CYBERSECURITY SPECIALIST

Posted on November 28, 2025

Hours Per Week: 40
Work Location: Delta, BC
Job Expires: 2026-11-28
Salary: $70 per hour

The Cybersecurity Specialist is responsible for safeguarding the organization's information technology systems,
networks, electronic medical records, pharmacy management systems, and digital assets against cybersecurity
threats and vulnerabilities. This role ensures the confidentiality, integrity, and availability of sensitive patient
health information, prescription records, and business-critical data in compliance with applicable privacy
legislation and healthcare industry standards.
The Cybersecurity Specialist develops, implements, monitors, and maintains cybersecurity controls and security
frameworks to protect clinical and pharmacy operations, including OSCAR Electronic Medical Records (EMR),
Kroll Pharmacy Management System (PMS), Microsoft 365 environments, cloud services, network
infrastructure, and endpoint devices.

he Employee shall devote his full professional time, attention, skill, knowledge, and efforts to the business and
interests of the Employer and shall perform the duties of Cybersecurity Specialist, including but not limited to
the following:
Cybersecurity Risk Assessment and Vulnerability Management
● Conduct cybersecurity risk assessments, security evaluations, vulnerability analyses, and threat
assessments of organizational systems, networks, applications, and infrastructure.
● Identify, assess, document, and remediate vulnerabilities affecting OSCAR EMR, Kroll Pharmacy
Management System, Microsoft 365 environments, cloud services, online booking systems, integrated

healthcare applications, and network infrastructure.
● Perform vulnerability scanning and security testing using industry-standard tools such as Nessus or
approved equivalent solutions.
● Develop and implement risk mitigation strategies and security improvement recommendations.
● Maintain risk registers, assessment documentation, and security records.
Security Monitoring and Threat Detection
● Monitor security events, audit logs, system activity, network traffic, and security alerts across all
corporate environments.
● Utilize Security Information and Event Management (SIEM) platforms, specifically Microsoft Sentinel, to
identify, analyze, and investigate security incidents.
● Monitor endpoint security solutions and threat detection systems, specifically utilizing Microsoft
Defender for Endpoint.
● Analyze threat intelligence information and security advisories to proactively identify emerging risks.
Incident Response and Security Investigations
• Investigate cybersecurity incidents involving unauthorized access, malware infections, phishing attacks,
ransomware threats, compromised accounts, and potential data breaches.
● Lead and coordinate containment, eradication, remediation, recovery, and post-incident activities.

Preserve digital evidence and maintain strict incident documentation for audit and compliance purposes.
● Prepare comprehensive incident reports, root cause analyses, and corrective action recommendations.
Identity and Access Management
● Administer role-based access controls (RBAC) for physicians, pharmacists, pharmacy technicians,
medical office assistants, and administrative staff.
● Manage user authentication systems, including Microsoft Entra ID, Multi-Factor Authentication,
Conditional Access Policies.
● Conduct periodic access reviews, privilege audits, and user activity monitoring.
● Review audit trails and system logs to identify and prevent inappropriate access to patient health
information and prescription records.
Security Architecture and Infrastructure Protection

● Configure, maintain, optimize, and enhance cybersecurity technologies, including firewalls, VPNs,
endpoint protection platforms, web filtering systems, email security solutions, and intrusion detection/prevention systems.
● Implement system hardening standards and secure configurations for servers, workstations, clinical
systems, and pharmacy applications.
● Support network segmentation, cloud security initiatives, secure remote access solutions, and
infrastructure security improvements to safeguard healthcare operations.
● Evaluate, recommend, and deploy new cybersecurity technologies and controls to strengthen the
organization's overall security posture.
Compliance, Privacy, and Governance
● Develop, implement, and maintain cybersecurity policies, standards, procedures, and technical controls.
● Ensure absolute operational compliance with applicable privacy legislation and healthcare security
requirements, including:
● Personal Information Protection Act (PIPA)
● Personal Information Protection and Electronic Documents Act (PIPEDA)
● All applicable British Columbia healthcare privacy and security regulations.
● Conduct regular security audits, compliance reviews, and access control assessments.
● Maintain security documentation, compliance reports, audit records, and risk assessment reports for
management and regulatory review.
Vendor and Third-Party Risk Management
● Evaluate cybersecurity risks associated with third-party vendors, healthcare software providers, cloud
service providers, online booking platforms, and integrated healthcare applications.
● Review vendor security practices, privacy controls, contractual obligations, and security certifications.
● Assess and mitigate technical integration risks affecting clinical and pharmacy environments.
● Participate in vendor security reviews and due diligence activities before onboarding

Business Continuity and Disaster Recovery
● Develop, implement, maintain, and test disaster recovery and business continuity plans for critical
healthcare and pharmacy applications.
● Manage, configure, and maintain robust backup and recovery solutions using Azure Backup or

equivalent technologies.
● Conduct periodic data recovery testing, disaster simulations, and validation exercises.
● Ensure organizational readiness to rapidly recover from system failures, ransomware incidents, or data
loss events.
Security Awareness and Training
● Design, develop, and deliver cybersecurity awareness training programs for physicians, pharmacists,
pharmacy assistants, medical office assistants, and administrative personnel.
● Educate staff regarding phishing prevention, password management, social engineering risks, secure
remote access practices, and incident reporting procedures.
● Promote cybersecurity best practices throughout the organization and conduct periodic phishing
simulations and security awareness assessments.
Continuous Security Improvement
● Research emerging cybersecurity threats, attack techniques, vulnerabilities, and industry trends
affecting healthcare organizations and pharmacy operations.
● Monitor security advisories, vendor bulletins, and threat intelligence sources.
● Recommend and implement security enhancements to strengthen the Employer's overall cybersecurity
posture.
● Participate in cybersecurity planning, technology modernization initiatives, and strategic security
projects.
Knowledge, Skills, and Abilities
• Strong knowledge of cybersecurity principles, frameworks, and best practices.
• Experience with healthcare information systems, electronic medical records, and pharmacy management systems.
• Knowledge of network security, cloud security, endpoint security, identity and access management, and
security monitoring technologies.
• Ability to conduct security investigations, risk assessments, and vulnerability analyses.
• Strong analytical, problem-solving, and incident response skills.
• Excellent written and verbal communication skills.
• Ability to prepare technical reports, policies, and compliance documentation.
• Strong attention to detail and ability to handle confidential information.

Working Conditions
• Work is performed in a healthcare environment supporting medical clinic and pharmacy operations.

• May be required to respond to cybersecurity incidents outside normal business hours.
• Must maintain strict confidentiality of patient, prescription, and business information.

Business Impact

The Cybersecurity Specialist plays a critical role in protecting patient health information, pharmacy records,
clinical systems, and organizational data assets. The position contributes directly to regulatory compliance,
operational continuity, information security, and the overall protection of healthcare services provided by
Prudential Pharmacy Inc., Sunstone Medical Clinic, and Pharmasave #1046