

Senior Epic Security Analyst

Job Code: 340029	FLSA Status: Exempt	Mgt. Approval: P. Verhage	Date: March 2022
Department: 1007422 IS - Risk & Compliance		HR Approval: N. Lazaro	Date: March 2022

JOB SUMMARY

The UW Health Senior Epic Security Analyst is the guardian of all staff identity and access to the electronic health record (EHR) with responsibility for safeguarding critical and confidential information belonging to UW Health or for which UW Health is the custodian.

The Senior Epic Security Analyst is responsible for Epic user records (EMP users, templates, and subtemplates), provider records (SER), security classes (ECL), and provider/patient groups (PGP) administration. This includes the life cycle management of the records (creation, modification, inactivation) and auditing as appropriate. The Senior Epic Security Analyst leads and participates in the development of workflows, system configuration, change documentation, optimization and support related to Epic security and Schedulable Epic Resources, while working with application teams to deploy functionality changes, new modules or departments, update security classes, modify provider records, conduct user analysis, and implement security enhancements.

The Senior Analyst leads and assists in the development of department and organization wide policies and procedures, while effectively communicating policies and procedures impacting Identity and Access management to end users, leadership, and peers to ensure compliant practices. The Senior Analyst provides guidance on optimizing security build based on appropriate minimum necessary standards. The Senior Epic Security Analyst is responsible for the on-going maintenance, testing, support and optimization of Epic user security and provider management, in addition to Identity Governance and Role Based Access Controls (RBAC).

The Senior Analyst mentors and trains others and consistently demonstrates leadership characteristics in line with the UW Health Way. The Senior Analyst leads and implements improvement projects to improve efficiency and accuracy of work performed. Additionally, team members will engage in other security related activities, as appropriate, to ensure the integrity, availability, and confidentiality of electronic information.

The Senior Epic Security Analyst is highly independent using established protocols and is involved in developing new standards. The Senior Epic Security Analyst maintains team-level and organization-level responsibilities and is involved in leading large scale projects.

MAJOR RESPONSIBILITIES

- Lead user account life cycle management, which includes creating, provisioning, updating, and inactivating.
- Plan, test, manage, and update security for the protection of and access to UW Health 's electronic health record.
- Act as the subject matter expert for Epic User Security and Schedulable Epic Resources.
- Lead the security owned portions of application Updates and Special Updates, evaluation of new technology, settings, and functionality.
- Troubleshoot security and workflow issues independently or in collaboration with other Information Systems teams and/or stakeholders, including mentoring others on troubleshooting techniques.
- Lead the development, implementation, and support of Role Based Access Controls (RBAC).
- Ensure all evidence of authorization is documented and archived according to internal standards.
- Enforce organizational policies and procedures to ensure only authorized personnel have access to information in compliance with the Minimum Necessary Rules.
- Identify, recommend changes and lead implementation of process improvements to improve efficiency and accuracy.
- Participate in ongoing auditing and risk assessments and implementation of audit recommendations.
- Identify and ensure dormant accounts/records are disabled; eliminate access for those who no longer need applicable information.
- Create and provide detailed security metrics to senior management to document the effectiveness of the overall security program.
- Responsible for the facilitation of security planning, build, and support of Epic implementations by actively participating in project teams meetings and planning.
- Develop system access and security implementation plans derived from operational customer needs and requests.
- Develop, validate, and maintain detailed documentation on system configurations and technical settings for internal team use, end user support, and other IS teams as needed.
- Generate Reporting Workbench and ad-hoc reports to perform in-depth analysis and data collection for issues associated with Epic software.
- Review system and application log files and investigate usage anomalies as needed, ensuring unauthorized access attempts are investigated and resolved.

- Demonstrate a living example of the principles of continuous quality improvement (CQI) whereby decision making is driven by data, and customer-supplier relationships are facilitated with professional integrity both within and outside the System.
- Assist in the enrollment of Haiku, Canto, and Electronic Prescribing of Controlled Substances (EPCS)
- Manage Security Benchmarking and enhancement implementation.
- Manage Security/Privacy Vulnerabilities (SPRE) and implement risk mitigating measures.
- Manage the Epic browser URL and activity allow list.
- Staff a 24x7 on-call rotation 365 days a year to ensure ongoing operations and security for a facility that operates continuously to provide the best possible care to the patients we serve.

