Office of the Auditor General of British Columbia

MANAGEMENT OF MEDICAL DEVICE CYBERSECURITY AT THE PROVINCIAL HEALTH SERVICES AUTHORITY

An independent audit report

February 2021

The Honourable Raj Chouhan
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Mr. Speaker:

I have the honour to transmit to the Speaker of the Legislative Assembly of British Columbia the report *Management of Medical Device Cybersecurity at the Provincial Health Services Authority.*

We conducted this audit under the authority of section 11(8) of the *Auditor General Act*. All work in this audit was performed to a reasonable level of assurance in accordance with the Canadian Standard on Assurance Engagements (CSAE) 3001—Direct Engagements, set out by the Chartered Professional Accountants of Canada (CPA Canada) in the *CPA Canada Handbook—Assurance.*

Michael A. Pickup, FCPA, FCA
Auditor General of British Columbia
Victoria, B.C.
February 2021

CONTENTS

The Office of the Auditor General of British Columbia would like to acknowledge with respect that we conduct our work on Coast Salish territories. Primarily, this is on the Lkwungen-speaking people's (Esquimalt and Songhees) traditional lands, now known as Victoria, and the W̱SÁNEĆ people's (Pauquachin, Tsartlip, Tsawout, Tseycum) traditional lands, now known as Saanich.

REPORT HIGHLIGHTS

What we found

The Provincial Health Services Authority (the health authority):

- has **NOT EVALUATED ALL CYBERSECURITY THREATS** and their potential harm to patients
- is **NOT EFFECTIVELY MANAGING CYBERSECURITY RISK** on all medical devices
- **LACKS MANY CYBERSECURITY CONTROLS** for its medical devices

What this means

The health authority:

- **cannot apply appropriate security controls** to all systems and devices
- **may not be able to detect when systems and devices** on medical device networks **are attacked**

Recommendations

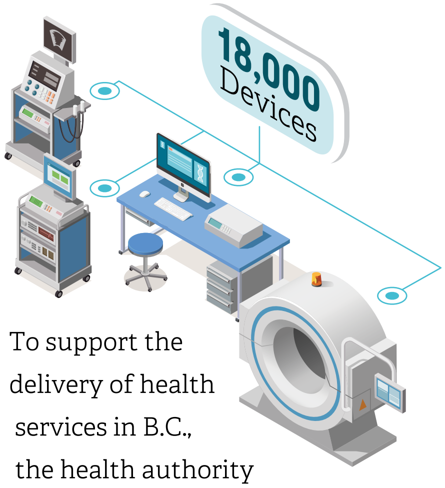
We recommend that the health authority:

- evaluate cybersecurity threats and their potential harm to patients, and take appropriate action

- identify all hardware and software on its medical device networks and their configurations
- monitor all systems and devices on its medical device networks to identify and act on vulnerabilities
- control all administrative access to systems and devices on its medical device networks

Background

- Medical devices are used to diagnose, monitor and treat patients.
- In British Columbia, over 36,000 of the devices are network-capable. They are essential to health care. But cyberattacks across networks can disrupt them and prevent or delay medical treatment.
- Good cybersecurity can neutralize most threats to medical devices.



- To support the delivery of health services in B.C., the health authority manages information technology (IT) services and medical devices. There are over 18,000 of these networkable devices in the Lower Mainland.
- Our audit focused on the health authority's cybersecurity practices in relation to medical devices.

AUDITOR GENERAL'S COMMENTS

MICHAEL A. PICKUP, FCPA, FCA
Auditor General of British Columbia

About this report

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

While adequate controls and processes can reduce much of the cybersecurity risk on medical networks, medical devices cannot always be remediated promptly because of restrictions on the devices and patient care demands. Patient treatment sometimes outweighs cybersecurity. The Provincial Health Services Authority (the health authority) faces the tough—but necessary—challenge of balancing cybersecurity and patient needs.

This audit examined whether the health authority is effectively managing cybersecurity around medical devices by implementing basic controls.

What we found

The health authority lacks many cybersecurity controls for its medical networks and is not effectively managing cybersecurity risk on all medical devices. Some measures are in place, but more should be done to ensure that, for example, authorized devices are the only devices on the network.

For security reasons, we are not disclosing findings that could expose details of the health authority's medical device networks. Instead, we gave the health authority a detailed technical report with our specific findings and recommendations.

