MANITOBA OMBUDSMAN

Five-minute Privacy Checkup: Personal Health Information

Practice notes are prepared by Manitoba Ombudsman to assist persons using the legislation. They are intended as advice only and are not a substitute for the legislation.

Trustees and their employees are responsible for protecting personal health information by adopting reasonable administrative, technical and physical safeguards, as required by the Personal Health Information Act (PHIA). Privacy breaches can result from inadequate safeguards that expose personal health information to various risks, including loss, theft or unauthorized use or disclosure.

This 5-minute privacy checkup is a self-assessment questionnaire about your day-to-day habits and security measures intended to help you safeguard personal health information. A "no" answer to any of the following questions is a warning sign that information may not be secure and that action may be required.

Periodic checkups can help strengthen privacy protection and security of personal health information. This questionnaire can be completed at regular intervals, such as when conducting an audit of security safeguards in accordance with subsection 8(1) of the Personal Health Information Regulation.

TRAINING AND KNOWLEDGE	YES	NO
Have you completed training on privacy and security of personal health information?		
Do you know the circumstances in which you have authority under PHIA to collect, use or disclose personal health information?		
If you have authority to collect, use or disclose personal health information under PHIA, do you know the limits and conditions of that authority?		

PHYSICAL SECURITY	YES	NO
At your workspace, do you store personal health information in a locked cabinet?		
Do you lock your cabinet or office door whenever leaving your workspace for an extended period of time, such as for a meeting or lunch?		
At the end of the day do you always:		
Clear your desk of all documents containing personal health information?		
Store your laptop and all documents containing personal health information in a locked office or filing cabinet?		
Lock the door to your work area or to the cabinet that contains personal health information?		
Log off your computer?		

EMAIL AND FAX	YES	NO
Before emailing personal health information do you:		
Ensure that the email address is correct and is that of the intended recipient?		
Send a test email the first time you are sending an email to a new email address?		
Ensure that the information is password protected or encrypted?		
Always include a confidentiality notice?		
Before faxing personal health information do you:		
Ensure that the fax number is correct and is that of the intended recipient?		
Always use a cover sheet that includes both the sender's name and telephone number and the intended recipient's name and telephone number?		
Always include a confidentiality notice?		

SECURITY OF ELECTRONIC FILES	YES	NO
Do you always have to log in to any system using a unique username and password?		
Is your password complex and long enough that it would be difficult for someone to guess it?		
Do you store your workplace passwords securely? (Common hiding areas that are not secure include under your keyboard, phone, mouse pad, monitor, desk, stapler or in an office drawer).		
Do you store all electronic documents containing personal health information on a secure central server? (For example, ensure that no personal health information is stored on a local hard drive).		
Is your computer screen set up so that no unauthorized individuals can view personal health information displayed? (For example, by screen positioning or using a privacy screen.)		
Have you set your computer and other electronic devices so that the device is automatically locked after a brief period of inactivity?		

ELECTRONIC AND REMOVABLE STORAGE DEVICES	YES	NO
Do you always store electronic devices (laptops, tablets, etc.) and removable storage devices (flash drives/USB sticks, CDs/DVDs, etc.) in a locked room or cabinet when not in use?		
Is the personal health information contained on your electronic devices, including cellphones and removable storage devices, limited to the minimum amount of personal health information necessary?		
Have you ensured that all personal health information contained on these devices is encrypted?		
Do you permanently delete personal health information from these devices as soon as you no longer need access to it on the device for the immediate future?		

SECURE DISPOSAL	YES	NO
When you dispose of hard copy records containing personal health information do you:		
Follow the relevant records retention schedule?		
Follow the relevant procedure for secure disposal? (For example, placing the records in a secure shredding bin or by shredding them yourself).		

PRIVACY HABITS	YES	NO
Do you avoid discussing personal health information in any area where the conversation can be overheard by those who do not need to know the information? This may include co-workers, patients' families or the general public.		
Do you share personal health information with co-workers only when it is necessary and authorized under PHIA?		
If you must take personal health information out of the workplace, do you always ensure that any information you have is either on your person or stored in a locked cabinet or room, and never left unattended in your vehicle (not even in the trunk)?		

The privacy checkup was adapted by our office with permission from the Office of the Information and Privacy Commissioner for Nova Scotia.

December 2019