ALL DUTIES AND REQUIREMENTS MUST BE PERFORMED CONSISTENT WITH THE UW HEALTH PERFORMANCE STANDARDS.

JOB REQUIREMENTS

Education	Minimum	Associate Degree in Healthcare, Information Technology, Business, or related field (2 years of relevant experience may be considered in lieu of degree in addition to experience below)
	Preferred	Bachelor's degree in Healthcare, Information Technology, Business, or related field
Work Experience	Minimum	<ul style="list-style-type: none"> • Demonstrated success leading and mentoring others on Epic Security • Demonstrated success using analytical tools and skills for the development of workflows, system configuration and documentation related to Epic Security • Demonstrated success leading large scale projects and processes
	Preferred	7 years relevant work experience and Software experience: Epic or other electronic health record management.
Licenses & Certifications	Minimum	None
	Preferred	Epic Certification in Security, Provider Badge, or other application modules including but not limited to EpicCare, EpicLink, Prelude, or Cadence

Required Skills, Knowledge, and Abilities	<p>Intermediate competency in the following areas:</p> <ul style="list-style-type: none"> • Leadership including leads with integrity, maintains strategic orientation, demonstrates business & financial acumen, champions innovation, manages execution, leads & develops people • Technical leadership of applicable products or platforms • Leading highly empowered, self-directed teams including cross-functional teams • Communication • Effective team member • Critical thinking • Applying lean management tools • Applying agile methodologies • Mentoring and teaching <p>Advanced competency in the following areas:</p> <ul style="list-style-type: none"> • Identity Management • Application Security <p>Other Knowledge, Skills and Abilities</p> <ul style="list-style-type: none"> • Advanced ability to analyze data and information with a detailed understanding of regulatory requirements that impact the healthcare industry, as well as security frameworks and methodologies. • Meticulous attention to detail • Advanced problem-solving skills • Ability to work comfortably under pressure and deliver on tight deadlines • Ability to maintain the highest standards of confidentiality, integrity, and personal accountability when working with sensitive and restricted data, including protected health information (PHI) • Knowledge of system and legal/regulatory requirements related to Identity and Access for which UW Health is subject to.
---	---

	<ul style="list-style-type: none"> Knowledge of Epic Security, Schedulable Epic Resource settings, and other Epic functionality
--	--

PHYSICAL REQUIREMENTS

Indicate the appropriate physical requirements of this job in the course of a shift. *Note: reasonable accommodations may be made available for individuals with disabilities to perform the essential functions of this position.*

Physical Demand Level	Occasional Up to 33% of the time	Frequent 34%-66% of the time	Constant 67%-100% of the time
X Sedentary: Ability to lift up to 10 pounds maximum and occasionally lifting and/or carrying such articles as dockets, ledgers and small tools. Although a sedentary job is defined as one, which involves sitting, a certain amount of walking and standing is often necessary in carrying out job duties. Jobs are sedentary if walking and standing are required only occasionally, and other sedentary criteria are met.	Up to 10#	Negligible	Negligible
Light: Ability to lift up to 20 pounds maximum with frequent lifting and/or carrying of objects weighing up to 10 pounds. Even though the weight lifted may only be a negligible amount, a job is in this category when it requires walking or standing to a significant degree.	Up to 20#	Up to 10# or requires significant walking or standing, or requires pushing/pulling of arm/leg controls	Negligible or constant push/pull of items of negligible weight
Medium: Ability to lift up to 50 pounds maximum with frequent lifting/and or carrying objects weighing up to 25 pounds.	20-50#	10-25#	Negligible-10#
Heavy: Ability to lift up to 100 pounds maximum with frequent lifting and/or carrying objects weighing up to 50 pounds.	50-100#	25-50#	10-20#
Very Heavy: Ability to lift over 100 pounds with frequent lifting and/or carrying objects weighing over 50 pounds.	Over 100#	Over 50#	Over 20#
List any other physical requirements or bona fide occupational qualifications:			

Work/Environmental: Moderate noise level consistent with an office environment