Change Healthcare Cardiology™

Staying focused on security

Cybersecurity threats have become ubiquitous in health care. In recent years, these threats have become extremely sophisticated and widespread. Modern cyber threat actors exploit vulnerabilities and attempt to gain access to restricted information or take control of systems and lock them down for ransom purposes.

We are committed to a continuous strategy of providing a secured system. We help our customers safeguard their organizations from malicious cyberattacks.

Change Healthcare Cardiology and Change Healthcare Cardiology Hemo recognized by KLAS* as a leader in Cybersecurity Preparedness:

- Network security
- Data protection
- Identity and access management
- Threat and incident response
- Legal and regulatory
- Resilience

* Jan 2023 KLAS. Visit KLAS Research for a complete view.

Optum

Best-practice cybersecurity

We help protect your organization from malicious cyberattack.

Health care organizations that fail to routinely update their technology systems — especially those using end-of-life platforms — often fall prey to ransomware attacks. Our suite uses industry-best practices for product development, design, and configuration, addressing potential security vulnerabilities during the development life cycle.

Change Healthcare Cardiology 15.1 features qualified technologies and security enhancements. Windows Server 2022 and Windows 11 where qualified.

The security enhancements include browser policies, user account control policies, operating system policies, firewall policies, permission policies, and Microsoft Office policies. The enhancements also include security toolkits.

Enhancements for both servers and Hemo/HAC/NCS workstations

- Disable Non-secure features such as internet explorer browser, HTTP port (80) was blocked all communication must be HTTPS only
- Non-secured encryption methods are disabled, remove from TLS 1.2 server and stations any vulnerable chipper suite

Database hardening

- SQL authentication method is disabled
- SQL server runs with minimal required permissions
- Users have minimal required permissions
- Database encryption (optional purchase)
- SQL Injection Prevention

General security enhancements

- Preform UpToDate penetration testing to supports product security
- Update user segregation (better access authorization)
- Promote better hardening for SQL and Windows server
- Upgrade outdated C++ Redistributable to the latest available
- Enhance automated security scanning

Visit us **to learn more**

Optum

Change Healthcare Canada Company
10711 Cambie Road
Richmond, BC V6X 3G5
Canada