Manual : General of Vitalité Health Network

Title :	CONFIDENTIAL INFORMATION SHARING		**N° : GEN.6.30.30**
Section :	6. Information Management	**Effective date:**	**2015-03- 18**
Issued by :	Regional Director Integrated Risk Management and Regional Chief Privacy Officer	**Date of last revision :**	2012-01-16
Approved by: (Signed by)	President and Chief Executive Officer Jean Castonguay	**Date approved / signed :**	2015-03-18
Facility / Program :		☑**Vitalité Zone :** ❒ 1 ❒ 4 ❒ 5 ❒ 6	

This is a joint policy of the Chief Privacy Officers' Working Group and shall not be modified except by agreement of that group.

INTRODUCTION

Each of the Regional Health Authorities (RHAs), FacilicorpNB and Ambulance NB, as health system partners (herein referred to as "the Partners"), is committed to collecting, using, disclosing and disposing of personal information (PI) and personal health information (PHI) entrusted to us in a manner that is accurate, confidential, secure and private.

OBJECTIVE

The purpose of this policy is to prescribe the processes that shall be undertaken in the sharing of confidential information, taking into account the sensitivity of the information being shared.

SCOPE

This policy applies whenever a Partners' employees or non-staff personnel are engaged in the sharing of confidential information, including personal information (PI) or personal health information (PHI).

LEGISLATIVE REQUIREMENTS

The Partners are subject to and must comply with the *Right to Information and Protection of Privacy Act* (*RTIPPA*), *the Personal Health Information Privacy and Access Act* (*PHIPAA*) and their regulations.

DEFINITIONS

The "**non-staff personnel**" includes, but is not limited to, board members, agents, students, volunteers, physicians, consultants, third-party service providers, external professionals or experts contracted to offer a service and vendors, demonstrating, installing or servicing equipment, software applications or hardware.

The "**confidential information**" includes, but is not limited to, the following information types:

- Personal information (PI)
- Personal health information (PHI)
- Sensitive / proprietary information (i.e., administrative information documented in personal notebooks / diaries)
- Human Resources / Payroll
- Legal
- Financial

The "**personal health information**" means identifying information about an individual in oral or recorded form if the information:

(a) relates to the individual's physical or mental health, family history or health care history, including genetic information about the individual,
(b) is the individual's registration information, including the Medicare number of the individual,
(c) relates to the provision of health care to the individual,
(d) relates to information about payments or eligibility for health care in respect of the individual, or eligibility for coverage for health care in respect of the individual,
(e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any body part or bodily substance,
(f) identifies the individual's substitute decision-maker, or
(g) identifies an individual's health care provider.

The "**personal information**" means recorded information about an identifiable individual, including but not limited to:

(a) the individual's name,
(b) the individual's home address or electronic mail address or home telephone or facsimile number,
(c) information about the individual's age, gender, sexual orientation, marital status or family status,
(d) information about the individual's ancestry, race, colour, nationality or national or ethnic origin,
(e) information about the individual's religion or creed or religious belief, association or activity,
(f) personal health information about the individual,
(g) the individual's blood type, fingerprints or other hereditary characteristics,
(h) information about the individual's political belief, association or activity,

(i) information about the individual's education, employment or occupation or educational, employment or occupational history,
(j) information about the individual's source of income or financial circumstances, activities or history,
(k) information about the individual's criminal history, including regulatory offences,
(l) the individual's own personal views or opinions, except if they are about another person,
(m) the views or opinions expressed about the individual by another person, and
(n) an identifying number, symbol or other particular assigned to the individual.

POLICY STATEMENT

The sharing of confidential information should only occur when it is appropriate and authorized by law.

Employees and non-staff personnel are accountable for how they handle confidential information, including PI and PHI, and should exercise appropriate caution when sharing such information, including the method by which the information is sent, in order to preserve confidentiality and privacy.

If an error is suspected or confirmed when sharing confidential information, it must be reported to your supervisor and to the Chief Privacy Officer of your organization immediately, as outlined in the Privacy Breach Policy.

PROCEDURE

In order to determine the most appropriate means for transmitting confidential information, including PI and PHI, individuals must evaluate their communication practices according to this policy and other known best practices where available.