Recommendations

We recommend that the health authority evaluate cybersecurity threats and their potential harm to patients, and take appropriate action.

We also recommend that the health authority:

- identify all hardware and software on its medical device networks and their configurations
- monitor all systems and devices on its medical device networks to identify and act on vulnerabilities
- control all administrative access to systems and devices on its medical device networks

We made a total of four recommendations, all of which were accepted by the health authority.

For more information, see Audit at a Glance.

Looking ahead

After reading this report, you may want to ask government the following questions:

1. What oversight exists to ensure the implementation of an effective cybersecurity program for medical devices at the health authority?
2. How are the other health authorities in B.C. protecting patients from medical device cybersecurity risk?
3. How well is patient information protected on medical devices?

Acknowledgements

I thank everyone at the Provincial Health Services Authority for their co-operation and support during this audit, especially with the challenges faced during the COVID-19 pandemic.

Michael A. Pickup, FCPA, FCA
Auditor General of British Columbia
Victoria, B.C.
February 2021

AUDIT AT A GLANCE

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.

SUMMARY

Medical devices are commonplace and varied. They range from infusion pumps to MRI systems, and they are vital to delivering health care and meeting patient needs. British Columbia's Provincial Health Services Authority (the health authority), in collaboration with other health organizations, manages medical devices in the Lower Mainland.

Medical devices are an integral part of hospital networks. Networking them can maximize patient benefit. But this also creates the potential for cyberattack.

Cyberattackers could potentially disrupt health care and thus harm patients. Cybersecurity of medical devices is therefore important for both patients and health-care organizations.

Most cybersecurity risk can be mitigated. An effective security program balances cybersecurity with patient needs. The right balance is achieved only when IT security and medical professionals work together.

COVID-19 has heightened the risk of cyberattacks on health-care organizations. Many workers have shifted to remote working—usually from home-based networks with less security.

Our audit examined whether the health authority is effectively managing medical device cybersecurity risk to protect patients.

We concluded that it is not. The health authority lacks many cybersecurity controls, so it may not be able to detect an attack on its networks and devices, and this may impact patients.

SUMMARY OF RECOMMENDATIONS

We recommend that the Provincial Health Services Authority:

1 Evaluate cybersecurity threats and their potential harm to patients, and take appropriate action.

2 Identify all hardware and software on its medical device networks and their configurations.

3 Monitor all systems and devices on its medical device networks to identify and act on vulnerabilities.

4 Control all administrative access to systems and devices on its medical device networks.

RESPONSE FROM THE AUDITEE

The Provincial Health Services Authority (PHSA) would like to thank the Office of the Auditor General for your review and analysis together with the advice and guidance on improving the cyber security protection of medical devices. The health sector in general has had a significant growth in the use of technology and experienced an amalgamation of systems, networks and infrastructure over the years. These recommendations support our ongoing program to ensure safety and security for patient care devices across our system.

PHSA has policies and programs in place to manage and improve the cyber security resilience across its programs and for the health authorities we support, and a number of planned improvements are scheduled for 2021. Among these improvements is an expansion of our cybersecurity action concerning medical devices.

PHSA leaders recognize that addressing cyber security requires a varied, sustained and continuous improvement effort to keep up with current threats. This effort is ongoing and is informed by regular threat assessments, improved cyber visibility and increased inventory to provide increased assurance that the systems and devices used for patient care and treatment are secure and trusted.

We accept all four recommendations in the report and are pleased to provide details of work underway and plans to further ensure medical device security through 2021.

RECOMMENDATION 1: We recommend that the Provincial Health Services Authority evaluate cybersecurity threats and their potential harm to patients, and take appropriate action.

RECOMMENDATION 1 RESPONSE: PHSA has a Security Threat and Risk Assessment framework in place to assess cyber risks and accountability for staff and programs in this process. We will review elements of this framework to ensure it is fully understood and utilized across our domain. We work with multiple partners within industry and government, including the Canadian Cyber Centre for Security and ECRI, to ensure we are aware of current adversaries and how best to defend against them.

We agree, as the threat landscape is constantly evolving, that it is important to regularly assess our technical infrastructure through multiple lenses. As a result we have expert consultants conducting a cyber-threat assessment for medical device networks, to assist and inform how we prioritize the improvements that need to be made. We are prepared to make any additional investments required in our network and hardware infrastructure, as well as policy and practice changes.

