DEFINITIONS

Access

The ability to view or collect data, particularly from an electronic database. When a record is accessed, it is usually considered a disclosure by the practice. Only authorized users should be able to access personal information in an EMR.

Application Service Provider (ASP)

A third party service provider that manages and stores the Electronic Medical Record (EMR) at its data centre, rather than the physician managing and running servers in their own practice. Physicians or their authorized employees have access to the EMR over the Internet or preferably over a private network.

Authentication

A method designed to allow a computer application to verify credentials—usually in the form of a user name and password for single-factor authentication or user name and password plus an access token for multi-factor authentication.

Canada Health Infoway

Canada Health Infoway is an independent, not-for-profit organization funded by the federal government and established in 2001. Canada Health Infoway invests funds and works with partners to accelerate the development, adoption and effective use of digital health solutions across Canada, including implementing an interoperable Electronic Health Record (EHR) system. Canada Health Infoway is accountable to its Board of Directors and the Corporation Members. The Corporation Members are made up of the deputy ministers of health for the 10 provinces, three territories and the federal government.

Circle of Care

Two or more health care providers that are delivering services to the same individual. Those health care providers have implied consent to share information with each other, unless the individual has expressly withheld or withdrawn consent. Health care providers in the circle of care can include organizations that have diagnostic information and professional case consultation information about the patient and share them with the patient's other health care providers. The circle of care should be obvious to the patient and

reflect common practices. “Circle of care” is a term that is used in provincial health information legislation outside of BC, but does not exist in PIPA, where direct patient care is based on “implied consent”. See also “Implied Consent”.

Collection

The act of gathering, receiving, accessing or obtaining personal information.

Confidentiality

In the health care context, it refers to a physician’s or other health professionals’ ethical and legal obligations to protect an individual’s personal health information, unless the individual consents to the disclosure or the disclosure is otherwise authorized.

Consent

The authority that an organization usually needs under PIPA to collect, use or disclose an individual’s personal information. A patient can provide express or implied consent. Implied consent can be “opt-out” or “deemed”. In limited circumstances, PIPA authorizes the collection, use and disclosure of personal information without consent. Consent must be voluntary, and the physician must be able to show that a reasonable person would consider the purpose for which the information is collected, used or disclosed to be appropriate in the circumstances. When providing health care services to a patient, a physician cannot require the patient to consent to the collection, use or disclosure of personal information beyond what is necessary to provide those services. An individual has the right to withdraw or change their consent by giving reasonable notice, and the physician must explain the consequences on the provision of care. See also “Express Consent” and “Implied Consent”.

Data Masking

The process of restricting access to data in an electronic record by substituting real values with random characters that obfuscate or disguise the data. Data Masking can be applied at different levels of granularity depending on the unique circumstances and system capabilities.

Data Stewardship

Also known as accountability, the legal, ethical and fiduciary responsibilities of a physician in managing and protecting personal health information including collection, use, disclosure and retention.

Disclosure

Sharing, exposing or providing access to information, including to another organization, third party or to the individual the information is about.

Disclosure Directive

A written instruction from an individual to mask their Personal Health Information contained in a specific Health Information Bank (HIB), restricting access to that information under the E-Health Act. Health care providers must obtain that individual's express consent to access the personal information, unless an emergency occurs, or other exceptions apply.

E-Health Act

Also known as the Personal Health Information Access and Protection of Privacy Act. Legislation introduced in 2008, it authorizes data flows, imposes specific privacy and security obligations for personal health information, and enhances openness and transparency regarding the sharing of information in the health sector. The E-Health Act applies only to those databases of the Ministry of Health and health authorities that have been designated as HIBs by the Minister of Health. The databases that have been designated as HIBs are the Provincial Laboratory Information Solution, the Client Registry/Enterprise Master Patient Index and the Provider Registry.

Electronic Health Record (EHR)

An electronic record system that contains personal information collected in the delivery of various health care services. Health authorities have their own EHR and there are also provincial and inter-jurisdictional EHRs, including Panorama, a public health information system. The personal information contained in an EHR system is available electronically to authorized users of the system.

Electronic Medical Record (EMR)

An electronic record system within a practice that enables a health care professional, such as a family physician, to record and store the information collected during a patient's visit instead of, or in addition to, a paper file. The EMR may also allow the physician to access personal health information from other electronic health record systems.

