# Some Privacy/Confidentiality and Ethical Issues in Public Health Practice

## Introduction

This is an opportunity to respond to a number of questions. These questions are likely the 'tip of the iceberg' and other questions may follow. Scenarios and examples discussed below are hypothetical and are used to illustrate possible issues. If this document has sparked new questions or if you are unsure of the implications, discuss concerns with your manager. If your questions remain unresolved, please send them to Horst Backé, Population and Public Health Privacy Officer.

## Service

1. **Question:** Is it appropriate for a staff person to provide care to their own friends, family or people with whom they work?

   **Answer:** This is primarily a question of ethics. The Conflict of Interest policy, 20.10.010, provides direction about preserving and enhancing public confidence in the integrity, objectivity, and impartiality of its clinical and business activities.

   Avoid caring for friends, family or others working in your workplace if at all possible. Providing care for friends, family or peers at work creates opportunities for avoidable blurred boundaries, moral dilemmas and potential allegations of privacy breaches. The role differences between being a person's 'health care provider' and the other relationships you may have with that person may create avoidable tensions. Providing health service to someone that you have or anticipate having a social relationship with, could inadvertently compromise perceptions of privacy, create social discomfort and create a perceived lack of safety for the client. Providing health care to friends, family or peers should be avoided except in rare and very unusual circumstances. An example of this type of rare situation might be if you were the only PHN at a school clinic where your niece experienced anaphylaxis and you needed to respond.

   The following is a hypothetical example of why caring for friends, family or others working in your workplace should be avoided. A health care provider immunized the teenage daughter of a friend who, in response to the screening questions, disclosed to the health care provider that she is pregnant. The daughter was uncomfortable with the fact her parent's friend knew this. The health care provider experienced a moral dilemma when hearing from the teenager's parent that the daughter drinks on weekends. In the meantime, the teenager's mother found out that her daughter is pregnant, causing the daughter to question whether the health care provider breached her privacy.

   In remote RHAs it may be impossible to avoid providing health care to family, friends and coworkers; this is only rarely the case in the WRHA.

   Ask others to provide all health care services when you believe you have or may have a relationship with a client outside of work.

Regarding care of work colleagues, Occupational and Environmental Safety and Health (OESH) delivers occupational health care services to employees including work-related immunization, work-related injury, work-related communicable disease exposures (e.g., tuberculosis or blood borne infections), work-related exposure to other biological hazards (e.g., scabies, lice, bed bugs) and return to work. No one should circumvent normal Occupational Health processes to provide health care for staff or others that they may know.

Staff can attend immunization clinics in another community area or see their normal health care provider (e.g., their family doctor, Quick Care Clinic) for immunization or other health services. Staff must use the same processes to access these services as would any member of the public (e.g., make an appointment, wait in queue if no appointment).

Staff must also use the same processes to access their own or family member's personal health information as would any member of the public. Staff persons are given access to systems containing PHI for work related purposes only. To misuse that access for their own purposes is a beach of WRHA policy and may be a breach of legislation and is subject to discipline.

The remaining questions are privacy related.

2. **Question:** Is it appropriate to use a real example of a client interaction when presenting to a class of health students?

   **Answer:** The purpose of presenting to students is to help them learn. We cannot compromise privacy to reach that objective. It would not be possible for anyone to provide informed consent to share information to a group of people with whom they have no relationship.

   Highlighting successes and challenges of real situations is often helpful. However, this should never compromise privacy. Any information that on its own or in combination with other information could identify a client should always be removed. Create fictitious scenarios that help meet learning objectives, and clearly identify these scenarios as fictitious so that the audience knows we take privacy seriously.

3. **Question:** Is it appropriate for me to send emails or texts of any kind for the purposes of providing health care to clients?

   **Answer:** Texting, and email communication outside of the WRHA firewall are not considered to be secure and may result in breaches of privacy. Further, electronic communication of PHI Outside of the secure WRHA environment is a breach of WRHA policy (Security and Storage of Personal Health Information 10.40.120). Personal health information includes the fact a client is receiving health care services.