General Considerations for the transfer of Data/Information

1. Face-to-Face Communication

   Confidential information that is transferred in a face-to-face situation should be done in a secure and private area such as a room with full partition walls and a closed door. If such an area is not available, discretion and good judgment must be exercised.

2. Non-Staff personnel

   When sharing confidential information with non-staff personnel, ensure that the individual or entity has signed a Confidentiality – Declaration of Understanding (as referred to in the Confidentiality Policy).

   For contracts with a third party, a data sharing agreement may also be required.

   The data sharing agreement should be completed in consultation with the Privacy Office.

3. Transporting Confidential Information in Paper Format

Carrying confidential information in a paper format ***within your facility*** should be limited. Precautions should include:

- Placing the information in a closed file folder, an interoffice envelope, on a clipboard with cover or in a box with cover so it is not readily viewable.
- There must not be any PI or PHI written on the envelope except as necessary for the delivery of the information.

Health records shall never be taken out of the facility unless by court order or special permission from Health Records. Patient records used by community services such as Public Health, the Extra-Mural Program, and mental health centres, can be brought in the community according to their respective policies.

Carrying confidential information in a paper format ***outside your facility*** should be limited. Additional precautions might include:

- Ensuring that confidential documents are not misplaced by tracking the removal from and the return of the information to its original storage area.
- Transporting only the minimal amount of information required.
- In the case of PHI, information must be transported in a secure manner, such as a locked briefcase and in the locked trunk of the vehicle.
- Confidential information should never be left unattended in a vehicle especially overnight.

For Ambulance New Brunswick, the above provisions are not applicable due to the nature of the business. While confidential information will be transferred directly to an agent, it may or may not be concealed in a folder or envelop.

4. Mail

4.1 Internal Mail

4.1.1 Sent within the same facility:

- Confidential mail sent within the premises of a facility must be placed in an interoffice envelope or in a sealed envelope, sealed at source, before being sent. The recipient's name and department must be clearly indicated on the envelope. There should be no PHI or patient label in the envelope.

- As for confidential documents that are **delivered directly to the mailboxes of physicians** by RHA staff members, these must be folded and the full name and family name of the physician to whom the documentation is addressed should be clearly indicated.

4.1.2 Sent to another facility within the Health Network:

- Mail containing confidential information, PI, or PHI sent to another facility within the Health Network and delivered by FacilicorpNB must be placed in an envelope and sealed before being sent to the mailroom, with the recipient's full name, department name, and

facility name indicated. The sender's contact information must also appear on the envelope. The envelope should be clearly marked "Confidential."

4.2 Regular Mail

To send PHI, PI, or confidential information through a mailroom (internal mail, regular mail, or through a company), the steps below must be followed:

- The information must be placed in a single-use envelope that is sealed at source (before being sent to the mailroom);
- The recipient's full name (first name and family name), department name, and full address must appear on the envelope;
- The sender's information (name and return address) must also appear on the envelope:
- The envelope must be marked "Confidential."

If the document or package is sent by registered mail or through a courier company, it must be trackable (have a tracking number).

5. Telephone

Landlines are generally considered a secure means of transmitting confidential information, provided the telephone is in a secure and private location.

Cordless, cellular, Blackberry or any other types of Smart or satellite phones devices are not considered entirely secure; therefore, unless another method is not readily available, one should limit the amount of identifiable information given over the telephone.

When contacting a patient and a voice message is required, leave only enough information on the telephone answering machine to be useful to the patient, such as:

- Your name.
- Where you are calling from (not program or provider specific; you can identify the name of the Regional Health Authority).
- Basic information about what the call is about (reminder of the patient's upcoming appointment or a change in the patient's appointment time).
- The message should not contain any specific information about the appointment, including the nature or location of the appointment, unless the patient has consented to, or asked for, a more detailed message.
- A call back number.

Example:

This is (name of employee) from Vitalité Health Network calling for (name of patient) regarding your upcoming appointment on (date and time). It is important that you call me at (number) to confirm that you will be attending this appointment

or that you are unable to attend so that we can reschedule your appointment. Thank you.

For booking departments that are contacting patients by telephone on short notice and leaving a voice message, it is permissible to leave the name of the department in the voice message.