Electronic Medical Record (EMR) Vendor

A third party service provider that sells and supports Electronic Medical Record (EMR) software.

Encryption

The process of protecting personal information by encoding data into an electronic form that can only be read by the intended authorized recipient. All personal information of a sensitive nature should generally be encrypted.

Express Consent

A type of consent that occurs when an individual provides verbal or written agreement to the collection, use or disclosure of their personal information, after being informed about the type of personal information being consented to, and the purposes for which the information is being collected, used or disclosed. Express consent can be verbal or written, though it is easier to prove that consent was given if it is provided in writing. Consent to the collection, use or disclosure of personal information cannot be a condition of providing health services, beyond what is necessary to provide those health services.

Freedom of Information and Protection of Privacy Act (FIPPA)

BC privacy legislation that governs how personal information is collected, used, disclosed and protected by public bodies, including health authorities and the Ministry of Health.

Health Authority

Includes the following entities that deliver health care services to British Columbians:

- Provincial Health Services Authority
- five regional health authorities:
    - Fraser Health
    - Interior Health
    - Northern Health
    - Vancouver Coastal Health
    - Vancouver Island Health
- First Nations Health Authority
- Providence Health Care

All personal health information collected, used and disclosed by the health authorities is governed by FIPPA with the exception of the First Nations Health Authority which is governed by PIPA. This toolkit uses the term to refer to the health authorities that are governed by FIPPA.

Health Information Bank (HIB)

An electronic database under the custody and control of the Ministry of Health or a health authority that contains personal health information and is designated by the Minister of Health under the E-Health Act as a HIB. The designation order authorizes specific data flows and establishes the privacy and security framework for the HIB.

Implied Consent

An individual's implied agreement to the collection, use or disclosure of their personal information by an organization that takes the form of either opt-out consent or deemed consent. Opt-out consent (see s. 8(3) of PIPA) is a form of implied consent that occurs when an individual receives notice, in a manner the individual can reasonably be expected to understand, that their personal information will be collected, used or disclosed for a specific purpose. The individual must also be provided with a reasonable amount of time to decline after being informed. The collection, use or disclosure must be reasonable, having regard to the sensitivity of the information in the circumstances, and must be limited to the purpose set out in the notice. Deemed consent (see s.8(1) of PIPA) is the second form of implied consent, where an individual volunteers information for a purpose that is obvious, and a reasonable person would think that it was appropriate for the individual to volunteer that information in the circumstances.

Information-Sharing Agreement (ISA)

A written agreement that sets out the terms and conditions for the collection, use and disclosure of personal information by an organization or public body from or to an individual or third party (such as a service provider). An ISA should generally include the specific purpose of the agreement, a description of the personal information covered by the agreement and how it will be collected, used and disclosed, any conditions or limitations on the collection, use and disclosure and information on maintaining the accuracy of the personal information, the security arrangements employed and how compliance with the agreement will be monitored and reviewed. Public bodies have specific requirements for ISAs in s. 69 of FIPPA, and information in a health information bank may only be disclosed if the ISA requirements in s. 19 of the E-Health Act are met.

Mobile Device

A handheld mobile device that provides computing, information storage or retrieval capabilities for personal or business use (e.g., Blackberry). Such devices are frequently used to maintain an electronic schedule or contact information.

"Need to Know" and "Least Privilege" Principles

The "need to know" principle states that authorized users of a system should only have access to the minimum amount of personal information that is necessary to perform their duties within a public body or an organization. The "least privilege" principle requires that each authorized user in a system be granted the most restrictive access privileges needed for performing authorized tasks. The principles are reflected in privacy law but not always expressly stated.

Personal Health Information

Information about an individual that is collected, used or disclosed as part of a medical record for the purpose of delivering health services to that individual. In the E-Health Act, personal health information is defined as "recorded information about an identifiable individual that is related to the individual's health or the provision of health services to the individual".

Personal Information

Information, including personal health information, about an identifiable individual which includes factual or subjective information about that individual. This information includes, but is not limited to, name, personal address, birth date, physical description, medical history, gender, education, employment and visual images such as photographs or videotapes.

Personal Information Protection Act (PIPA)

BC privacy legislation that governs how personal information is collected, used, r disclosed, and protected by private sector organizations, including physicians' private practices and other private health care facilities.