RECOMMENDATION 2: We recommend that the Provincial Health Services Authority identify all hardware and software on its medical device networks and their configurations.

RECOMMENDATION 2 RESPONSE: Asset hardware and software inventory is a priority for PHSA. We are initiating work to extend technology to discover vulnerabilities and remediation processes used in other parts of our network to include medical device environments, using a risk-based approach to ensure no unintended impacts on these critical devices or patient care.

The rapid growth for technology within the health sector has necessitated a need to merge the asset inventories of traditional network, server, Internet of Things and other devices together. The Health Organizations have large and complex networking environments, and some of these older designs need to be modernized to reflect the changing technological landscape and security control benefits.

RECOMMENDATION 3: We recommend that the Provincial Health Services Authority monitor all systems and devices on its medical device networks to identify and act on vulnerabilities.

RECOMMENDATION 3 RESPONSE: Our teams agree that monitoring systems and devices and applying fixes are a priority to ensure patient safety. Within the health sector it is crucial that we work with device manufacturers to ensure that these actions do not have adverse effects. PHSA has processes and technology to proactively monitor and detect vulnerabilities that will be extended across the full range of these more sensitive systems and devices. Additionally we are exploring technologies that may expand this capability.

RECOMMENDATION 4: We recommend that the Provincial Health Services Authority control all administrative access to systems and devices on its medical device networks.

RECOMMENDATION 4 RESPONSE: PHSA agrees that limiting the use of administrative access is good security practice. We work within the limits of the configuration options set by medical device manufacturers, which can affect our ability to modify or change settings. We are introducing new processes to ensure devices have updated security settings and that administrative access is more tightly controlled.

ABOUT THE AUDIT

Background

What is a medical device?

A medical device[1] is any instrument used to:

- diagnose, treat, mitigate or prevent a disease, disorder or abnormal physical state
- restore, correct or modify a body function
- diagnose pregnancy

In simple terms, a medical device is used to diagnose, monitor and treat patients' health conditions.

Many medical devices use digital technology. Examples are cardiac pacemakers, infusion pumps and MRI (magnetic resonance imaging) systems. Many medical devices connect to networks, and some stand alone. Most medical devices are external—making only physical or electrical contact with a patient's body—while others are implanted in a patient's body (for example, cardiac pacemakers).

Why are medical devices important for patient care?

Medical devices can help health-care workers understand and make better decisions about patients' conditions and treatment, so they can provide the right care at the right time. Thousands of medical devices are used in hospitals to diagnose, treat and rehabilitate patients—from vital sign monitors to infusion pumps, dialysis machines and MRI systems. In British Columbia, over 36,000 of these devices are network-capable.

Why does cybersecurity for medical devices matter?

Networked medical devices have both benefits and risks. They are more efficient and produce better patient outcomes. But since the devices can connect to hospital networks, mobile applications and the internet, they are vulnerable to cyberattack, as are all networked computers.

Globally, cyberattacks are on the rise. Health-care organizations are key targets for attackers because health information is so valuable. Sophisticated attackers are exploiting vulnerable

[1] We based our definition of *medical device* on three globally accepted sources: Health Canada, the World Health Organization and the International Electrotechnical Commission.

medical devices and networks. A successful cyberattack on networked medical devices could harm patients and significantly interrupt hospital operations. It could also expose or damage sensitive patient information. A more severe attack (such as with ransomware) could shut down critical medical devices and networks.

RANSOMWARE

Software that denies access to files until a ransom is paid.

Why is it hard to ensure cybersecurity for medical devices?

It is hard for health-care organizations to secure medical devices on their networks because:

- there is a vast number of devices
- medical device updates can be complex and require careful evaluation
- some medical devices rely on legacy systems that are hard or impossible to secure
- timely access to a medical device sometimes outweighs cybersecurity

These factors increase the risk of successful attacks on medical devices and networks.

How has COVID-19 affected cybersecurity?

On March 11, 2020, the World Health Organization declared the coronavirus (COVID-19) outbreak a pandemic, resulting in a huge global impact and increased pressure on health-care workers providing patient care.

COVID-19 has heightened the risk of cyberattacks on health-care organizations. Already under intense pressure to save patient lives, health-care workers are less likely to notice as cybercriminals increasingly:

- exploit technical weaknesses in exposed health-care systems
- use psychological manipulation (such as phishing) to gain unauthorized access to health-care systems

And the increased exposure to cyberattacks has happened when many workers have shifted to remote work—usually from home networks with less security.

