Privacy and Security Checklists

Version 1.0

Disclaimer

The information in these resources does not constitute legal advice. It is general information intended to assist physicians in understanding their obligations and general duties under the Newfoundland and Labrador *Personal Health Information Act*. *The information is provided as guidance for clinics in Newfoundland and Labrador for developing their privacy program. In the case of a discrepancy between PHIA and the document, PHIA shall be taken as correct.*

The eDOCSNL Privacy and Security Resource materials have been developed to align with applicable legislation and best practices. The eDOCSNL Privacy and Security Resources are based on original work completed by the Saskatchewan Medical Association, EMR Program.

Table of Contents

Things to Consider when Engaging an Information Manager

An Information Manager is a person or body, other than an employee of a custodian, acting in the course of his or her employment, that processes, retrieves, stores or disposes of personal health information for a custodian, or provides information management or information technology services to a custodian. Some examples of an Information Manager include an IT Service and Support Provider, an information disposal company, and/or an Internet Service Provider.

An agreement with your Information Manager will clarify the relationship and outline expectations.

A vendor providing you with an Electronic Medical Reccord (EMR) in your clinic is considered an Information Manager. eDOCSNL has negotiated a standard agreement for your EMR implementation with Telus Med Access which has been included as part of the participation agreement.

For other Information Managers you might engage for IT Services and Support or Information Storage and Disposal Services, use the sample Information Manager Agreement template provided as a starting point. Many Information Managers, particularly smaller ones, may use a simple one-page agreement that may not meet your expectations for services or the protection of personal health information.

Questions you might ask an Information Manager?

- What type of on-site services do they provide?
- What is the fee structure for each service?
- Are there any additional costs?
- Do they offer software/workstation updates?
- What is the standard turnaround time if hardware needs to be replaced?

Information Manager Checklist: IT Support and Storage

Who will have access to your data?	
❒	Data access must be limited to those with a "need to know" and controlled by a designated individual(s).
❒	Stolen, lost and unauthorized access to personal health information must be reported to the Physician or clinic privacy officer immediately.
❒	Breach notification processes should be in place with the Information Manager to ensure breaches are communicated in an agreed upon manner.
❒	Physical access to facilities where data are stored should be limited and controlled.
❒	Standard non-disclosure language must be included, with protection to keep information private and confidential, except as specifically provided for in the contract. Data is not to be shared with or sold to third parties.
Does data managed by the Information Manager meet all integrity and accuracy requirements?	
❒	The Information Manager must be able to maintain the integrity and accuracy of the data it manages for the clinic.
Does the Information Manager comply with data retention and protection regulations and policies?	
❒	The maintenance and retention of all data must comply with the physician's data retention schedule.
❒	Personal health information must be encrypted when stored and transmitted, and masked on displays and reports.
❒	All access to personal health information must be tracked and audited.
❒	All data will be retained for periods approved by the Physician and returned to the clinic or a third party authorized by the Physician upon termination of the contract. The method of data destruction must be approved by the Physician.
Response time	
❒	Document when response time for support is required, e.g. 24-hour, weekdays, week-ends, holidays.
❒	State expectations on how to contact the Information Manager, e.g. phone or email and whether there will be a service number for each logged contact.
❒	What are the minimum and maximum response time expectations?
❒	What are the minimum and maximum fix time expectations?
❒	Are the response and fix times the same on weekends, evenings and holidays?
Contract termination	
❒	The Physician retains the right to terminate the contract for any reason related to the security items listed in the contract.

Adapted from: http://security.utexas.edu/admin/

Information Protection Checklist

❒ Placement of computer monitor maximizes privacy – i.e. positioned to minimize viewing by others.
❒ Computer / Laptop is set to “lock workstation” mode when away from desk.
❒ Portable devices (laptops, memory keys, blackberries, tablets) have passwords and encryption if they contain personal, confidential or personal health information and are only used according to policy.
❒ Portable devices are securely stored when not in use
❒ Keys for drawers and cabinets are kept in a secure location
❒ Drawers and cabinets in your workspace are locked when away from desk for extended periods
❒ Computer / Laptop / Tablet is logged out and restarted or shut down at the end of the day
❒ Files/papers that contain personal, confidential or personal health information are locked away
❒ “In” & “out” baskets / storage are clear of personal, confidential or personal health information
❒ Passwords are <u>not</u> accessible (*this includes not posted/attached to computer monitor, desktop, white board or bulletin board, etc.*) or shared with anyone else
❒ Only designated recycling bins are used for personal, confidential and personal health information
❒ Garbage cans are never used for personal, confidential and personal health information
❒ Personal, confidential and personal health information that has been approved for disposal is destroyed in accordance with clinic procedures
❒ Mail containing personal, confidential or personal health information is not left where it can be viewed by others

Securing your Wireless Network Checklist

❒ Ensure all devices accessing the wireless network have an antivirus program installed.
❒ Ensure all devices using the wireless network have a personal firewall installed.
❒ Change the factory default password of the wireless router to a strong, complex password.
❒ Use the strongest form of encryption for your network, implementing Wi-Fi Protected Access (WPA)2 were possible.
❒ Change encryption keys periodically if you are using (Wired Equivalent Privacy) WEP or any of the pre-shared key (PSK) variations of WPA.
❒ Place wireless Access Points in a secured location to prevent unauthorized access.
❒ Keep drivers on all wireless devices updated.

Securing your Mobile Devices Checklist

❒ Ensure all mobile devices are password protected using strong passwords.
❒ Set devices to automatically lock after five to 15 minutes of inactivity.
❒ Configure devices to automatically wipe after 10 failed login attempts.
❒ Enable encryption on your mobile device to protect unauthorized access to your data.
❒ Enable remote wipe on mobile devices to force a device to delete its contents in the event the device is lost or stolen.
❒ Use secure wireless network connections to prevent unauthorized access to the information you send and receive across networks.
❒ Avoid connecting to two separate networks (such as Wi-Fi and Bluetooth) simultaneously, which may turn your device into an access point.
❒ Configure your devices so that any wireless connection is off by default (i.e. Wi-Fi and Bluetooth). Turn on wireless connections only when it is required.
❒ Enable automatic update services to ensure that your mobile devices stay current with security updates, device drivers, service packs and application updates.
❒ Ensure your mobile devices have anti-virus, malware and spyware software installed and enabled.
❒ Only install applications from trusted sources. Avoid downloading free software and applications from the Internet without a high level of assurance that the product is safe and contains no adware, spyware, or viruses.
❒ Ensure your mobile devices are securely stored when not in use or when in use in remote locations.

Privacy and Security Awareness, Education and Training for New Employees Checklist

	Employee Initials	Privacy Officer Initials
Policy and Procedures Manual has been provided and an opportunity to read, understand and ask questions was given.		
Oath or Affirmation of Confidentiality has been administered and obligations to uphold it understood.		
An Acceptable Use Agreement to govern use of the clinic's Electronic Medical Record System has been signed.		
PHIA Online Education Training course applicable to role has been completed.		
Privacy and Security Training specific to [Clinic Name] and individual's role conducted.		