When an outside caller is requesting information on a client, PHI on the client can only be discussed when the identity of the caller can be confirmed by the caregiver and that caregiver has obtained prior consent from the client to share his/her information with the caller.

6. Fax

When considering whether to fax confidential information, the following general process should be observed at a minimum:

- Faxes must use a cover sheet which includes a confidentiality notice for confidential information received in error. For example, a confidentiality notice such as the following may be used:

Confidentiality Notice

This fax may contain confidential and privileged information intended to the addressee only, Disclosure and reproduction of this information is prohibited. If you have received this fax by error, please notify the sender indicated below. Thank you

506- _____ Name: _____

- Cover sheet must identify the recipient, the date, the fax number of the destination, the total number of pages, any special instructions and the telephone number and name of the sender in case of need; no personal information or personal health information should be included.
- Sender must use pre-programmed fax numbers to avoid errors
- Sender must double check the recipient's fax number.
- Under especially sensitive circumstances such as related to mental, sexual health, the sender must notify the recipient that the fax is coming and request that the recipient confirm that the fax has been received.
- The sender must also verify, upon transmittal confirmation, that the faxed telephone number was the intended fax number.
- The fax machine should be located in a secure area.

Fax to e-mail transmission is another means of transmitting confidential information. It limits the access to confidential information at the receiving end and it's considered a more secure alternative than fax to fax transmission. To assure the security of a transfer, the sender should double check the e-mail prior to sending or asks for a confirmation of receipt from the receiver for example.

Unintended Transmission or Receipt of Transmission:

If a confidential fax has been sent to the wrong recipient, the sender must:

- Contact the recipient to advise them of the error,
- Contact the Chief Privacy Officer to report the incident,
- Ask the unintended recipient to securely destroy the document and confirm the destruction verbally.

If you receive a confidential fax in error you must:

- Contact the sender to advise them of the error;
- Contact the Chief Privacy Officer to report the incident;
- Destroy the document as directed by the sender and confirm the destruction.

7. Sending Confidential Information to a Printer

- The printer should be in a secure location;
- Documents containing confidential information which are sent to the printer must be retrieved immediately;
- Sending documents containing confidential information to a printer in another location should be done with caution. Ensuring proper secure transmission should include measures such as using a confidential print option when available on printers, checking and confirming printer number or code, or again ensuring someone is present to retrieve the information. To use the confidential print option on most printers, click the print button followed by the properties button under which you should access the settings for a confidential print option.

8. Electronic Transfer of Confidential Information

The organization's confidential information should never be transferred to a device not supplied to you by the Network.

8.1 E-mail

In general, e-mail cannot be considered entirely secure for the transmission of confidential information. However, compared to alternative means of information sharing, **e-mailing within a single network is not technically considered a high risk**.

The following addresses are considered "trusted networks", when communicating with each other:

- firstname.lastname@horizonnb.ca
- firstname.familyname@vitalitenb.ca
- name@facilicorpNB.ca
- name@nbed.nb.ca
- name@gnb.ca

For AmbulanceNB, only internal e-mails are permitted (i.e., to and from name@anb.ca and name@smunbems.ca only).

In order to ensure completeness of the patient chart, which is the legal record, communications undertaken by e-mail must be limited to a strict minimum and, when required, the clinical content reflected in the client's record.

Best practices when using e-mail include:

- Before sending a message, verify that the recipient(s) are as intended;
- Personal information or personal health information shall not be included in the subject line;
- Care should be used when directing messages to a distribution list to ensure that all users on the list are authorized and intended to receive that information;
- Indicate that the information is "confidential" by entering this statement at the very beginning of the body of the e-mail;
- If you send a message to someone by accident, try to "recall" the e-mail. The recall function for e-mails has very limited effect and should not be relied upon. Therefore, you must also send the unintended recipient an e-mail explaining that they received a message in error and ask that they permanently delete the e-mail immediately;
- If multiple recipients received the message, and one of the recipients was included by error, you must notify all recipients to remove the unintended recipient before they "reply to all";
- When sharing PHI by e-mail inside a trusted network, encryption is not mandatory but due caution should be observed.

