Hôpital général juif
Jewish General Hospital

Jewish General Hospital's Information Security Policy

Last updated: 21 oct 2024

Mission and vision

In the respect of our core missions which are providing the highest quality of Care, as well as ensuring safety of our patients and their families, the Jewish General Hospital is committed to ensure compliance to the highest standards when it comes to information security.

To do so, the Jewish Hospital follows best practices and adopts a risk-based approach, meaning that the Jewish General Hospital carefully assesses its environment, its operations and impacts using a structured approach based on industry standards, including NIST's Risk Management Framework to ensure the best cybersecurity posture and protect the Confidentiality, Integrity and Availability of its systems and data.

Our vision at the Jewish General Hospital is to become a premier surgical department and national leader in surgical innovations. We are all committed to providing exemplary physical, emotional and spiritual care for each of our patients, their families and our community. We demonstrate this obligation by embracing cutting-edge surgical techniques and advanced medical technologies, leading innovations that enhance patient outcomes and improve quality of life, and a culture of proactive security to ensure the protection of patient data and operational resilience.

Scope

This Information Security Policy applies to all departments, employees (including permanent, temporary and interns), consultants, researchers and contractors. Third Parties[1] and Foundations are also covered by this policy. (third party are required to comply and regulatory assessment are in place). And all other assets like hardware and software.

Objectives

The main objectives of the Policy are:

- The primary objective of this policy is to protect the confidentiality of patients and organizational data, while confidentiality is our priority due to sensitive data, we are committed to protect availability and integrity of our data.
- To determine and formalize the Jewish General Hospital's approach to Information Security and Information Assets.
- To provide an overall all view of Information Security and how its organized.
- To define roles and responsibilities related to Information Security.
- To provide Hospital's Employees and Third Parties guidance regarding Information Security.

Roles and Responsibilities

Employees

All employees play a crucial role in protecting the hospital's information assets (software, hardware, data) and making sure employees health and personal data are handled properly. Therefore, all employees are responsible and accountable to adhere and comply to the Jewish General Hospital's information security policies and procedures. Employees shall comply with training and awareness internal requirements. Employees are also expected to play a proactive role in ensuring Information Security by reporting any incidents, risks, or suspicious activities according to internal procedures.

Risk owners[1]

As mentioned previously, the Jewish General Hospital adopts a risk-based approach to manage information security and other operational risks. Risk owners, including the IT, Finance, and HR departments, are expected to adopt the best practices in information security and collaborate with the Information Security team. The IT department is responsible for managing cybersecurity risks, maintaining and securing critical hospital systems, managing access controls, and responding to security incidents. The Finance department focuses on protecting sensitive financial information, monitoring transactions for unauthorized activity, and ensuring compliance with financial regulations. The HR department safeguards employee records, ensures compliance with privacy laws, and manages secure onboarding and offboarding processes. All risk owners are also responsible for ensuring compliance with applicable laws, such as the Personal Information Protection and Electronic Documents Act (PIPEDA) and other relevant regulations.

Senior Management

Senior Management are responsible for providing strategic direction, guidance and resources to the development, the maintenance and the continuous improvement of Information Security efforts in line with the Jewish General Hospital's mission and objectives. They are also responsible for representing and embodying the Jewish Montreal Hospital's Information security culture by promoting Information Security initiatives and measures in their departments.

Chief Information Security Officer

As part of Senior Management, the Jewish General hospital's Chief Information Security Officer (CISO) is held accountable for information security. The CISO's is responsible for:

- Deciding the Information Security strategy and objectives in accordance with the Hospital's objectives.
- Leading the development, the implementation, the maintenance and the continuous improvement of the Hospital's Information Security Program including all policies and procedures related to Information Security.
- Overseeing information security risk management processes, threat monitoring, the hospital's security posture and report on it to Senior Management (including Boards/stakeholders).
- Ensuring, promoting and advocating for an integrated Information Security culture across all levels of seniority and all departments of the Jewish General Hospital.
- Ensuring the Hospital is compliant with applicable regulatory industry standards and requirements, by collaborating with appropriate Risk Owners.
- Participating and overseeing Incident Response

Internal Audit

As stated in the Risk Management Policy, Internal Audit are the third line of defense for risks. Therefore, they are responsible for evaluating compliance and efficacy of internal information security measures, controls, and procedures. Internal Audit is also responsible for conducting internal audit and providing the Information Security Team and relevant risk owners with recommendations and areas of improvements. Depending on the audit cycle, audit reports and recommendations can also be shared with the Board.

