Guidelines for Confidentiality Agreements, Service Contracts and Information Sharing Agreements

This section will:

- identify key elements to include in confidentiality agreements
- identify key privacy-protective elements to include in service contracts
- identify key elements to include in information sharing agreements (ISAs)

Service providers, suppliers, partners, employees, and others may be engaged by physicians to assist them in their practices. During their work, these third party individuals or organizations are likely to be exposed to personal information in the custody and control of the practice. Therefore, depending on the situation, privacy-protective contractual clauses, confidentiality agreements, and ISAs should be in place to ensure that third parties comply with the practice's expectations that personal information will be appropriately safeguarded in compliance with PIPA. If third parties must collect, use or disclose personal information as part of their contractual obligations, it's important to ensure they have the legal authority to do so.

Confidentiality Agreements

A physician's obligation to safeguard personal information means having internal staff and third parties who have access to personal information sign a confidentiality agreement. Some of the elements to be included in a confidentiality agreement include establishing what personal information must be kept confidential and what security safeguards are required, clarifying who has custody and control of the personal information, and what the consequences are for non-compliance with the agreement. These sample confidentiality agreements may be used as a guide:

- Confidentiality Agreement for Employees
- Confidentiality Agreement for Third Parties
- Confidentiality Agreement for Health Authority Employees Working in a Physicians Private Practice

Privacy Considerations in Service Contracts

Before entering into a service contract with an external service provider (e.g., application service provider, EMR vendor, record destruction services, storage retrieval services), physicians can protect personal information by ensuring:

- Service providers have effective and comprehensive information management practices that are at least equal to those implemented by the practice
- Contracts include the appropriate security arrangements and privacy protection clauses

These requirements should be monitored and enforced by the service provider. For service providers that frequently handle sensitive personal information as part of the contract, the practice should undertake audits to verify compliance.

When preparing a contract with a service provider, the following elements may be included:

- Identification of:
    - all applicable privacy laws and clearly state that the service provider must comply with these as well as their own privacy laws and policies
    - the purposes for which the personal information can be collected, used, or disclosed based on the patient's initial consent and restrictions on any further use to those purposes, except as permitted or required by law
    - who will maintain custody or control of the personal information
    - all reasonable physical, administrative and technical safeguards to protect the personal information from unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks
    - any financial or other consequences that may result from non-compliance with the contract
- A requirement that service providers:
    - only collect, use, access and retain the information provided to them as identified in the contract
    - only allow access to subcontractors after the practice is made aware of it and has approved their access
    - allow the practice to access its information upon request and never deny access because of a disputed payment for services
    - notify the practice if any personal information has been lost, stolen, used, or accessed in an unauthorized manner
    - report any privacy breach or security incident within an agreed-upon timeframe
    - return or destroy personal information when the contract ends as specified
- It is recommended that only service providers who store and access personal information within Canada be engaged. However, many service providers do operate some or all portions of their services out-of-country for a variety of reasons. In these circumstances, the contract should specify:

- where personal information is being stored, who has access, and what security provisions are in place
- in situations where there are remote access capabilities, from what locations personal information may be accessed
- for any aspect of the service provider's operations that are out-of-country, the contract binds the service provider to PIPA, as their own jurisdiction may not have any or adequate privacy laws, compared to BC standards

For information on service contracts for record storage and destruction, see:

- Guidelines for Protecting Medical Records When Leaving a Practice
- Guidelines for Secure Destruction of Personal Information

Guidelines for ISAs

If sensitive personal health information is shared with third parties on a frequent and regular basis (e.g., with health authorities or specialists), an information-sharing agreement (ISA) should be in place. ISAs help clarify how personal health information will be exchanged and how it will be protected.

ISAs can also assist in supporting new and evolving models for structuring a practice. For example, physicians may implement different organizational models based on whether they choose to have electronic medical records (EMRs) or a paper-based system. If personal health information in an EMR is shared with third party care providers, ISAs can help determine who is accountable for the personal information affected, who has custody and control, what the authorities are for collecting, using and disclosing personal information, and what security safeguards are in place to protect personal information.

An ISA will usually:

- reference all applicable legislation that provides the legal authority for collection, use, and disclosure of personal information
- identify:
  - types of information each party will share with each other
  - the purpose for data sharing
  - permitted uses for the specified purpose
  - disclosure restrictions
  - retention periods

- who has custody and control of the information

- describe:
  - what personal information will be shared
  - who will have access and under what conditions
  - how personal information will be exchanged
  - security safeguards in place to protect personal information
  - secure destruction methods when retention expires
  - processes for:
    - responding to access requests by individuals whom the personal information is about
    - ensuring accuracy
    - managing privacy breaches, complaints, and incidents
    - terminating the agreement

The Canadian Medical Protective Association (CMPA), in partnership with the Canadian Medical Association, has produced Data Sharing Principles for EMR/EHR Agreements.