E-mailing outside the organization's network

E-mailing PHI outside trusted networks **is not** secure and can only be done if the following steps are followed:

- A bilingual confidentiality notice should be attached to all electronic transfer sent outside your network;
- When sharing PHI by e-mail outside the trusted networks (listed above) encryption is required unless one of the following two conditions is met:

i) A patient has consented to communicating with the user via e-mail. The healthcare provider and patient should have an established relationship.
ii) The e-mail is required for a one-time, emergency health purpose between care providers. In such cases, the sender must follow up using alternative communication methods, such as phone, to ensure the information reached the intended recipient and is being handled with appropriate care.

- Unencrypted personal health information must not be sent via e-mail over the Internet to an employee's home e-mail address to enable the employee to complete work at home.

Sending and receiving e-mails from patients

Authorized care providers may communicate with patients/clients via e-mail to support that patient's care if the following conditions are met:

1. Program directors and managers must define the type of information that can be sent via e-mail and obtain approval from their organization's Chief Privacy Officer.

2. Care providers wishing to use e-mail to communicate with patients/clients must identify in writing, with the patient, the types of transactions (e.g., appointment scheduling, prescription refill) and level of sensitivity of messages that can be sent by e-mail, in accordance with the program's policy.

3. Care providers must obtain express (written) consent from individual patients/clients to communicate with a patient/ client by e-mail. Consent should be obtained in person at the time of a patient's appointment. Consent may be obtained by mail if a long-standing relationship exists between a care provider and patient, and patient appointments are infrequent. No exchange of information through e-mails is allowed prior to obtaining, in person, a written consent.

4. A signed copy of the consent must be filed on the patient's health record.

5. Once patient/client consent has been obtained for e-mail communications, care providers must respect the following e-mail policies:

    - Document the relevant clinical content of any communication (i.e. email, phone, etc.) within the progress notes of the Patient's/Client's record.
    - Instruct patients to put the category of the transaction in the subject line of the e-mail message, e.g., prescription, appointment, medical advice, or billing question.

8.2 Texting

This method of communication cannot be used when confidential information is involved, unless texting a patient or client is the only method of contact available. The message should contain the minimum information required. Before proceeding with this type of communication, a written informed consent should be obtained from the patient or client.

8.3 Transferring Data Electronically

When transferring data electronically, appropriate safeguards must be used. Contact should be made with Information Services to determine the appropriate method for transfer.

Best practices include:

- Password protection - the sender should notify the receiver of the password by a separate method;

- Using a limited access shared drive;
- Adherence to an appropriate file transfer protocol, such as the Secure File Transfer Protocol (SFTP), Virtual Private Network tunnel (VPN tunnel), etc.;
- Use of encryption technology

8.4 Dial up Modem or Network (non-high speed)

A dial-up modem uses telephone lines to transfer data from one computer to another. Dial-up modems are an acceptable method to transfer confidential data between individuals, provided the dial-up modem is a direct connection to the designated server or host. A dial-up modem connected to an Internet Service Provider is NOT an acceptable method of transferring information unless encryption software is used.

ACCOUNTABILITIES

Accountability for management of PHI rests with the respective CEO's of the Partners. The Chief Privacy Officers of each Partner have been delegated to act on behalf of its CEO.

Each **Partner** is responsible for:

- Ensuring resources are available to support compliance with privacy policies and procedures;

Chief Privacy Officer is responsible for:

- Maintaining policies and tools to support confidentiality and effective information sharing practices;
- Assisting with identification of privacy and security risks and mitigation strategies.

Managers are responsible for:

- Identifying privacy and security risks within their area of business and developing appropriate mitigation strategies.
- Ensure compliance with policies and procedures related to protection of PI and PHI.

Partners' employees and non-staff personnel are responsible for:

- Complying with this Policy in the day-to-day collection and processing of PI and PHI to the extent that the Partner identifies as being applicable to them. A Partner may apply sanctions to employees or non-staff personnel acting on its behalf found in violation of this Policy, consistent with the Partner's disciplinary and procurement policies and procedures.

REFERENCES AND ASSOCIATED DOCUMENTS

Personal Health Information Privacy and Access Act
Right to Information and Protection of Privacy Act

INQUIRIES

For more information on this Policy, contact the Chief Privacy Officer *for your organization*.