Board

The Board oversees the Information Security program and posture. The Board will review and approve risk expositions as well as mitigation strategies. They will also review the Information Security Road Map and any other subjects of interest related to Information Security.

Legal Team

The legal team is responsible for handling legal compliance with federal and state laws such as PIPEDA and Quebec Bill 64, the team is also responsible for conducting a contract review with third party vendors to evaluate risk and identify shared responsibilities.

In case of a breach the legal team is responsible for notifying the law enforcement agencies while monitoring the legal part of the incident repose.

With the help of other departments, the team is required to conduct Privacy Impact Assessments (PIAs) for new technologies or projects to ensure privacy risks are identified and mitigated.

Also, the team is responsible of offering necessary legal training to staff on regular basis.

Jewish General Hospital's Information Security Policy Statement

At the Jewish General Hospital, we are committed to upholding the highest standards of information security, guided by the principles of ISO 27001[4]. Our policy is structured around the main domains of the ISO 27001, ensuring a robust approach to safeguarding our information assets.

1. Organization of Information Security

1.1. Security Organization Structure

1.1.1. Establish and maintain an up-to-date chart depicting roles and responsibilities related to ISMS[6].

1.1.2. Form a committee with cross-departmental representation to oversee the implementation of ISMS.

1.2. Internal Communication

1.2.1. Detail the process for internal communication of information security events and policy changes.

1.2.2. Establish a feedback loop for staff to report security concerns and suggestions.

2. Human Resource Security

2.1. Prior to Employment

2.1.1. Implement thorough background checks consistent with legal and ethical guidelines.

2.1.2. Provide specific security training and awareness based on the role prior to granting data access.

2.2. During Employment

2.2.1. Engage employees in ongoing training regarding information security.

2.2.2. Require employees to acknowledge understanding and acceptance of security policies.

2.3. Termination or Change of Employment

2.3.1. Outline secure processes for revoking access and returning company assets upon termination.
2.3.2. Inform departing employees of their ongoing security responsibilities that were signed in the NDA[6].

3. Asset Management

3.1. Asset Identification

3.1.1. Develop and regularly update an inventory of all information assets.
3.1.2. Assign owners to each information asset who are responsible for its maintenance and protection.

3.2. Asset Handling

3.2.1. Classify information assets according to their importance and sensitivity.
3.2.2. Establish procedures for the handling, storage, and destruction of information assets.

4. Access Control

4.1. Access Management

4.1.1. Grant access rights based on roles and the minimum necessary for job functions.
4.1.2. Develop a registration and de-registration process for granting and revoking access.

4.2. remote work

4.2.1 Employees working remotely must use the organization's VPN connection to access hospital systems, ensuring secure communication through untrusted networks.
4.2.2 Access to hospital systems and sensitive data requires multi-factor authentication (MFA) to ensure that only authorized personnel can gain access.
4.2.3 Limit access to sensitive systems based on the principle of least privilege, granting employees only the permissions necessary to perform their job functions.
4.2.4 All data transferred between remote devices and hospital systems must be encrypted to protect confidentiality and prevent unauthorized access.
4.2.5 Employees are encouraged to use corporate-owned devices for remote work to ensure they follow security policies, including regular software updates and patches.
4.2.6 If personal devices are used, they must be configured with anti-virus software, multi-factor authentication (MFA), and strong passwords, and must regularly receive security updates and patches.
4.2.7 Employees must report any lost or stolen devices immediately to the IT team, so appropriate security measures can be taken to protect sensitive data.
4.2.8 Employees must connect to trusted Wi-Fi networks only, and avoid public networks unless using the VPN for a secure connection.
4.2.9 Enable password-activated screensavers on remote devices to ensure that they lock after a period of inactivity, adding an extra layer of protection if left unattended.
4.2.10 Implement application allow listing on corporate devices to prevent unauthorized applications from running and to protect against malware or other security threats.

5. Cryptography

5.1. Cryptographic Controls

5.1.1. Utilize industry-standard encryption methods to secure sensitive data.

5.1.2. Implement procedures for the management of cryptographic keys throughout their lifecycle.

6. Physical and Environmental Security

6.1. Secure Areas

6.1.1. Define security perimeters and barriers for physical protection of sensitive areas.
6.1.2. Establish secure entry controls to restricted areas to prevent unauthorized access.

