Guidelines for Providing Virtual Health Care

This section will:

- identify security safeguards to use when providing virtual health care
- identify patient consent requirements if systems involve access and storage of information outside Canada
- discuss implied consent in relation to disclosure to health authorities

Security Safeguards

It is essential that physicians ensure virtual health care systems have appropriate security measures and are otherwise PIPA compliant. For example, physicians should only use systems with up-to-date, industry-standard encryption for transmission of data. To reduce the amount of personal health information disclosed to companies providing virtual health care systems, physicians and health authorities should try to communicate with each other about patient medical conditions without referring to the patient's unique identifiers, where feasible.

Storage and Access Outside Canada

Certain virtual health care systems involve access to and storage of personal information outside Canada. This is permitted under PIPA but not under FIPPA, which governs health authorities. If personal information will be shared between a practice and a health authority, personal information in a health authority's custody or control must be stored and accessed only in Canada unless the health authority obtains patient consent for access or storage outside of Canada.

The physician or the health authority can obtain this consent in the following manner:

- The consent must be in writing and specify the personal information for which the individual is providing consent, the date on which the consent is effective, the purpose of the storage of or access to the personal information, and to whom it will be disclosed.
- If practicable, the consent form should also indicate the date on which the consent expires, who may store or access the personal information and the jurisdiction in which the personal information may be stored or accessed.
- Consent must be voluntary. If the patient cannot receive health care services unless they give their consent to having their information accessed or stored outside of Canada, the consent may not be voluntary. This is because health care is increasingly considered an indispensable (as opposed to

optional) service. In such cases, systems that store and access personal information in Canada should be used.

Indirect Collection by Health Authorities

FIPPA requires that heath authorities only collect personal information directly from the individual (as opposed to indirectly through the physician), unless limited exceptions apply. One of the exceptions is that the individual has authorized another method of collection (e.g., by agreeing to indirect collection by the health authority). Generally, physicians have implied consent from the patient to disclose personal information to a health authority when the health authority is providing direct care to that patient. However, health authorities may not have the authority under FIPPA to collect that personal information. In situations where the physician adequately informs the patient that the patient's personal information will be disclosed to, and collected by the health authority, the health authority may collect that personal information.