The Security Informatics Nurse Specialist Role
Introduction

- Claribel Sawyerr, MSN/MPH, RN-BC
- Kim Stevens, MSN, RN
- Susan Martin, RN, JD, CIPP/G, CPHIMS

Disclaimer – No conflicts of interest to disclose
Polling Instructions

Answer choices:
A = Nurse Informaticists
B = IT Department
C = Other
D = Don’t Know
Polling Question

In your organization, who creates EHR end-user accounts?

- Nurse Informaticist
- IT Department
- Other
- Don't know
What are the security features of your EHR system?
Create

50% IT Department
25% Security Team
25% DBA/Engineer

Maintain

63% IT Department
37% Data/Application Analyst

Deactivate

75% IT Department
25% Data/Application Analyst

Similar Processes

Creation Requests
Deactivation Requests
Role-Based Access Control (RBAC)
Objectives

- Describe the role of the security informatics nurse specialist related to end-user access, use and security of EHR
- Identify key functional areas for security INS
- Describe the laws and regulations governing the protection of electronic protected health information (ePHI)
- Discuss administrative, physical & technical safeguards for ePHI
- Describe role-based access control (RBAC) with regards to EHRs
- Discuss functions of the security INS
- Explore future implications for the security informatics nurse specialist role
Informatics Nurse Specialist (ANA)

“The informatics nurse specialist is a registered nurse with formal graduate-level education in informatics or an informatics-related field” – pg. 7

Functional Areas of Nursing Informatics:

- Compliance and Integrity Management
- Safety, security and Environmental Health
Nursing Informatics Functional Areas

- Administration, Leadership & Management
- Systems Analysis & Design
- Compliance & Integrity Management
- Consultation
- Coordination, Facilitation & Integration
- Development of Systems, Products & Resources
- Educational & Professional Development
- Genetics & Genomics
- Information Management/Operational Architecture
- Policy Development & Advocacy
- Quality & Performance Improvement
- Research & Evaluation
- Safety, Security & Environmental Health
- Safety, Security & Environmental Health
- Safety, Security & Environmental Health
Compliance and Integrity Management

Regulatory standards and ethical requirements:

- Develop/ and or revise operational procedures
- Establish technical processes to maintain compliance (HIPAA, etc)
- Meet new mandates at local, state, national and global levels
Safety, Security & Environmental Health

- Assure safety & security of HIT-related products
- Prevent harm due to HIT from unintended consequences
- Improve usability and safety of HIT (not just EHRs)
- Provide role-based security for EHR access
ANA Code of Ethics for Nurses

Provision 3: “The nurse promotes, advocates for and strives to protect the health, safety & rights of the patient”

- Restrict access to patient data
- Ensure accurate data is used to benefit healthcare outcomes
Why Does Privacy & Security of the EHR Matter?

- Patient
- Healthcare organization/provider
- Regulatory bodies
Regulatory Frameworks

- Privacy Act (PA) of 1974
- Federal Information Security Management Act (FISMA) of 2002
Regulatory Frameworks

- Fair Credit Reporting Act (FCRA) of 1970

- Health Insurance Portability and Accountability Act (HIPAA) of 1996:
  - HIPAA Security Rule
  - HIPAA Privacy Rule
  - HITECH Act
Administrative Safeguards for ePHI:

- Security management process
- Security personnel
- Information access management
- Workforce training and management
- Evaluation
Physical Safeguards for ePHI:

- Facility access controls
- Workstation and device security
- Workstation security restriction measures (e.g. computer monitor filters)
Technical Safeguards for ePHI

- Access controls
- Audit controls
- Integrity controls
- Transmission security measures
NIH Clinical Center

- Largest U.S. in-patient biomedical research hospital
- 240-inpatient beds & ambulatory care
- Support Research Programs:
  - Intramural
  - Extramural
Department of Clinical Research Informatics (DCRI)

- IT Operations
- Clinical Informatics (14 INS):
  - Build (Orders & Documentation)
  - Liaison
  - Training
  - Project Management
  - Security
EHR Security INS Role

- Manage EHR end-user accounts (4400 + End-Users)
- Create, modify, and deactivate
- Troubleshoot account issues
- Configure EHR security
EHR Background

- 1975 - 2004: Legacy EHR
- 2004 - EHR implemented
- 2015 - HIMSS Stage 7
  - 1st federal U.S. medical facility
EHR Security Structure

- Status Rights
- Functional Rights

System-Supplied Rights → Enterprise-Defined Rights

Rights

Permissions

Security Groups

Users

Any chart according to status rights
Chart access permissions restricted by provider
Chart access permissions restricted by location
Chart access permissions restricted by service

*Adapted from vendor*
EHR Security Architecture Model

- Authorizes users to act in certain roles
- Assigns a set of permissions to each role
- Role-based access control (RBAC)
Role-Based Access Control (RBAC)

Definition:

- Access granted based on predefined roles
- May be assigned to more than one role
- User granted all permissions associated with each assigned role
- Restricted security groups
### Section 2: Request Account

Please select the employee’s role based on their NIH credentialing status, job function and need to know.

