INDEX NO: **PROFESSIONAL PRACTICE GUIDELINE 16.8**

SUBJECT: **Protection of Personal Health Information in Electronic Format**

APPROVAL BY COUNCIL: January 21, 2015
UPDATE: January 13, 2015
REVIEWED: **May 11, 2015**

Background:

The use of electronic means for storage and transmission of health information has advantages for both the health care professional and client. However, safeguards are necessary to protect the privacy of the clients personal health information and meet the requirements of both The Personal Health Information Act (PHIA) and the Freedom of Information and Protection of Privacy Act (FIPPA).

With respect to electronic sharing and storage of health information, PHIA specifies:

" if the trustee uses electronic means to request disclosure of personal health information or to respond to requests for disclosure, implement procedures to prevent the interception of the information by unauthorized persons;" (Section 18 (2)) and

" A trustee who maintains personal health information in electronic form shall implement any additional safeguards for such information required by the regulations". (Section 18(3))

Health professionals employed by a facility are responsible for adhering to the facility/program security arrangements and safeguards to ensure confidentiality, as well as College of Dietitians of Manitoba (CDM) practice direction, Protection of Personal Health Information in Electronic Format.

Practice Direction

As a trustee of personal health information, dietitians have a responsibility to comply with both PHIA and FIPPA, which set out rules to protect Manitobans against unauthorized use and/or disclosure of their personal health information. With the increasing use of electronic means in day-to-day practice, dietitians must be aware of the privacy risk and take steps to mitigate this risk.

Note: Electronic health records are not specifically addressed in this guideline as facilities will, and are responsible for, addressing this in policy.

Web Based Care

Dietitians must ensure that any transmission of information to or from a website remains confidential and complies with all the confidentiality and privacy requirements of the Personal Health Information Act, Code of Ethics and Professional Standards for Registered Dietitians.

Mobile Devices

Mobile devices include laptops, tablets, smartphones as well as portable storage devices such as USB drives, CDs etc. There are a number of precautions to consider when using a mobile device to access or store personal health information.

1. Avoid storing personal health information on mobile devices.

Personal health information should not be stored on mobile devices unless absolutely necessary. If RDs determine that it is necessary to store this type of information, the following precautions must be taken:

a. The device must be password protected with a strong password

i.e. at least 8 characters and a combination of upper and lower case letters, numbers and symbols. The Ontario Office of the Information and Privacy Commissioner suggests basing a mixed, multi-character password on a phrase or favorite song, book title or TV program. For example, My favorite show 24 is on Tuesdays at 9 can become the password: Mfs24ioT@9.

b. Encryption must be used

RDs are advised to seek input from their IT department or other qualified professional to choose the appropriate encryption solution

c. Avoid unsecured networks

d. Be aware of the physical security of your device. Devices should always be kept in secure location i.e. locked office, locked desk

e. Remove personal and personal health information from your device as soon as possible.

Email

The risks with sending personal and personal health information by email and facsimile include:

- Sending information to the wrong email address
- Email is viewed by an unintended recipient
- Email is forwarded to others

To protect your clients' privacy:

- Personal and personal health information should not be emailed unless absolutely necessary.
- All personal identifiers and confidential information should be removed before sending the information, wherever practical.
- Include a confidentiality clause, specifying the information is confidential and intended only for the recipient. This clause should request that the sender be contacted immediately if the information was received by someone in error. When sending information by facsimile, this information should be included on the cover sheet.
- Confirm the email/fax number before transmitting.
- Contact the recipient to advise the information is being sent or to confirm receipt of information.
- Do not use distribution lists to send personal health information
- Disable automatic name completion function to reduce the risk that information is sent to the wrong recipient
- All email boxes should be password protected and should be locked or logged off when not in use.
- Emails containing personal health information should be encrypted.

Text Message

Text messages carry many of the same risks as email, i.e. interception, misdirection. Additional concerns with the use of text messages include:

- documentation and management of patient records. An email can be printed or forwarded easily. It can be a little more difficult to manage these functions with text messages.
- Identification - it can be more difficult to identify yourself and conversely, your clients with the use of text messaging.

Further information and resources are available on the PHIA website at:
http://www.gov.mb.ca/health/phia/

Source Documents

1. Manitoba Ombudsman. Practice note: privacy considerations for emailing personal and personal health information. Winnipeg: 2008. https://www.ombudsman.mb.ca/uploads/document/files/bbt-22-privacy-considerations-for-emailing-pi-and-phi-en-1.pdf. Accessed September 29, 2014.
2. Office of the Information and Privacy Commissioner of Alberta. HIA Practice Note #5. Communicating with patients via email: Know the risks. August 2012. http://www.oipc.ab.ca/Content_Files/Files/Publications/HIA_Practice_Note_5.pdf. Accessed September 29, 2014.
3. Manitoba Ombudsman. Practice Note: Protecting personal and personal health information when working outside the office. Winnipeg: 2007. https://www.ombudsman.mb.ca/uploads/document/files/pn-bbt12-protecting-personal-and-personal-health-information-when-working-outside-the-office-en-1.pdf. Accessed September 29, 2014
4. Office of the Information and Privacy Commissioner of Saskatchewan. *Helpful tips: Best practices: Mobile device security*. 2009. Updated 2011. http://www.oipc.sk.ca/Resources/Helpful%20Tips%20-%20Best%20Practices%20-%20Mobile%20Device%20Security%20-%20March%202011.pdf . Accessed September 29, 2014.
5. Information and Privacy Commissioner of Ontario. Order HO-004. 2007. http://www.ipc.on.ca/images/Findings/up-3ho_004.pdf. Accessed September 29, 2014.