Guidelines for Consent and Masking Options

This section will:

- define physician responsibilities regarding a patient's implied, deemed and express consent for the collection, use, and disclosure of their personal information
- discuss masking options and physician responsibilities in EMRs and EHRs when personal information is masked by way of disclosure directive or protective words

Implied and Express Consent

Under PIPA, the collection, use, and disclosure of personal information by a practice operate primarily on an "implied consent" model. Individuals who form part of a patient's "circle of care" (e.g., specialists, referring physicians, lab technologists) may collect, use, disclose and retain personal health information for the purposes of ongoing care and treatment on the basis of "implied consent".

"Implied consent" must be voluntary and informed, and physicians have a responsibility to provide adequate information to patients on how the practice manages personal health information (See Ten Essential Steps for PIPA Compliance and the handout Patient Handout - Privacy of Your Personal Health Information). "Implied consent" may be established when an individual is provided with a notice about the collection, use, and disclosure of personal health information in a form they can reasonably understand and for reasonable purposes given the sensitivity of the personal health information. Also known as the "opt-out" model, "implied consent" is established after the individual is provided with a reasonable opportunity to decline. For "implied consent" to be meaningful, the individual has to know that he or she has the right to expressly withhold or withdraw consent at any time without fear of retribution.

Another form of consent that may apply to a patient's circle of care is "deemed consent". "Deemed consent" applies only in situations where the purpose of the collection, use or disclosure of personal information at the time consent is sought is clear and obvious to a reasonable person. The individual must also voluntarily provide their information for that specific purpose.

"Express consent", also known as the "opt-in" model, is a person's verbal or written agreement to the collection, use and disclosure of their personal information for a defined purpose. Express consent from a patient is required when personal information is intended to be collected, used, or disclosed outside of the "circle of care" or for secondary purposes, such as education or research. For more information, see Guidelines for Secondary Use of Personal Health Information for Research. If the practice anticipates

using personal health information for educational or research purposes, these purposes should be clearly stated in the practice's privacy policy and in the patient Consent for Research form.

Masking Options (Disclosure Directives and Protective Words)

Patients may have the option to restrict access to certain personal health information about them that is stored in EHR and EMR systems. This privacy protective feature of an EHR or EMR system is known as "masking", and patients should be informed of this right. The following are examples of "masking" options in EHR systems in BC.

The **Provincial Lab Information Solution** (PLIS) is a provincial repository of lab information that has been designated as a health information bank under the **E-Health Act** (Personal Health Information Access and Protection of Privacy Act). A person whose personal health information is contained in this repository may make a disclosure directive that restricts access to their lab results for clinical purposes. Once a disclosure directive is made through the addition of a "keyword" to the record, lab results can only be accessed by an authorized user for clinical purposes, after the person who made the disclosure directive shares their "keyword" or if there is a need to provide urgent or emergency health care.

Under the **Pharmaceutical Services Act**, a person may request that a "protective word" be attached to their medical and claims history recorded in **PharmaNet**. They may also request that a "protective word" be applied to the record of a minor or adult for whom they have authority to make such decisions. Similar to the disclosure directive model, once the "protective word" is attached, authorized users of PharmaNet can only access medication information for clinical purposes after the person shares their "protective word". Some authorized users may also request the protective word be removed to allow them to provide care in an emergency where neither the person nor their representative is able to provide the "protective word". For more information on PharmaNet protective words, see Protective Word for a PharmaNet Record.

Some health authorities permit patients to mask personal information in their EHR systems. For example, patients can make a disclosure directive in the **CareConnect** system at **Vancouver Coastal Health Authority**.

Many EMR applications have explored and implemented "masking" options. The ability to mask is often considered when a single EMR application is shared in a group practice setting. This provides patients with the ability to control who in the group practice may or may not have access to some or all of their personal information.

Physicians should inform patients about the option to mask personal information in their record, as well as the effects of "masking" on delivery of care. If a competent patient decides to mask their record, physicians must:

- honour the patient's decision and only access the personal information with express consent
- document in the patient's medical record the discussion and the patient's decision
- provide the best care possible working with the information at their disposal

Alternatively, in the absence of an emergency, if the lack of masked information creates a situation where the physician feels the patient's safety is at risk, the physician can refuse to provide treatment. The physician should explain the reasons for their decision not to treat the patient and note all relevant discussions in the patient's medical record.

A physician who is treating a patient whose information has been masked and who does not give the physician express consent to permit access, still has an obligation to obtain a proper history from the patient. Taking a proper history may elicit relevant information, even if that information is masked. To the extent that a patient refuses to discuss relevant information, this refusal should also be adequately documented.