Policies and Regulations

PR-006

Procedure for managing confidential information

July 2019

Preamble

Considering the need to manage confidential information with a high level of professionalism and discretion, SIRIUSMEDx is issuing this procedure to clearly outline the steps to be taken and the process for managing confidential information.

›

Confidential Information

Confidential Personal Information

Personal information is information that relates to a natural person and allows that person to be identified. It is confidential. With few exceptions, it cannot be communicated without the consent of the person concerned. The following is a non-exhaustive list of this information:

Identification

- Signature
- Social Insurance Number
- Date of Birth

Work

- Disciplinary File
- Salary
- Vacation dates

Health

- Medical Record
- Drugs consumed and prescriptions issued
- Hospitalization

Finance

- Bank account of a natural person
- Credit card information of a natural person
- Property owned by a natural person

Confidential Information of a non-personal nature

his information may allow a third party to gain a competitive advantage or compromise the internal security of SIRIUSMEDx. The following is a non-exhaustive list of such information:

Informations of a strategic nature

- Recruitment of personnel
- Internal compensation policies
- Working conditions
- Financial Statements

Information that may pose a threat

- Security Incident Information
- Details of vulnerabilities related to security mechanisms
- Secrets, such as encryption keys
- Administration code passwords
- Source code for applications developed by the organization

Internal Management Information

- Service reorganization before the official announcement
- Abolition of position before official announcement
- Internal survey
- Policies, directives, processes, procedures...

Protect confidential information

Here are a few tips to help you better protect confidential information:

- Make sure that access is granted on an as-needed basis
- Adopt a good management of your passwords
- Deposit your documents in a directory with the appropriate protection for the type of document
- Preserve the confidentiality of documents during their communication and transportation
- Be sure to store your paper documents in a secure location, such as a filing cabinet that you can lock.

Classifying confidential information

In order to ensure effective management of confidential information, SIRIUSMEDx classifies data into three categories:

Category A: Medical Information
This information is accessible only by a health care professional duly authorized in the course of his or her duties to consult it. Each consultation of a medical record must be recorded in order to ensure the traceability of patient records.

Category B: Personal, but not medical information
This information is accessible only by SIRIUSMEDx administrative employees or managers who are authorized to view it in the course of their duties.

Category C: Non-personal Confidential Information
This information is accessible to employees, consultants or subcontractors provided that they are authorized in the course of their duties to access this type of document.

Storage of Confidential Information

To ensure the proper and secure storage of confidential information, SIRIUSMEDx implements various security measures. These measures are adapted according to the classification of confidential information :

Category A

- The electronic version is only accessible by the healthcare professional(s) needing access to the medical documents. The electronic version is protected by restricted access and a one-time professional password.
- The paper version is only accessible by the health professional(s) needing access to the medical documents. The paper version must always be kept under lock and key and only accessible by duly authorized persons. When the document is archived at the head office, a consultation register must be signed at the time of consultation with the reason for consultation.

Category B

- The electronic version is only accessible by the employee who needs to access the documents. The electronic version is protected by restricted access and a one-time password.
- The paper version is only accessible by the employee who needs to access the documents. The paper version must always be kept under lock and key and only accessible by duly authorized persons.

Category C

- The electronic or paper version of a document containing confidential information is only accessible and given to persons duly authorized by the organization.

Access to Confidential Information

The professional, employee, trainee or subcontractor wishing to have access to certain confidential information must make a written request to his or her manager. The manager must then complete the access request form, specifying the type of documents the person may be required to consult and forward it to the person responsible designated by the Branch.

Transmission of confidential information

When Category A information is to be transmitted by e-mail to another authorized person, the e-mail must be encrypted to promote security and ensure confidentiality. Category B or C information should be sent in the most confidential and secure manner possible and never to more than one person at a time.

Destruction of Confidential Information

When confidential information must be deleted or removed, the paper or computer media must be completely destroyed. It is therefore essential that paper documents be shredded before being sent for recycling or to the garbage.

Retention period of documents

The company relies on data provided by the office of the National Archives of Quebec as well as on the recommendations of the Canadian Medical Protective Association or other relevant legislation.

Deadline	Documents
1 year or less	• Invoices for supplies, goods or services; • Bank or credit card transaction statements; • Collective insurance documents;
2 years	• Applications and candidate files;
3 years	• Property tax receipts; • Utility bills (electricity, gas, oil, water, etc.); • Health care and professional fees bills; • Employee records (after termination of employment); • Pay statements and supporting documents;
4 years	• Quebec Pension documents;
5 years	• Information used in a pay equity program; • Records of an occupational health and safety committee; • OHS sampling and measurement records;
6 years	• Contract of sale of a house, building or land; • Income tax return and supporting documents; • Instalment, GST and QST/PST payment statements; • Mortgage Discharge; • Job related training; • Records of employment (or until the end of a dispute);
10 years	• Medical records from all provinces except British Columbia;
16 years	• Medical records from British Columbia;
20 years	• Medical records of a worker; • Work accident/disease claims records; • Record of workstations, duties and conditions;
While in possession of an asset/goods	• Lease • Invoice and warranty contract for an appliance; • Invoice and warranty contract for a good over 500$; • Invoice and statement of account for a good paid with a credit card; • Invoices for services or leisure activities; • Lease and insurance contracts • Mortgage Loan Agreement • Certificates of deposit or investment