<table>
<thead>
<tr>
<th>Employee Role</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Clinician - IRTA, Administrator, Researcher, Patient Escort, Patient Care Coordinator, Volunteer, Student, etc.</td>
<td>View/Retrieve Only</td>
</tr>
<tr>
<td>Clinician (Non-Credentialled) – Physician, Nurse Practitioner, Physician Assistant, Fellow, Nurse (RN/LPN), Dental Hygienist, Registered Dietician, Genetic Counselor, Pharmacist, Phlebotomist, Respiratory Therapist, Social Worker, Rehab Therapist, Technician, Technologist</td>
<td>View/Retrieve Only</td>
</tr>
<tr>
<td>Intern (Social Work, Nutrition, Rehab Med, Spiritual Ministry), Post-Doc, IRTA</td>
<td>View/Retrieve &amp; Clinical Documentation &lt;br&gt;<strong>Note:</strong> All entries will be monitored on a regular basis &amp; discrepancies reported.</td>
</tr>
<tr>
<td>(Co-Signature by a Credentialled Clinician <strong>REQUIRED</strong> on page 3)</td>
<td></td>
</tr>
<tr>
<td>Patient Care Technician, Spiritual Ministry, Bioethicist, HIMD, NIH Teacher</td>
<td>View/Retrieve &amp; Clinical Documentation</td>
</tr>
<tr>
<td>Admissions Staff, Program Support Assistant, Unit Clerk/RSA</td>
<td>View/Retrieve, ADT functions, unit support functions (release non-medical orders, transfer patients). Select Role:<strong>Choose from drop-down option</strong>&lt;br&gt;<strong>Select Adjunct/Affiliate Medical Staff:</strong>&lt;br&gt;<strong>Choose from drop-down options</strong>&lt;br&gt;Adjunct/Affiliate Medical Staff privileges <em>(Refer to table on page 3)</em></td>
</tr>
<tr>
<td>Clinician (Credentialled) – Dental Hygienist, Registered Dietician, Genetic Counselor, Geneticist (PhD), Pharmacist, Phlebotomist, Licensed Practical Nurse, Respiratory Therapist, Social Worker, Rehab Therapist, Technician, Technologist, Clinical Psychologist, Audiologist, Infection Control Specialist</td>
<td>View/Retrieve, ADT functions, unit support functions (release non-medical orders, transfer patients). Select Role:<strong>Choose from drop-down option</strong>&lt;br&gt;<strong>Select Adjunct/Affiliate Medical Staff:</strong>&lt;br&gt;<strong>Choose from drop-down options</strong>&lt;br&gt;Adjunct/Affiliate Medical Staff privileges <em>(Refer to table on page 3)</em></td>
</tr>
<tr>
<td>Registered Nurse (Credentialled)</td>
<td>View/Retrieve, ADT functions, unit support functions (release non-medical orders, transfer patients). Select Role:<strong>Choose from drop-down option</strong>&lt;br&gt;<strong>Select Adjunct/Affiliate Medical Staff:</strong>&lt;br&gt;<strong>Choose from drop-down options</strong>&lt;br&gt;Adjunct/Affiliate Medical Staff privileges</td>
</tr>
<tr>
<td>Security Group Code</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ADMMEOClerk</td>
<td>Admissions Clerk (Program Support Assistants (PSA), Admissions Clerks) - CC / Nursing</td>
</tr>
<tr>
<td>ADMMEOStaff</td>
<td>ADMMEOStaff (PSAs, Admissions Staff, Admissions Clerk) - CC / Admissions</td>
</tr>
<tr>
<td>ADMStaff</td>
<td>Admissions Staff - Health Information Management Department (HIMD) &amp; some DCRI staff</td>
</tr>
<tr>
<td>ALL</td>
<td>All Security Groups</td>
</tr>
<tr>
<td>AMSCore1</td>
<td>Affiliate Medical Staff (Lab Techs, Nutritionists, Imaging/Rad Techs, Social Workers, Rehab Med, Resp Therapists)</td>
</tr>
<tr>
<td>Auditor</td>
<td>Auditors with HIMD</td>
</tr>
<tr>
<td>DataEntry1</td>
<td>LPNs, Patient Care Technicians (PCTs), HIMD staff, Spiritual Ministry</td>
</tr>
<tr>
<td>DCRI Config</td>
<td>DCRI Configuration Team</td>
</tr>
<tr>
<td>DCRI DST Ops</td>
<td>DCRI Technical Support Team (UST)</td>
</tr>
<tr>
<td>M&amp;EServices</td>
<td>Messenger &amp; Escort</td>
</tr>
<tr>
<td>MRDExpSvReq</td>
<td>HIMD Staff</td>
</tr>
<tr>
<td>NurseCore1</td>
<td>Registered Nurses - Clinical Center Nursing Department</td>
</tr>
<tr>
<td>NurseRes1</td>
<td>Registered Nurses - Institutes</td>
</tr>
<tr>
<td>OMSAdmit</td>
<td>Occupational Medicine Service (OMS) Staff to admit OMS patients</td>
</tr>
<tr>
<td>OMSAMSCore1</td>
<td>OMS Affiliate Medical Staff</td>
</tr>
<tr>
<td>OMSDataEntry1</td>
<td>OMS LPNs, PCTs</td>
</tr>
<tr>
<td>OMSNurseCore1</td>
<td>OMS RNs</td>
</tr>
<tr>
<td>OMSNurseRes1</td>
<td>OMS RNs</td>
</tr>
<tr>
<td>OMSPrescriber1</td>
<td>OMS MDs, NPs, PAs</td>
</tr>
<tr>
<td>OMSUnitClerkRSA</td>
<td>OMS Unit Clerks/RSAs</td>
</tr>
<tr>
<td>OMSViewDataOnly</td>
<td>OMS View Only users</td>
</tr>
<tr>
<td>Pharm Config</td>
<td>Pharmacy Configuration Team</td>
</tr>
<tr>
<td>PrescriberCore1</td>
<td>MDs, NPs, PAs (credentialled at NIH)</td>
</tr>
<tr>
<td>SDGeneralUser</td>
<td>SunDown print and view general user</td>
</tr>
<tr>
<td>SMM Build Pharm</td>
<td>Sunrise Medication Manager (SMM) Configuration for pharmacy staff</td>
</tr>
<tr>
<td>SMM Pharm Tech</td>
<td>SMM Pharmacy Tech</td>
</tr>
<tr>
<td>SMM Pharmacist</td>
<td>SMM Pharmacists</td>
</tr>
<tr>
<td>UnitClerkRSA</td>
<td>Unit Clerks/RSAs, PSAs</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>All general users with view only access</td>
</tr>
</tbody>
</table>
### Security Rights