6.2. Equipment Security

6.2.1. Set up a maintenance routine to ensure continuous security of physical assets.
6.2.2. Ensure that equipment holding sensitive data is securely wiped or destroyed when decommissioned.

7. Operations Security

7.1. Data Backup Process

7.1.1. Implement a regular schedule for backing up all critical data, including patient information, administrative records, and system configurations.
7.1.2. Store backups in a secure, off-site location that can withstand natural and man-made disasters to ensure data preservation.
7.1.3. Encrypt backup data to protect sensitive information during transit and while stored.
7.1.4. Regularly test backup copies for integrity and to ensure a successful restoration process.
7.1.5. Restrict access to backup data to authorized personnel only and log all access attempts.

7.2. Protection from Malware

7.2.1. Deploy and regularly update anti-malware defenses across all systems.
7.2.2. Conduct user awareness programs about potential malware risks and prevention methods.

8. Communications Security

8.1. Network Security Management

8.1.1. Implement controls to protect information on networks from unauthorized access and disclosure.
8.1.2. Ensure that sensitive data is segregated within the network.

8.2. Information Transfer

8.2.1. Establish policies and procedures to protect information transferred via electronic means.
8.2.2. Secure email and instant messaging systems against information leakage and unauthorized access.

8.3 Access to External Data Sources (e.g., Quebec Dossier Santé - DSQ)

8.3.1 Access to external data sources, including the Quebec Dossier Santé (DSQ), must be restricted to authorized personnel only, with permissions granted based on job roles and responsibilities.
8.3.2 All access to external data sources must be protected by multi-factor authentication (MFA) to ensure that only authorized personnel can gain access.
8.3.3 All data transmitted between hospital systems and external data sources must be encrypted to maintain the confidentiality and integrity of the information.
8.3.4 Employees accessing external data sources must ensure that they are using secure, trusted networks (e.g., VPNs) to protect against potential cyber threats such as eavesdropping or traffic manipulation.

8.3.5 All access attempts and data interactions with external sources (such as DSQ) must be logged and monitored to track and audit usage, ensuring compliance with data security policies.
8.3.6 Employees must undergo regular training on the proper use of external data sources and be educated on the potential security risks associated with accessing external systems.
8.3.7 The hospital must ensure that third-party agreements with external data providers (e.g., DSQ) include strict data security standards, including data encryption, breach notification requirements, and compliance with PIPEDA and Bill 64.
8.3.8 Data from external sources must be stored in compliance with the hospital's data residency policies and Canadian privacy regulations, ensuring that sensitive data is not stored or transmitted inappropriately.

9. Information Security Incident Management

9.1. Incident Management Procedures

9.1.1. Establish mechanisms and procedures to report information security events and weaknesses.
9.1.2. Form a team responsible for acting on reported security incidents.

10. Information Security Aspects of Business Continuity Management

10.1. Continuity of Medical Services

10.1.1. Ensure that critical medical services can continue uninterrupted in the event of a power outage or other disruptions.
10.1.2. Maintain and regularly test backup power systems, such as generators, to support essential services like life support systems, emergency lighting, and critical care monitoring.

10.2. Emergency Response and Recovery

10.2.1. Develop and maintain an emergency response plan that integrates with local health care and emergency services.
10.2.2. Conduct regular simulations to prepare for transitioning to and from backup power and other contingency operations.

10.3. Regular Maintenance and Upgrades

10.3.1. Schedule regular maintenance for all emergency and backup equipment to ensure functionality when needed.
10.3.2. Monitor advancements in emergency power solutions and upgrade systems as needed to improve resilience and efficiency.

11. IOT Security

11.1. Device Inventory and Risk Management

11.1.1. Maintain an updated inventory of all connected medical devices, including details about the manufacturer, software version, and patch status. Each device must have an assigned owner responsible for its maintenance and security.

11.1.2. For new medical devices, conduct pre-market risk assessments to identify potential cybersecurity risks before integrating the devices into hospital networks.

11.1.3. Regularly assess the cybersecurity risks of legacy devices, ensuring that they receive software updates and that alternative mitigation strategies are in place for devices that are no longer supported by the manufacturer.

