13 Privacy Tips for Family Health Teams

1. **You are not alone**. If you don't know what to do or have a privacy question ask for advice from the Privacy Officer, your supervisor, a physician, the Lead Physician, your regulatory College or professional association or insurer or Canadian Medical Protective Association or a privacy lawyer.

2. **Safety trumps privacy.** If there is a significant risk of serious bodily harm to a patient or someone else and sharing information would reduce or eliminate that risk – share the information. Usually that will mean calling 9-1-1 or police or another person (such as an intended victim) to meet your duty to warn. Only share the minimal health information necessary to warn. If unsure what to do – seek advice (see tip #1 above). In an emergency if you cannot get timely advice err on the side of protecting safety.

3. **No snooping**! Do not look at health records if you do not have a legitimate job reason to do so. Think: "am I allowed and supposed to look at this?" Do not look at health records out of your interest or curiosity. Do not look at your family member's or friend's health record or your own health record without following the procedures any other patient or substitute decision-maker or third party would have to follow to get a copy. Here's a 50 second video on the consequences of snooping.

4. **Report** all privacy breaches to the Privacy Officer of your organization. Make sure you know who that is.

5. **Taking patient information off-site has risks.** You must be authorized by the health information custodian or Privacy Officer before you take any patient information off site (in paper or electronically). If you have not been told you are allowed to take patient information off-site – don't! Laptops, USB keys and other mobile devices must be encrypted if transporting patient information. Do not save patient information on the hard drive if the device is unencrypted. Do not store patient information at home. If you have questions, please ask the Privacy Officer.

6. **Find out how patients would like you to communicate with them by phone**. Do they want you to leave detailed messages on voicemail? Do they want you to share information with a spouse/partner/parent/child if they call to make an appointment or get test results? Is there any sensitive information they do not want shared? Physicians and allied health professionals need to make it obvious to front line administrative staff what can and cannot be shared by phone or in person and with whom. See the "Communicating with Our Office" handout as an example of how to have a conversation with patients. When in doubt – do not share information with family members or on voice messages.

7. "**Circle of care**" means physicians and allied health professionals can share patient information with other health care providers to coordinate health care to shared patients relying on implied consent. Hospitals, CHCs, CCACs, long-term care homes, community social workers and psychologists and other health agencies and individuals providing direct health care to a shared patient can be IN the circle of care. The following ARE NOT in the circle of care: police, insurance companies, employers, family members, landlords, Workplace Safety and Insurance Board (WSIB), or a Children's Aid Society (CAS). If a patient says "don't share information with the hospital or another health care provider" the circle of care ends. In that case – you would need express consent to share information going forward.

8. You need **express consent** to share patient information with anyone who is not a health care provider (such as insurance companies, employers, family members (who are not substitute decision-makers), and lawyers) – unless you are otherwise permitted or required by law to disclose. Express consent can be verbal or written (but you should chart all verbal consents in the eMR).

9. When a **third party** such as the WSIB or CAS or an insurance company or a lawyer or a regulatory College says "you are required by law to share with me" ask them to put their request in writing and include the section of the law to which they are referring. Include that written instruction in the chart. If you are unsure whether they have given you sufficient documentation to require you to disclose, consult with the Privacy Officer.

10. **There is no age of consent for making privacy decisions**. Some children and youth will decide who knows about their care and will make their own decisions about releasing their health information. To be "capable" a patient must be (1) able to understand the information that is relevant to making a privacy decision and (2) able to appreciate the reasonably foreseeable consequences of the decision. Patients who make their own treatment decisions generally also make decisions about how information about their treatment is collected, used and disclosed. Similarly, if a patient is incapable of making treatment decisions, the substitute decision-maker usually makes privacy decisions for the patient. Parents of children under the age of 16 may also agree to the release of patient information UNLESS the information relates to treatment the child consented to on his/her own.

AGE	CAPACITY	DECISION MAKER
Person of any age	If capable	Can make decisions about release of everything in his/her own health record
Person of any age	If incapable	Needs a substitute decision-maker to release anything in health record
Under age of 16 (birth to 16 less a day)	If capable	Can make decisions about release of everything in his/her own health record AND A parent can also consent to release of information about any treatment or counseling that child did not consent to on his/her own BUT NOT IF THE CAPABLE CHILD OBJECTS TO PARENT MAKING SUCH DECISIONS

11. **Sign off in between patient visits**. Do not leave your password signed in when you leave a computer or a room. Do not share your password with your colleagues or anyone else.

12. **Do not recycle patient information. Shred it!** Do not use patient information as scrap paper or write on the back of a piece of paper that could have patient information on it. Do not leave the key in the confidential shredding bin lock to make it easy to open the box if you inadvertently shred something you should not have. Do not put health records in your recycling bin before you walk your bin to the confidential shredding bin. Do not pile or store extra documents for confidential shredding beside the confidential shredding bin.

13. **Support a culture of privacy.** Ask others their "go to phrases" for dealing with privacy issues. Talk about ways in which you can support each other to be more privacy respectful.