Personal Information Protection and Electronic Documents Act (PIPEDA)

Federal legislation that governs the collection, use and disclosure of personal information by federally regulated private sector organizations.

Privacy

The right to be free from intrusion, influence or interruption and to control one's personal information. It is linked with other fundamental rights such as freedom of expression, security of the person, dignity and personal autonomy. Privacy also includes the right of individuals to determine when, how and to what extent they share information about themselves with others.

Privacy Breach

Unauthorized access, collection, use, disclosure, or disposal of personal information.

Privacy Impact Assessment (PIA)

An assessment tool/process that identifies the privacy risks of a proposed initiative involving the collection, use or disclosure of personal information and the steps that will be taken to mitigate those risks.

Privacy Management Program

A program that demonstrates an organization's accountability for personal information and capacity to comply with applicable privacy laws and related industry standards, as well as correctly identifying, addressing or minimizing privacy-related obligations and risks. Includes appointing a privacy officer, responding to requests for access and complaints under PIPA, and developing, implementing, maintaining and updating policies, systems, procedures and training for collection, use, disclosure, consent, notification, access to information, retention, disposal, privacy breaches and corrections. See also "Privacy Officer".

Privacy Officer

The individual designated to be accountable for ensuring organizational compliance with privacy legislation, industry standards for privacy and privacy-related professional and regulatory obligations. In a medical practice, one physician must be designated as the privacy officer. If it is a solo practice, the solo physician is the de facto privacy officer. The responsible physician may choose to delegate

responsibilities for the privacy management program to an employee but they remain ultimately responsible.

The privacy officer is responsible for

- developing policies and procedures
- implementing program controls
- designing and implementing employee training and education
- conducting ongoing assessments and revising program controls
- monitoring for compliance
- managing privacy breach incidents
- managing complaints
- answering questions
- responding to requests for access to or correction of personal information
- demonstrating leadership in creating and maintaining a culture of privacy
- being informed of any privacy related changes in legislation

Private Network

A secure, private, end-to-end network that allows secure, high-speed access to an EMR or an EHR, secure Internet access and secure email messaging.

Reasonable Security Measures

The measures taken to protect personal information from unauthorized collection, use or disclosure by implementing physical controls (e.g., locked cabinets, securely stored laptops or key card access), technical controls (e.g., firewall, document encryption or user access profiles) and administrative controls (staff training, privacy policy or retention and destruction policy). Factors to consider when implementing reasonable measures include the sensitivity of the personal information (medical records are considered highly sensitive), the likelihood of a privacy breach, the harm caused if a breach occurred, the type of record involved, the cost of the security measures and current industry standards.

Remote Access

The ability to get secure access to a computer or network from outside the practice. Individuals who are travelling or working from home may need access to information and may access the network and systems remotely.

Role-Based Access

A policy and technical architecture involving the assignment of access privileges to roles based on job functions rather than to individual users. Users are granted privileges in accordance with the "need to know" and "least privilege" principles by virtue of being authorized to act in specific roles.

Security

Controls that protect personal information from unauthorized collection, use or disclosure. Examples include locking cabinets, or in relation to electronic records, password protections, encryption and firewalls. See also "Reasonable Security Measures".

Staff

May include employees, locum physicians, associates, visiting specialists, medical students, residents, physicians-in-training, contractors and volunteers with whom you collect, use or disclose personal information.

Strong Password

A password that is sufficiently long or random such that it is producible only by the user who creates it. It is case sensitive and includes a random combination of alphanumerics and symbols. The College recommends that a strong password should be eight or more characters in length and contain at one or more numbers, upper and lower case letters and symbols (e.g., IloveParis!936).

Third Party

In the context of personal information that is controlled by a practice, refers to anyone outside the practice or the individual the information is about.

Two Factor Authentication

The combination of user name/password (something an authorized user knows) and some other physical identification tool like a secure ID token (something an authorized user has), which are both required in order to verify the identity of a person.

Use

Any operation (other than collection or disclosure) performed on, or use made of, personal information by the practice or third party that collected the information for a specified purpose.

USB Memory Key

A compact data storage device that is typically removable and rewriteable. The most common use of USB memory keys are to transport and store files such as documents, pictures and videos.

Virtual Private Network (VPN)

An authentication and encryption method that allows connection from outside the practice to the EMR over the Internet with enhanced security.