   Client names should never be entered into a cell phone. Any cell phone used for client care must automatically lock if left inactive. Call history should be deleted.

4. **Question:** Is it ever appropriate to share my user name and password with anyone else? Can I let others use my identity and password if they are inadvertently without access?

   **Answer:** It is not acceptable. Protect your user ID and password; this is your electronic professional "identity," subject to system checks, such as audits and reviews. Do not walk away from a computer terminal while logged in; you will be held responsible for any activity in your name.

5. **Question:** What should I do if I become aware of a privacy breach or suspect a privacy breach?

   **Answer:** Any person associated with the WRHA, who has received a complaint, or who has knowledge of a privacy breach or reasonable suspicion of a privacy breach, must immediately notify their manager or site privacy officer or the WRHA Chief Privacy Officer.

## eChart

6. **Question:** A PHN receives the Grade 4 class list within the context of the school immunization program. For students who have not returned their consent forms, the PHN calls, leaves voicemail messages and completes a door stop home visit with no response. The PHN accesses eChart to determine if there is a new address. Is it necessary to document viewing this record in eChart?

   **Answer:** The use and disclosure of demographic information for the purposes of providing health care is permitted under the Personal Health Information Act (PHIA). It is not necessary to document that demographic information was viewed.

7. **Question:** A PHN completes a Hepatitis B investigation. The PHN identifies household contacts. The contacts to the case complete the follow up with their primary care provider and call the PHN to inform their Hepatitis B status is "negative". The PHN accesses eChart to review the lab results and clarify what the client meant by "negative". An alternative scenario is where the PHN has not received a phone call from the household contacts of the person with Hepatitis B to indicate their status. Therefore the PHN accesses eChart to confirm if the household contacts have followed up with a primary care provider and have had lab work completed. Are these legitimate uses of eChart?

   **Answer:** Yes. The purpose of the Public Health Act is "to enable the delivery of public health services to protect and promote the health and well-being of the people of Manitoba". Reportable communicable disease referrals are sent to us under the authority of the Public Health Act and the case investigation and related contact investigation are considered a public health service in accordance with the Act.

   Client service for referrals under the Public Health Act begins at the time of referral from Manitoba Health or when cases or contacts are identified as part of an investigation. Health-care providers are authorized to view the specific information they need to complete the investigation of the communicable disease.

8. **Question:** A PHN receives a prenatal referral on a woman with many risk factors, and no primary care provider is listed. You know that this referral was sent with her consent. Letters and phone calls to connect with the client have not resulted in success. The PHN uses eChart to find updated demographic information. Is this appropriate?

   **Answer:** Yes. The use and disclosure of demographic information for the purposes of providing health care is permitted under (PHIA). It may also be helpful to ask the referring source for updated identifying information. It is not necessary to document that demographic information was viewed.

   Perinatal services are not regulated by the Public Health Act, so use of eChart to look at personal health information outside of demographics would be a violation of PHIA unless (1) you already made contact with the client *and* (2) you needed that information for the purposes of providing health care. It is not appropriate to use eChart (except to get updated demographic information) or any other information system unless you are currently in an episode of care with that person. The only acceptable use of eChart in the situation where you know that the referral was sent with consent would be to view demographic information to locate a person to initiate an episode of care. We need to respect that a person may have decided not to follow through on the referral to our program.

9. **Question:** If I inadvertently access information in eChart that I did not intend, what should I do? An example is I accidentally clicked on the wrong tab in the correct person's health record.

   **Answer:** With one exception, all views are recorded as part of the audit trail. That is, who looked at it, when it was looked at, and the length of time the information was displayed are all included in the audit information. People who accidentally access information they did not intend are usually there for only a few seconds at most.

   If all you looked at was the demographic page and you realize you have the wrong person, no audit trail is generated.

   If you inadvertently view other information, you should advise your manager and keep written documentation detailing your error and what you did about it.