PHISHING

Phishing is a social engineering technique where an attacker deceives email recipients into providing sensitive information (such as usernames and passwords) by masquerading as a legitimate email sender.

What is the Provincial Health Services Authority?

Health services in B.C. are primarily delivered through six health authorities: the Provincial Health Services Authority and five regional health authorities.[2]

In collaboration with these regional authorities and other health organizations, the Provincial Health Services Authority operates and coordinates specialized provincial health-care programs. In the Lower Mainland, the health authority also provides IT services and medical device management.

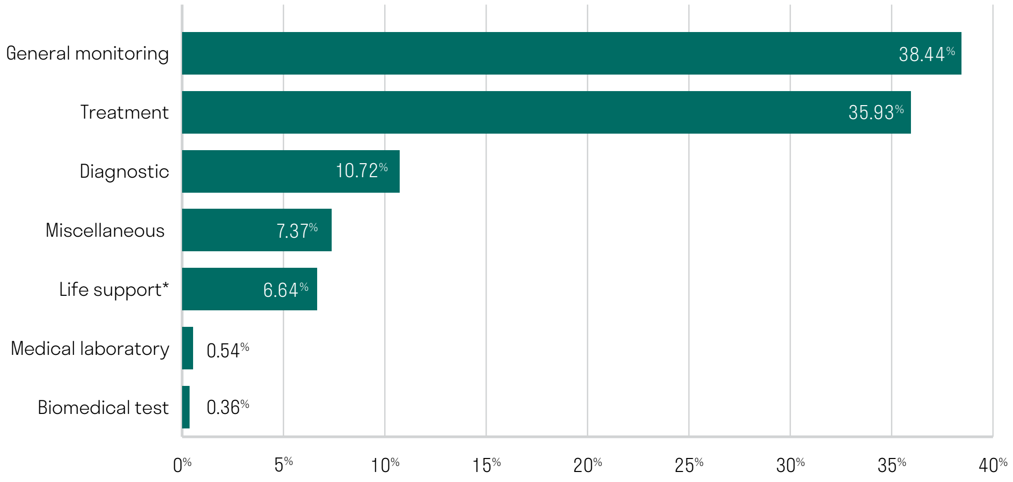
Audit scope

We examined how the Provincial Health Services Authority (the health authority) manages cybersecurity risk in relation to its medical devices.

All medical devices and systems that can connect to systems and networks were covered in the audit. There are over 18,000 of these devices in the Lower Mainland (Exhibit 1 shows the relative proportions of medical devices by category). This includes all information technology (IT) and system infrastructure components supporting the operation of these medical devices.

[2] The five regional health authorities are Fraser, Interior, Island, Northern, and Vancouver Coastal.

EXHIBIT 1: *Medical devices managed through the health authority, by category, 2020*



*Life support equipment is networkable but not connected to the network

Audit method

We looked at the period from November 2019 to May 2020.

Our audit work involved:

- interviewing key staff on IT controls and cybersecurity practices related to securing medical devices and systems
- reviewing policies, procedures and other documentation for supporting evidence of control implementation
- verifying processes and analyzing supporting data to confirm effectiveness of controls implemented
- visiting the health authority's primary medical device management site to observe the control environment
- consulting an external subject matter expert for advice on our audit findings

We developed the agreed-upon audit criteria (Appendix A) based on the critical security controls in the cybersecurity good practices guide issued by the Center for Internet Security.

CIS CONTROLS

The Center for Internet Security (CIS) is a non-profit entity (based in the United States) that develops standards to safeguard organizations against cybersecurity threats. The CIS has issued 20 sets of controls for organizations to improve their cybersecurity defences—referred to as critical cybersecurity controls or CIS controls. By implementing these sets of controls, organizations can eliminate many common cybersecurity vulnerabilities and reduce the risk of successful cyberattacks.

This report is dated February 1, 2021. This is the date on which the audit team finished obtaining the evidence used to determine the findings and conclusions of the report.

AUDIT OBJECTIVE AND CONCLUSION

Audit objective

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

Audit conclusion

The Provincial Health Services Authority (the health authority) is not effectively managing cybersecurity risk to all its medical devices to protect patients.

