# RISK NOTE

HIROC

## Contracts – Data Sharing Agreements

### OVERVIEW OF ISSUE

Data sharing agreements are contracts which outline terms and conditions for collecting, using, exchanging, retaining, or disclosing data/information for a defined purpose within a defined timeframe between two or more parties. In addition, they specify provisions related to accountability for maintaining the security and privacy of the shared data/information. From a risk management perspective, important requirements included in data sharing agreements are specifications for who owns the shared data/information, how confidentiality will be maintained, and security and safeguards taken by each party to protect the data/information during transmission and/or in storage.

HIROC recommends that subscribers have their corporate counsel (and privacy officer if personal health information is involved) review all contracts.

Refer to related Risk Notes: Contracts – Important Provisions, Contracts – Indemnification Clause with Hold Harmless and Defense Provisions

### KEY POINTS

- Data sharing agreements must delineate who is accountable for maintaining the security and privacy of the shared data/information.

### THINGS TO CONSIDER

#### Common Clauses

- A data sharing agreement typically includes clauses related to the following:
  - Ownership of data;
  - Confidentiality and privacy;
  - Security and access;
  - Accuracy and data quality;
  - Record maintenance requirements;
  - Quality assurance;
  - Scope of services and functionality;
  - Termination for convenience;
  - Termination and the continuity of operation of the electronic medical system;
  - Indemnification;
  - Limitation of liability;
  - Representation and warranties;
  - Dispute resolution;
  - Funding; and
  - Governing law.

#### Purpose

- Data sharing agreements should specify what data/information is being shared between parties and the purpose for sharing this information.

#### Ownership of Data

- Data sharing agreements should specify:
  - Which party has ownership of the data being shared and who owns the data at the termination of the agreement;
  - Who has access to the shared data/information and why;
  - 
  - Accuracy of the data/information, method of exchange, its frequency and duration.

#### Retention

- If patient data is being shared, the original data should be retained in the health record.

#### Confidentiality and Privacy

- Data sharing agreements should:
  - Clarify applicable provincial/territorial legislation governing the protection of personal health information and remind the parties of their obligations to comply with the legislation;
  - Outline what patient information can be collected, used, retained, and disclosed on the basis

# Contracts – Data Sharing Agreements

of implied consent. If explicit patient consent is required, this should be stated;
- Consider if confidentiality should survive termination of the agreement;
- Clarify how data/information will be returned/destroyed at the termination of the agreement. A secure method of destruction is paramount and should be detailed in the agreement if applicable. If the data/information is not returned/destroyed at the termination of the agreement, the agreement should outline the retention period;
- Clarify how responsibility for costs and notifications for privacy breaches will be addressed.

- Relevant organizational policies may be referenced in this section of the agreement, e.g. confidentiality policy and the need to sign a confidentiality agreement.

## Safeguards and Security

- Data sharing agreements should:
  - Specify security measures, safeguards, and precautions to be taken to minimize the risk of loss, corruption, theft, or unauthorized access to shared data/information. Typical safeguards include: encryption, firewalls, strong password policies, secure file transfer, data back-up strategies, audits to determine unauthorized access, etc.;
  - Outline what happens if there is a privacy or security breach and the process for patient notification if required. This includes consequences for improper use or disclosure of patient information.

## Key Contacts

- Data sharing agreements should include key contacts should something go wrong and a contact person(s) at the organization needs to be notified quickly. This typically differs from the individual who signs the contract as they may be less accessible in an emergency.

## Insurance

- The insurance clause should include a thirty-day prior notice of material change to, cancellation and non-renewal of the insurance policy. This is important so that all participants are aware of significant changes in coverage.
- Ensure the third party's insurance includes:
  - Privacy breach costs, including notification;
  - Cyber coverage.

## REFERENCES


- Canadian Medical Association. (2009). Data sharing agreements: Principles for electronic medical records/ electronic health records.
- Canadian Medical Protective Association. (2014). Electronic records handbook.
- Sawatsky E. (2010). Information sharing agreements for disclosure of EHR data within Canada.
- Service Alberta. (2003). Guide for developing personal information sharing agreements. Freedom of Information and Protection of Privacy Act.






Date last reviewed: October 2017