10. **Question:** Should I print information from eChart?

    **Answer:** People should be going into eChart with a specific question in mind. There is no need to print information. Any printed document creates additional privacy risks. All relevant information from eChart can be transcribed into the health record. eChart printouts should never become part of a client record.

    We should not provide the client with printed information from eChart. The client should complete an access request form to obtain any printouts. Printouts would be mailed to them from the eChart office. Please ask your privacy officer for details.

    For an operational guideline for MANAGEMENT OF PRINTED DOCUMENTS FROM eCHART see http://home.wrha.mb.ca/hinfo/rhif/files/HIS_RG_08.pdf

## eHealth Account & Access Request Form

11. **Question:** When is it necessary for a manager to complete an eHealth Account & Access Request Form?

    **Answer:**

| Situation | iPHIS & Panorama | HPECD Database | eChart | MIMS | EMR | Email | Shared Folders |
|---|---|---|---|---|---|---|---|
| New PPH staff | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | As required |
| Transfer out of office | | ✓ | ✓ | | ✓ | | As required |
| Transfer into office | | ✓ | ✓ | | ✓ | | As required |
| Staff leaving PPH employment | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | As required |

This table assumes that there is a need for this electronic system and that access to the system is standardized for that particular staff grouping. The HPECD Database, eChart and EMR track a person's home office for auditing purposes.

## HPECD Database

12. **Question:** I want to ensure that all referrals are fairly distributed within the team using the Referral Summary report. Is this an appropriate use of the HPECD database?

    **Answer:** It depends. If it is your explicit role to ensure fair distribution of referrals, you have a need for this information. If, for example, it is your role to distribute new referrals, that is a strong reason to run this report. Running this report would constitute a privacy breach if this is not your role because it contains personal health information.

13. **Question:** Will the HPECD Database be audited?

    **Answer:** Yes. The HPECD Database has built in audit capabilities. There will be routine audits as required by legislation, and clients may request audits at any time. Anyone using the database can be audited if there are concerns.

## MIMS

14. **Question:** I use MIMS to look up postpartum addresses when I think they may be incorrect. Is this appropriate?

    **Answer:** Databases should be used for the specific purpose they were intended for and for no other reason. If you need to find information about current addresses in order to provide health care that is not immunization related, use eChart. MIMS is designed specifically to support immunization.

15. **Question:** Is it appropriate to access information from MIMS about family, friends or coworkers?

    **Answer**: It is not appropriate for the reasons outlined in the answer to question 1. It is never appropriate to look at your own PHI within any health information system. Staff must use the same processes to access their own or family member's personal health information as would any member of the public. Staff persons are given access to systems containing PHI for work related purposes only. To misuse that access for their own purposes is a beach of WRHA policy and may be a breach of legislation and is subject to discipline.

16. **Question:** Is it possible that use of MIMS could be audited?

    **Answer**: MIMS is a legacy system that does not have internal audits built into it. However everyone has an ethical and legal responsibility to use systems for the purpose for which they were designed.

    If you notice someone using MIMS inappropriately, you have an obligation to inform the Manager or Privacy Officer.

## Information Sharing or Disclosure

17. **Question:** What information can I share with others?

**Answer:** The Information Sharing Regulation of the Public Health Act identifies under what circumstances and to whom a medical officer, public health inspector or public health nurse may disclose information as related to issues within the scope of the Public Health Act.

PHIA relates to all other disclosures of personal health information. Consult the PHIA policies to learn more.

In all situations disclose the minimum required information.

## Privacy Breach Consequences

18. **Question:** What are the consequences of a privacy breach?

**Answer:** The WRHA Policy #10.40.110 'Reporting and Investigating Breaches and Complaints' describes the procedure to be followed in the event of a privacy breach.

Registered Nurses have an obligation to report "unsafe practice, professional incompetence, professional misconduct and incapacity or unfitness to practice." Professional colleges make decisions about consequences for their members.