprint, voice scan, iris scan, retina scan

*Two-factor or dual factor is a combination of #1 and #2 = a Best Practice*

**NOTE:** User ID and password is NOT two-factor
Authorization

• User based
  – A new user’s privileges are established by copying another user’s privileges; “Set Ann’s to be just like Mary’s access.”

• Role based
  – Any changes to the privileges within a particular role automatically change everyone’s privileges within that same role

• Content based (or project based)
  – Access privileges to data are allowed or denied based upon the content requested to be accessed or displayed

*Often access is a combination of one or more methods*
Role Based Access Control (RBAC)
- Assigning access privileges based upon pre-established set of rules
- Sometimes called “security groups” or “user groups”
- Intended to reduce the time and cost of user administration

Not beneficial if:
- There is only one person in a role (CFO, CIO, CEO, CNO, etc.)
- There are a small number of users of an application or system
- Small organization where each employee fills multiple roles
### Role Based Access Control

**Key to Access Codes:**
- **S** = System Administrator
- **C** = Enter Data/Create
- **E** = Update/Chart/Modify
- **V** = View only
- **X** = General access needed

All other requests should be reviewed by data owners or managers before they are fulfilled.

<table>
<thead>
<tr>
<th>Department</th>
<th>Position Title</th>
<th>Outlook Email</th>
<th>Internet</th>
<th>ADT (scheduling, billing)</th>
<th>CPSI ChartLink</th>
<th>Electronic Health Record</th>
<th>Coding</th>
<th>PACS</th>
<th>Pharmacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>2nd Floor Med/Surg</td>
<td>Charge Nurse</td>
<td></td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>V</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd Floor Med/Surg</td>
<td>Educator</td>
<td>X</td>
<td>X</td>
<td>C</td>
<td>C</td>
<td>V</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd Floor Med/Surg</td>
<td>Med Tech/Unit Coordinator</td>
<td></td>
<td></td>
<td></td>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd Floor Med/Surg</td>
<td>Manager</td>
<td>X</td>
<td>X</td>
<td>C</td>
<td>C</td>
<td>V</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd Floor Med/Surg</td>
<td>Staff Nurse</td>
<td></td>
<td></td>
<td></td>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admitting</td>
<td>Clerk</td>
<td>X</td>
<td>X</td>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admitting</td>
<td>Senior Clerk - Lead</td>
<td>X</td>
<td>X</td>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Billing/Patient Accounts</td>
<td>Clerk I (File Clerks)</td>
<td>X</td>
<td>X</td>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Billing/Patient Accounts</td>
<td>Coordinator</td>
<td>X</td>
<td>X</td>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Billing/Patient Accounts</td>
<td>Manager</td>
<td>X</td>
<td>X</td>
<td>S</td>
<td></td>
<td>S</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
User changes and account management:

– Department or job responsibilities
  • New privileges added while the old privileges may remain
  • Users rarely ask IT to terminate their old, unneeded access privileges
  • Access to a certain system or data does not imply that a user is authorized to view or use all the information on that system

– Last name changes

– Leave of absence

– No longer a need to access an application or system
Challenges
Identity and Access Management

• Information about users’ identity and accounts may be scattered across the organization
  – Different geographical locations
  – Too many applications and systems to track
    • Users may require access rights to multiple applications/systems
  – Some are departmental systems not managed by IT, and accounts are created by different administrators
    • Pharmacy, Lab, Radiology, Biomed, etc.
  – Deactivation of all IDs across all systems can be a challenge

• Users can be employees and nonemployees
Nonemployees (1)

Workforce Members

- Medical students, nursing students
- Volunteers
- Contracted nurses (nurse registry, PRNs, temps, etc.)
- Service providers (Transcriptionists, day registry, cancer registry, hearing screeners, scribes, etc.)
- Consultants or vendor support staff working onsite or offsite
- Business associates and vendors
Nonemployees (2)

Other Covered Entities

• Credentialed providers that are affiliated with a hospital or health system through the Medical Staff office:
  – Physicians, physician assistants, nurse practitioners, and allied health professionals
  – Hospital based physicians – contracted (hospitalists, anesthesiologists, etc.)