- **Prescribers** = 656
- **Clinical Research Nurses** = 614
- **ViewDataOnly1** = 183

<table>
<thead>
<tr>
<th>Security Group</th>
<th>Right Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ViewDataOnly1</td>
<td>Can view visit demographic</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>Can view patient/visit</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>Can view ultra privacy visits on list</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>Can View Clinical Summary Tab</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>Can view Outpatient Med Profile</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>ES Can edit resource</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>Can acknowledge results</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>Can view Ultra Privacy data/AM Header</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>Maximize multi-pat worklist-allow mod</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>Do Not Auto Select First Patient</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>ES Can view schedules</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>Apply user's security to Unack Alerts</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>NIH Can View AP Results</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>NIH Can View CCMD SvReq</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>NIH Can View DIALYSIS Order</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>NIH Can View HERB Order</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>NIH Can View MES Order</td>
</tr>
<tr>
<td>ViewDataOnly1</td>
<td>NIH Can View NERU Order</td>
</tr>
</tbody>
</table>
EHR Accounts Creation

How does your organization know when to activate an EHR user’s account?
EHR Accounts Creation Workflow

Supervisor submits eCARF

User meets RBAC criteria?

User meets RBAC criteria?

Security INS creates user’s EHR account

User granted access

INS activates account (after user completes training)

Yes

No

User registers for EHR training

Security INS notifies supervisor reason for denial

Supervisor contests/disputes?

Yes

No

Security INS refers to HIMD for decision

Approved?

Yes

No

Security INS refers to HIMD for decision

HIMD refers to S&Q for decision

Approved?

Yes

No

User denied access

Key:
eCARF – Electronic [EHR] Account Request Form
INS – Informatics Nurse Specialist
HIMD – Health Information Management Department
RBAC – Role-Based Access Control
S&Q – Safety & Quality Department
Operations & Maintenance

- Accounts Modifications
- System Change Requests
- Generic/Test Accounts
- External Auditor Accounts
- Dictionary Configurations
EHR Dictionary Configuration

Bulk Load:

- Enterprise Directory data
- End-User profiles
- Data Dictionaries
Deactivating Accounts

Automated Query Reports (SQL Server Reporting Services – SSRS):

- Users Not found in the Active Directory
- Users With No Access Last 365 Days
- Users With No Activity
Security INS Future Role

Where do you see the role of the security informatics nurse specialist in the next 5 years?
Implications for the Future

- Privacy & Security
- Cybersecurity
- Database Administrator
- Application Analyst
- Data Analytics
- Medical Device Security
Contact Us

Claribel Sawyerr, MSN/MPH, RN-BC
csawyerr@cc.nih.gov
Kim Stevens, MSN, RN
stevenskd@cc.nih.gov
Susan Martin, RN, JD, CIPP/G, CPHIMS
smartin@cc.nih.gov
References