11.2. Secure Device Configuration and Authentication

11.2.1. Ensure that all connected medical devices use multi-factor authentication (MFA) to restrict access to authorized personnel only. Avoid using default passwords or hard-coded credentials on devices.

11.2.2. Isolate medical devices on a segmented network to prevent unauthorized access. Implement strict access control measures to limit communication between IoT devices and critical systems.

11.2.3 All connected medical devices must have their default passwords changed before being deployed within the hospital's network.

11.3. Data Protection and Encryption

11.3.1 All data transmitted from connected medical devices, including patient health information (PHI), must be encrypted to prevent interception or tampering by unauthorized parties.

11.3.1. Ensure that data transferred from devices to cloud service providers (CSPs) complies with privacy regulations like PIPEDA and Bill 64. The CSP must implement strong data security measures, including MFA and encryption.

11.4. Regular Software Updates and Patching

11.4.1. IoT devices must be regularly updated to fix any security vulnerabilities. Implement an automated patch management process to ensure all devices receive the latest security updates as soon as they are available.

11.4.2. Devices that are no longer supported by the manufacturer or cannot receive security updates must be decommissioned and removed from the hospital's network.

11.5. Incident Detection and Response

11.5.1. Use intrusion detection systems (IDS) to monitor network traffic and detect suspicious activity related to connected medical devices.

11.5.2. Develop an incident response plan tailored to IoT device incidents, specifying the steps to take if a medical device is compromised. This includes isolating the device, notifying affected parties, and conducting a root cause analysis.

11.6. Regulatory Compliance and Oversight

11.6.1. Ensure that all connected medical devices meet the cybersecurity standards set by Health Canada and the Medical Devices Bureau of the Therapeutic Products Directorate.

11.6.2. Work closely with manufacturers to ensure that cybersecurity is integrated into the design phase of medical devices, considering both physical safety and cyber risks. Devices should have manual override options for patient safety in case of cyber threats.

12. Shared Computer usage

12.1. All shared computers must require unique user logins for official users, ensuring accountability and tracking of all activities. Guest users must access the guest account, which is isolated from internal systems and sensitive data. Guest users should not have access to shared computers connected to critical hospital systems nor to sensitive data.

12.2. Shared computers must automatically log out or lock after 5 minutes of inactivity to prevent unauthorized access. If the screen locks, re-authentication should be required to resume the session.

12.3. Activity on shared computers must be logged and monitored to ensure compliance with security policies. Logs should track: Login and logout times, applications used, files accessed and any security events or unauthorized access attempts.

12.4. Anti-virus software must be installed on all shared computers and regularly updated to protect against malware and other security threats. The anti-virus software should automatically scan files and applications for malicious activity and alert the IT team to any detected threats.

12.5. Shared computers must be located in secure areas with controlled physical access. Guest users should be restricted to designated areas and should not have access to shared workstations handling sensitive data.

12.6. Ensure that encryption is used on shared computers that store or access sensitive data, ensuring data remains protected even if the device is compromised.

Applicable Laws and Regulations:

The Jewish General Hospital is committed to upholding the highest standards of data privacy and information security by adhering to a comprehensive framework of federal, provincial, international laws, and industry standards. This commitment ensures the protection of patient information, financial data, and other sensitive information across all our operations. Below is an overview of the primary regulations and standards guiding our information security policies:

Federal and Provincial Laws and Regulations (Canada)

Personal Information Protection and Electronic Documents Act (PIPEDA):

Canada’s federal privacy law for the private sector that governs how organizations handle personal information during commercial activities. PIPEDA mandates how the hospital collects, uses, and discloses personal information, including patient health data and financial information.

Bill 64 (Law 25) – Quebec:

An amendment to Quebec’s privacy law that strengthens data privacy rights and imposes stricter obligations on organizations handling personal information. It mandates the use of privacy impact assessments (PIAs), breach notification within 72 hours, and data encryption for sensitive information. This applies to both electronic and non-electronic data.

Act Respecting Health Services and Social Services (ARHSSS):

Quebec’s specific legislation governing how health data is managed and shared, including rules on patient consent, protection of health information, and access to patient records.

Digital Privacy Act (Amending PIPEDA):

Introduces mandatory data breach reporting, requiring organizations to notify affected individuals and the Office of the Privacy Commissioner of Canada if a breach poses a risk of significant harm.