• Private practice physicians/physician groups and their staff
  – But not part of the hospital’s medical staff

• Health insurance companies
  – Nurse or case managers from insurance companies
  – Their billing auditors
Nonemployees (3)

Other Third Parties

• Professional fee billers (Business associates to the physicians)
• Auditors (HIM and coding audits, financial auditors)
• Medical Staff Students (Business associates to the physicians)
• Federal and State agencies – regulatory agency personnel
• Accreditation surveyors (Joint Commission or Lab, etc.)
• External legal counsel
Password Management

• System administrator accounts
  – “The keys to the kingdom”
  – Generic logon accounts used at the highest level of privilege

• Multiple user IDs and passwords create problems; users will:
  – Write down their passwords
  – Reuse the same password on several systems
  – Forget their passwords, resulting in calls to the Help Desk / Service Desk
Best Practices
User Provisioning

• **Automatic provisioning and automatic deactivation**
  – Automated processes help ensure consistency for employees
  – Tied to HR/payroll system; creates or deactivates the user’s account in Active Directory based upon a personnel action
  – Organizational units (OUs) in AD based on users
  – Workflow (new employee is entered into HR/Payroll system, IT sets up network access (user account in Active Directory (AD), then standard applications (by location, department, and role)
  – Manager requests additional access to other non-standard applications (management by exception)
Unique User IDs

• Once a user ID has been assigned, it should not be reused (pros and cons to this)
• User IDs are uniform across systems and platforms and are not based upon the user’s name, department, or employee number
• Use only letters and numbers instead of names
  – Reference SAMPLE on next slide
Assign unique user IDs based upon user status, for example:

- **A** = Associate (or employee) + 5 digit employee number
- **C** = Contractor
- **P** = Physician
- **S** = Student
- **T** = Temp or training user ID
- **V** = Volunteer

... followed by a numeric sequence, to create a unique ID; for employees, it could be their five digit employee number:

**A62120** *(where “62120” = the employee number)*
Authorization

• **Best practices for system administrators include:**
  – Two separate user IDs:
    1) Their normal employee user access
    2) Their system administrator access
  – Make passwords more stringent than user passwords
  – Log of all of their activities (account modifications in particular)
  – Conduct periodic background checks
    • People change over time
Avoid collecting signed agreements

Instead try...

“Agreement by Default”
Managing User Accounts

• IT and/or system administrators are automatically notified by the HR/payroll system when an employee’s account should be changed or inactivated
  – Resignation or termination
  – Leave of absence
  – Leave without pay (disciplinary action)

• Auto expiration of access for nonemployees
  – Contractors, students, vendors, temps, etc.

• Establish termination procedures to remove user access (physical and logical) in a timely fashion
Managing User Accounts

• Create a certification or review process of privileges
  – Provide managers a list of their workers (employees and nonemployees) with an inventory of applications and systems the user can access and their access privileges
  – Require management to review and approve
    • Sign off on the report
    • Flag questionable access privileges for possible removal
  – Focus the review on applications and systems that pose a significant business risk
Managing User Accounts

Message for Quarterly Access Review

Below is our current list of authorized users from your office with access privileges to [Hospital] information systems data. Because of the HIPAA Security Rule (§164.312(a)(1) Access Control) and the HIPAA Audit Program Protocol, we are required to:

- Perform user access reviews to our systems and applications on a periodic basis
- Identify users who should or should not have access to our systems
- Remove or change user access privileges on a timely basis

It is important that you please review the list of your users and please place a check mark to indicate a user’s access as either: “Active” or “Remove.”

The form must be returned within 10 working days of the letter date in order for your users to remain active. Otherwise, we will be forced to remove access for all of your users.

Please contact the [IT Help Desk / IS Service Desk] at: ______ if you have any questions or concerns. Thank you.

Please remember to notify the [IT Help Desk / IS Service Desk] immediately when an employee no longer needs access. As a covered entity, your practice must also comply with the HIPAA Security Rule.
Password Management

• Synchronization (network/AD versus clinical application when it is not AD aware)
• Create a self-service portal (application) for password resets
• Implement single sign-on (SSO), but be aware that:
  – Password compromise has a greater impact
  – Legacy applications may require specialized code to support SSO
• Implement “Tap-n-go” badges
Unlocking User Accounts

- **Password resets**
  - Good judgment should be exercised when validating the identity of users requesting their passwords be reset or when unlocking a disabled user account
    - Caller ID
    - “Frequent flier” – Known person who calls often for help
    - Ask someone to vouch for the caller
  - Resets should be documented appropriately in the IT Help Desk (or Service Desk) ticket system
Audience Discussion
Discussion Items

• User access privileges should be periodically reviewed by application owners and/or department managers to ensure they are appropriate. How can this help reduce the harmful effects of ransomware?

• Why would generic user accounts need to be used?

• Prohibit concurrent logons with the same User ID – Why?
Questions
Tom Walsh
Founder and Managing Partner
tw-Security.com

boston.healthprivacyforum.com | #hitprivacy