AUDIT AT A GLANCE

MANAGEMENT OF MEDICAL DEVICE CYBERSECURITY AT THE PROVINCIAL HEALTH SERVICES AUTHORITY

Why we did this audit

- Networked medical devices are an essential part of health care.
- Cyberattacks can disrupt medical devices and prevent or delay medical treatment.
- Medical devices and their networks must be secure.

Purpose of our audit

To determine whether the Provincial Health Services Authority (the health authority) is effectively managing medical device cybersecurity risk to protect patients.

Audit period: November 2019 to May 2020

Overall audit conclusion

- The health authority is not effectively managing cybersecurity risk to all its medical devices to protect patients.
- The health authority lacks many cybersecurity controls for its medical devices.

What we found

Cybersecurity of medical devices and patient need

The health authority has not evaluated all cybersecurity threats and their potential harm to patients.

RECOMMENDATION 1

Many cybersecurity controls are missing or only partly present

The health authority is not identifying all hardware and software or their configurations.
It cannot know what systems and devices it has or secure them.

RECOMMENDATION 2

The health authority is not monitoring all systems and devices.
It cannot detect all cybersecurity incidents.

RECOMMENDATION 3

The health authority is not controlling all administrative access.
It cannot ensure that all access is appropriate.

RECOMMENDATION 4

The health authority has accepted all 4 recommendations that we made on managing cybersecurity risk.

OFFICE OF THE
Auditor General
of British Columbia

bcauditor.com