The health authority has not evaluated cybersecurity threats to all systems and devices on its medical device networks and their potential harm to patients. And it lacks many cybersecurity controls for its medical devices. Specifically, the health authority:

- does not know what hardware or software is on its medical device networks or their configurations because it is not maintaining a complete inventory of them
- cannot monitor for all cybersecurity incidents because it is missing some detection and monitoring mechanisms on its medical device networks
- cannot ensure that all access is appropriate because it is not effectively controlling all administrative access to its medical device networks

KEY FINDINGS AND RECOMMENDATIONS

Cybersecurity of medical devices and patient needs

The Provincial Health Services Authority has not evaluated all cybersecurity threats and their potential harm to patients

Cyberattacks targeting medical devices in health-care organizations can disrupt health care and harm patients. The Provincial Health Services Authority (the health authority) has not established appropriate controls to manage cybersecurity risk. Many of the cybersecurity controls are inadequate or missing. The health authority may not be able to detect whether its systems and devices on medical device networks are under attack.

It is important that the health authority assess threats (and their potential harm to patients) to all systems and devices on its medical device networks. Then it must apply appropriate security controls to all systems and devices, balancing cybersecurity with patient needs.

RECOMMENDATION 1: We recommend that the Provincial Health Services Authority evaluate cybersecurity threats and their potential harm to patients, and take appropriate action.

Many cybersecurity controls are missing or only partly present

Most cybersecurity risk in relation to medical devices can be reduced by using basic controls. Basic cybersecurity controls require the health authority to:

- know what hardware and software it has and how it is configured
- monitor and manage what it has
- control administrative access

The Provincial Health Services Authority is not identifying all hardware and software on its medical device networks or their configurations

Knowing what devices are operating on the network is the first step in reducing the health authority's cybersecurity risk. By actively managing (inventorying, tracking and verifying) all devices on the network, the health authority can ensure that only authorized devices have access.

Knowing what software is running on the health authority's systems and devices, and how it is configured, is also essential. By actively managing the software inventory, the health authority can ensure that only authorized software can run.

Having configuration baselines[3] for hardware and software further improves cybersecurity. With these baselines, the health authority can automatically receive security alerts when unexpected changes occur, and then quickly restore systems if the changes result from a cyberattack or a component failure.

Finally, knowing how networks are configured and understanding how they interact is vital for all aspects of cybersecurity.

We looked at whether the health authority:

- is identifying all hardware and software on its medical device networks and their configurations

We found that the health authority:

- is not identifying all hardware and software on its medical device networks or their configurations
- is not actively managing all hardware devices on the network, so it cannot ensure that only authorized devices access its medical device networks
- does not have a complete inventory of software running on its medical device networks, so it cannot ensure that only authorized software is installed
- is not securely managing system configurations and does not monitor for changes to them, so default (and possibly insecure) configurations may be used
- does not maintain sufficient network documentation, so it cannot ensure that all access is authorized, or fully understand how to secure its networks

The health authority is ensuring secure communication for connections originating from outside its core network. This is good, but it does not diminish the risk of not having standardized configurations for all systems and devices.

The health authority therefore cannot ensure that only authorized hardware and software is operating on the network.

[3] Configuration baselines are established specifications applicable to all hardware and software components that impact an organization's network operations and security. The purpose is to provide a clearly documented basis for change control management.

RECOMMENDATION 2: We recommend that the Provincial Health Services Authority identify all hardware and software on its medical device networks and their configurations.

The Provincial Health Services Authority is not monitoring all systems and devices on its medical device networks

Regular security scans can help the health authority reduce the likelihood of system and device vulnerabilities going undiscovered. Any vulnerabilities found can then be patched or mitigated. Continuously acquiring, assessing and acting on new information can help the health authority prevent cyberattacks in the first place.

However, prevention is never 100% effective. So the health authority needs to collect and analyze system and device audit logs and use them to detect and understand cybersecurity incidents. Many cybersecurity incidents that might have gone unnoticed will be discovered through good log management. Early detection of a cyberattack allows for rapid response and limiting of damage to systems and devices.

We looked at whether the health authority:

- is monitoring all its systems and devices on its medical device networks to identify and act on vulnerabilities

We found that the health authority:

- is not monitoring all of its systems and devices on its medical device networks
- has a weak vulnerability management program

The health authority therefore cannot proactively correct some vulnerabilities and may not be able to detect cyberattacks.