Personal Health Information Protection Act (PHIPA) – Ontario:

Although primarily applicable in Ontario, any transfer of patient health information to or from Ontario must comply with PHIPA. It governs the collection, use, and disclosure of personal health information in healthcare settings.

International Regulations

General Data Protection Regulation (GDPR) – European Union:

Governs the protection of personal data and privacy of EU citizens, affecting how the hospital processes the data of EU residents. GDPR applies when the hospital handles or stores the data of European patients or conducts cross-border data transfers.

Health Insurance Portability and Accountability Act (HIPAA) – United States:

Ensures the protection and confidentiality of patient health information (PHI, ePHI) for US-based patients. This applies to the hospital's handling of US clients' health data, requiring compliance with HIPAA standards for data security and breach reporting.

Health Information Technology for Economic and Clinical Health Act (HITECH) – United States:

Strengthens HIPAA's data privacy and security provisions, requiring the hospital to manage electronic health records (EHRs) securely and report data breaches related to US patients.

Payment Card Industry Data Security Standard (PCI DSS):

A security standard governing how the hospital handles credit card payments. PCI DSS applies to any transactions involving credit card data from patients in Canada, the US, and the EU.

Children's Online Privacy Protection Act (COPPA) – United States:

Applicable when the hospital provides online services or collects data from children under 13 years of age in the US, COPPA governs how personal information is collected, used, and protected.

Third-Party Data Transfers and Cross-Border Compliance:

Data Transfers to US and EU must comply with Canadian data privacy laws (PIPEDA, Bill 64) as well as the applicable international laws such as HIPAA for the US and GDPR for the EU. The hospital ensures that any cross-border data sharing is conducted with data residency and compliance requirements in mind.

Compliance to the Policy (Santos, 2018, p. 502-534; Rights, 2022; Stiglic, 2024)

Compliance Monitoring and Verification

- ***Routine Audits****:* Conduct regular audits of information security practices to ensure adherence to the policy. Audits will be performed by the Internal Audit team in collaboration with the Information Security Department.

- ***Security Assessments**:* Utilize external third-party assessments annually to validate the effectiveness of security measures against industry standards and regulations.
- ***Continuous Monitoring**:* Implement continuous monitoring technologies to detect deviations from the policy in real-time, allowing for immediate corrective actions.
- ***Employee Compliance Checks**:* Regularly review employee access logs and activity records to ensure compliance with access control policies and data handling procedures.

Enforcement and Penalties for Non-Compliance

- ***Disciplinary Actions**:* Employees found in violation of the policy will face disciplinary actions, which may include retraining, suspension, or termination, depending on the severity of the breach.
- ***Incident Response**:* In the case of a security incident, the Incident Response Team will be activated to contain, remove, and recover from the breach. A post-incident analysis will be conducted to prevent future events.
- ***Legal and Regulatory Penalties**:* Non-compliance with federal, state, and international laws and regulations, such as HIPAA, GDPR, or PIPEDA, could result in legal penalties, including fines and sanctions against the hospital.

Compliance Documentation and Reporting

- ***Compliance Reports***: Generate and maintain reports documenting audit findings, assessment results, and compliance checks to be reviewed by Senior Management and the Board.
- ***Regulatory Filings**:* Prepare and submit required compliance filings to regulatory bodies in agreement with applicable laws and regulations.

Training and Awareness

- ***Mandatory Training**:* Require all new hires to complete information security training as part of their orientation. Existing employees must complete annual refresher training.
- ***Awareness Programs***: Implement ongoing awareness programs to keep information security at the forefront of employees' responsibilities.

Exceptions

In instances where it is not feasible to adhere to any part of this information security policy, a Jewish General Hospital Exception Request must be completed and submitted to the Information Security Department. Our Information Security team will review the business case, assess the associated risks, and offer advice on how to proceed. Exceptions to the policy will only be granted when the Data Owner has acknowledged and accepted the risks involved by signing off on them.

Update Requirements

The present policy should be reviewed every 2 years or at every relevant occasion such as major organizational changes. The policy should be approved by the Chief of Information Security. Every major update should trigger a new version of the Policy (e.g.: from 1.0 to 2.0). Lastly, the Version Control Table should be updated every time the policy is updated or reviewed.

