Cybersecurity Readiness in Healthcare

Departments of Health and Wellness, Cyber Security and Digital Solutions, and Nova Scotia Health

Key Messages

- The Departments of Health and Wellness, Cyber Security and Digital Solutions, and Nova Scotia Health are not effectively providing cybersecurity for Nova Scotia's digital health network.
- The same three government entities share responsibility for the digital health network, but there is a lack of accountability for cybersecurity.
- Critical deficiencies identified in key network controls.
- Audit reveals pervasive tolerance for accepting cybersecurity risk and failure to manage ongoing risks.
- We will follow up to evaluate progress on sensitive technical observations not publicly reported within one year.

Why We Did This Audit

- Digital networks are increasingly prevalent in delivery of patient care and hold some of Nova Scotians' most sensitive health information.
- Serious cyber-attacks on healthcare organizations that disrupt patient care, disable networks, and steal sensitive information are becoming frequent in Canada.
- Nova Scotia's government has prioritized expanding digital technologies to transform health care.
- Without robust cybersecurity, Nova Scotia's digital health network is at serious risk.

Shared responsibility, but minimal accountability between DHW, NSH and CSDS

- Governance framework set out in shared service agreement abandoned in 2021-22. Once governance committees abandoned, cybersecurity initiatives stalled.
- Department of Health and Wellness (DHW), as the executive sponsor of the health system, failing to establish priority for cybersecurity across the digital health network.
- Nova Scotia Health (NSH), as the business owner of major clinical systems, failing to establish meaningful accountability for cybersecurity.
- Cyber Security and Digital Solutions (CSDS), as a service provider, may raise cybersecurity concerns, but has no authority to take action to protect the digital health network.
- Key performance indicators to measure and track cybersecurity still not established.

Deficiencies in Key Digital Health Network Controls

- Key network control weaknesses have been confidentially communicated to DHW, NSH and CSDS.
- Cybersecurity policies and standards are not regularly reviewed and updated.
- Digital asset inventory listings are unreliable and incomplete.
- Cybersecurity training program not mandatory for all users of the digital health network.

Failure to Appropriately Manage Cybersecurity Risks by DHW, NSH and CSDS

- Heavy reliance on vendors to provide digital assets, but contracts are not required to include cybersecurity protections and contract management is lacking.
- The Architecture Review Board allows projects to connect to the digital health network without meeting established cybersecurity standards.
- NSH policy lets health decision makers decide which cybersecurity standards to apply on a case-by-case basis, leading to high levels of risk acceptance.
- Testing showed cybersecurity risks frequently accepted.
- Ongoing risk management of digital assets once connected to the digital health network is weak and unreliable, hampered by a lack of role clarity and a lack of accountability mechanisms.
- Control weaknesses in cybersecurity risk management results in the accumulation of cybersecurity risk across the digital health network.