RECOMMENDATION 3: We recommend that the Provincial Health Services Authority monitor all systems and devices on its medical device networks to identify and act on vulnerabilities.

The Provincial Health Services Authority is not controlling all administrative access to medical device networks

Administrative access to systems is necessary, but it always introduces some risk, because administrative accounts must be able to perform any task a system is capable of. For example, admin accounts on medical device networks must be able to override safety features, lock out other accounts and even disable medical devices. To minimize accidental and deliberate misuse of administrative access, the health authority must carefully limit access to those who need it and to when they need it.

Measures to control administrative access include logging and regularly monitoring administrative access, limiting access to scripting tools—which by default use admin accounts—and changing default passwords for all systems and devices. Additionally, encrypting communications for administrative work further reduces the likelihood of unauthorized administrative access.

We looked at whether the health authority:

- is controlling all administrative access to systems and devices on its medical device networks

We found that the health authority:

- is not effectively controlling the use of all administrative access to medical device networks

The health authority therefore cannot ensure that only authorized users have high-level access to systems and devices on its medical device networks.

RECOMMENDATION 4: We recommend that the Provincial Health Services Authority control all administrative access to systems and devices on its medical device networks.

AUDIT QUALITY ASSURANCE

We conducted this audit under the authority of section 11(8) of the *Auditor General Act*. All work in this audit was performed to a reasonable level of assurance in accordance with the Canadian Standard on Assurance Engagements (CSAE) 3001—Direct Engagements, set out by the Chartered Professional Accountants of Canada (CPA Canada) in the *CPA Canada Handbook—Assurance*. These standards require that we comply with ethical requirements and conduct the audit to independently express a conclusion on whether or not the subject matter complies in all significant respects to the applicable criteria.

The Office applies the CPA Canadian Standard on Quality Control (CSQC 1), and accordingly, maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements. In this respect, we have complied with the independence and other requirements of the code of ethics applicable to the practice of public accounting issued by the Chartered Professional Accountants of British Columbia that are founded on the principles of integrity, objectivity and professional competence, as well as due care, confidentiality and professional behaviour.

APPENDIX A: COMPLETE AUDIT CRITERIA

Audit criteria

1. Inventory and control of hardware assets
Inventory of hardware devices should be maintained, managed and controlled.

1.1 The Provincial Health Services Authority (the health authority) should use automated asset inventory discovery tools to identify all systems and devices, including those that should not be connected to its medical device networks.

1.2 The health authority should deploy dynamic host configuration protocol (DHCP) server logging (if IP addresses are dynamically assigned using DHCP) or other IP address management tools to detect unknown systems and devices connected to its medical device networks.

1.3 The health authority should maintain an accurate and up-to-date device inventory of all systems and devices connected to its medical device networks.

1.4 The health authority should deploy network-level authentication to validate system connections.

1.5 The health authority should remove unauthorized devices from its medical device networks.

2. Inventory and control of software assets
Inventory of software should be maintained, managed and controlled.

2.1 The health authority should maintain a list of authorized software required for its systems.

2.2 The health authority should use software inventory tools to identify the software resources that are running on its systems.

2.3 The health authority should document detailed software information (e.g., version level).

2.4 The health authority should physically or logically segregate systems to run high-risk applications in secured network segments to keep them isolated from attacks.

2.5 The health authority should remove unauthorized software.

3. Secure configuration for hardware and software
Security configurations for hardware and software should be established and managed on all devices.

3.1 The health authority should establish standard, secure configurations of operating systems and software applications as the baseline settings for configuration management.

3.2 The health authority should strictly manage the configuration on all new systems and when rebuilding systems following a compromise.

3.3 The health authority should validate master images and store them securely.

3.4 The health authority should use secure channels for remote administration of servers, workstations, network devices and other equipment to protect data during transmission.

3.5 The health authority should use file-integrity–checking tools to ensure that critical system files have not been altered.

3.6 The health authority should implement an automated configuration monitoring system that verifies all configuration elements and sends an alert when unauthorized changes occur.

3.7 The health authority should use a system configuration management tool to automatically enforce configuration settings to systems.