Version Control

Version	Date	Purpose/Change	Signing Authority
1.0	21-10-2024	Creation, review	John Doe, CISO

Glossary

[1]**Third Parties:** Any external party providing services to the Jewish General Hospital.

[2]**Risk owners***:* Individuals and/or groups who are responsible for managing risks affecting their areas of expertise.

[3]**Risk Management Policy:** The risk management policy establishes an internal framework for enterprise risk management. It establishes roles and responsibilities and explains the overall process for the identification, assessment, mitigation, management and communication of risks.

[4]**ISO 27001:** The ISO27001 is an international standard providing a framework to manage Information Security, Cybersecurity and Privacy Protection (ISO, n.d.).

[5]**ISMS:** Information Security System.

[6]**NDA:** Non-Disclosure Agreement.

References

1. Bigelow, S. J. (2023, January 18). The 7 critical backup strategy best practices to keep data safe. Data Backup. https://www.techtarget.com/searchdatabackup/feature/The-7-critical-backup-strategy-best-practices-to-keep-data-safe
2. Brands, M. (2023, November 13). 2023-11-13-Cybersecurity laws and legislation. *ConnectWise.* https://www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation

3. Canadian Institute for Health Information. (2021). *Information Security Policy.* https://www.cihi.ca/sites/default/files/document/information-security-policy-en.pdf

4. Clacke, R., Olcott, J. (n.d.). *The board's role in Cyber-Security*. https://work.boardspan.com/library/articles/the-board-s-role-in-cyber-security

5. *Cybersecurity Laws & Regulations - IPOHub.* (n.d.). https://www.ipohub.org/article/cybersecurity-laws-regulations

6. Deloitte. (n.d.). Cybersecurity and the role of internal audit. https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-internal-audit-role.html

7. Hospital security policies & procedures | Infosec. (n.d.). https://resources.infosecinstitute.com/topics/healthcare-information-security/hospital-security-policies-procedures/

8. *ISO/IEC 27001:2022*. (n.d.). ISO. https://www.iso.org/standard/27001

9. Naskar, S. (2023, December 26). What are the 14 domains of ISO 27001? ISO Templates and Documents Download. https://iso-docs.com/blogs/iso-27001-faq/what-are-the-14-domains-of-iso-27001

10. Roumiguieres, R., Salawda, A., Shankar, A. (2024). *Assignment 1: CISO responsibilities.* [Unpublished]. McGill University.

11. Santos, O. (2019). *Developing cybersecurity programs and policies*. Pearson Education, Inc. pp.502-534

12. Standford University. (n.d.). *Definition of risk owner*. https://ocro.stanford.edu/enterprise-risk-management-erm/key-definitions/definition-risk-owner#:~:text=Risk%20Owner%3A%20The%20individual%20who,his%2Fher%20risk%20management%20efforts.

13. Stringfellow, A. (2022, February 12). *6 Key regulations for healthcare cybersecurity.* Tausight. https://www.tausight.com/key-regulations-for-healthcare-cybersecurity/

14. Sunnybrook, Health Science Center. (2015). *Information Security Policy.* https://sunnybrook.ca/uploads/1/patients/privacy/sunnybrook-security-policy-150525.pdf

15. Rights, O. F. C. (2022, October 20). *Summary of the HIPAA Security Rule*. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

16. Canada, C. S. E. (2021, November 5). *Cyber security for connected medical devices (ITSAP.00.132) - Canadian Centre for Cyber Security*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/cyber-security-connected-medical-devices-itsap00132

17. Canada, C. S. E. (2024, March 5). *Security tips for organizations with remote workers - ITSAP.10.016 - Canadian Centre for Cyber Security*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/telework-security-issues-itsap10016

18. *Légis Québec*. (n.d.). https://www.legisquebec.gouv.qc.ca/en/document/cs/R-22.1

19. *Quebec's Law 25: What is it and what do you need to know?* (n.d.). https://www.onetrust.com/blog/quebecs-law-25-what-is-it-and-what-do-you-need-to-know/

20. *Shared Computers & Internet access: Best practices for privacy & security*. (n.d.). https://techsafety.ca/resources/toolkits/shared-computers-internet-access-best-practices-for-privacy-security

21. *Information Security Guides | eHealth Ontario | It's working for you*. (n.d.). eHealth Ontario. https://ehealthontario.on.ca/en/security/guides