Audit criteria
4. Continuous vulnerability management Systems and devices should be continuously validated as secure by performing vulnerability assessment and remediation.
4.1 The health authority should run automated vulnerability scanning tools against all systems on the network to identify potential vulnerabilities and security risks.
4.2 The health authority should perform vulnerability scanning in authenticated mode and use dedicated accounts.
4.3 The health authority should use automated patch management tools and software update tools to keep security patches up to date.
4.4 The health authority should compare the results from back-to-back vulnerability scans to verify that critical vulnerabilities have been remediated in a timely manner.
4.5 The health authority should establish a process to risk-rate vulnerabilities to prioritize remediation effort.
5. Controlled use of administrative privileges Administrative privileges should be controlled and managed.
5.1 The health authority should minimize administrative privileges and use administrative accounts only when they are required.
5.2 The health authority should use automated tools to inventory all administrative accounts.
5.3 The health authority should change all default passwords before deploying any new device or application to prevent unauthorized access to systems.
5.4 The health authority should configure systems to log and alert when administrative accounts are added or removed to ensure that changes are authorized.
5.5 The health authority should configure systems to log and alert unsuccessful administrative logins to detect unauthorized access attempts.
5.6 The health authority should use multifactor authentication for all administrative access to ensure that only authorized users are given access to systems.
5.7 The health authority should require user accounts to use long (strong) passwords where multifactor authentication is not supported.
5.8 The health authority should require the use of dedicated administrative accounts for all system administrative activities to limit access and protect account credentials from theft.
5.9 The health authority should require initial access by administrators to be via non-administrative accounts that are logged, providing an audit trail that promotes individual accountability.
5.10 The health authority should limit access to scripting tools to authorized users only.
6. Maintenance, monitoring and analysis of audit logs Audit logs of activities should be collected, managed and analyzed.
6.1 The health authority should use synchronized time sources so that timestamps in logs are consistent, enabling accurate analysis of audit logs from multiple systems.
6.2 The health authority should enable audit logging on all systems and devices to allow monitoring of events.
6.3 The health authority should manage logs centrally, aggregating them for analysis, review and detection of incidents.

Audit criteria
7. Secure configuration for network devices and services The security configuration of network infrastructure devices and the ongoing operational use of ports, protocols and services on networked devices should be established and managed.
7.1 The health authority should ensure that only approved ports, protocols and services are enabled to reduce vulnerabilities.
7.2 The health authority should maintain documented security configuration standards for all authorized network devices and use automated tools to validate configurations and alert staff to deviations.
7.3 The health authority should manage network devices using secure connections on dedicated workstations and dedicated networks for all network administrative tasks.
8. Network boundary and wireless access control Network boundary and wireless connections should be controlled and managed.
8.1 The health authority should maintain an inventory of network boundaries, identifying all network interconnections.
8.2 The health authority should scan for unauthorized connections across trusted network boundaries to detect any unauthorized inbound connections.
8.3 The health authority should deny network communications with unknown addresses to prevent unauthorized connections.
8.4 The health authority should deny communication on unauthorized ports to limit unauthorized connections.
8.5 The health authority should use network-based intrusion detection system (IDS) sensors to detect unusual traffic.
8.6 The health authority should require all remote logins to use multifactor authentication and encrypted channels.
8.7 The health authority should maintain an inventory of authorized wireless access points that identifies all wireless connection points to the wired network.
8.8 The health authority should detect unauthorized (rogue) wireless access points connected to the wired network.
8.9 The health authority should limit wireless access on devices to allow only connections to authorized wireless networks and only where there is a business need.
8.10 The health authority should use the Advanced Encryption Standard (AES) to encrypt wireless data, providing protection from unauthorized access during transmission.

OFFICE OF THE
Auditor General
of British Columbia

AUDIT TEAM

Malcolm Gaston,
Assistant Auditor General

Cornell Dover,
Assistant Auditor General

Ada Chiang,
Executive Director, IT Audit

Greg Morhart,
Manager, IT Audit

Uchenna Amaefule,
IT Auditor

John Bullock,
Senior IT Audit Specialist

SUBJECT MATTER EXPERT

Jens Weber,
Professor, University of Victoria

LOCATION

623 Fort Street
Victoria, British Columbia
Canada V8W 1G1

OFFICE HOURS

Monday to Friday
8:30 am – 4:30 pm

Telephone: 250-419-6100
Toll-free through Enquiry BC: 1-800-663-7867
In Vancouver: 604-660-2421

FAX: 250-387-1230
EMAIL: bcauditor@bcauditor.com
WEBSITE: www.bcauditor.com

This report and others are available on our website, which also contains further information about the office.

REPRODUCING

bcauditor.com