# Guidelines Regarding Patients' Personal Health Information

# for New Brunswick Dentists

New Brunswick Dental Society
Société Dentaire du Nouveau-Brunswick

520 rue King Street, HSBC Place #820
P.O./C.P. Box 488, Station "A"
Fredericton, N.B. E3B 4Z9
Tel.: (506) 452-8575 Fax: (506) 452-1872

*June 2015*

# TABLE OF CONTENTS

# I. INTRODUCTION

New Brunswick Dentists are "**custodians**" of confidential personal health information and have legal obligations pursuant to the *Personal Health Information Privacy and Access Act* (the "Act").

The New Brunswick Dental Society (NBDS) Privacy Guidelines are designed to assist Members in understanding their obligations as custodians and to ensure best practices in:

- obtaining personal health information;
- keeping personal health information secure;
- the destruction of personal health information; and
- transferring of personal health information between health care custodians.

These guidelines are designed to provide sensible and practical information for Dental Offices and are not intended as a substitute for legal advice. Should you have specific questions regarding the *Act*, you should consult appropriate legal counsel.

## II. THE PURPOSE OF THE ACT

The *Act* has multiple purposes, including:

- Setting rules about the collection, use, disclosure, retention and secure destruction of personal health information;
- Ensuring accountability of people with access to personal health information;
- Safeguarding the security and integrity of personal health information;
- Giving individuals access to their personal health information;
- Permitting individuals to request corrections to their personal health information (ensuring its accuracy and completeness); and
- Further improving the health care system.

## III. WHAT IS "PERSONAL HEALTH INFORMATION"?

Personal health information may be oral, written or photographed and applies to all information media including paper, microfilm, x-rays, and electronic records. Specifically, it will include a patient's

- Name;
- Address;
- Telephone number;
- Email address; and
- Date of birth.

Personal health information will also include a patient's,

- Physical and/or mental health;
- Health care history;
- Family history;
- Genetic information;
- Blood type;
- Health care providers;
- Substitute decision-maker;
- Drugs and medications; and
- Health care aids, products and programs.

*** With respect to dental practices, personal health information will <u>also</u> include information about dental insurance, banking or credit card information that may be collected for payment purposes.**

# IV. COLLECTION, USE AND DISCLOSURE OF PERSONAL HEALTH INFORMATION

Three well-established principles guide the collection, use, and disclosure of personal health information:

## 1: Consent

Unless otherwise provided by law, dentists should always obtain the patient's consent when collecting, using or disclosing personal health information.

In simple terms this means that the patient must understand:

- Your role and the services you will provide;
- What personal information is necessary for you to do your work and why;
- How you will use the personal health information; and
- With whom the personal health information will be shared and why (such as an insurance company for pre-determination or payment, or another health-care provider).

## 2: Collect Only the Minimum Personal Health Information Necessary

Collect the minimum personal health information necessary and take reasonable steps to ensure that the information you collect is accurate, current, and complete.

## 3: Use and Disclose Personal Health Information on a "Need-To-Know" Basis

The use and disclosure of personal health information should be done solely on a "need-to-know" basis. That is, only those individuals (whether other healthcare professionals, or dental office staff) who require access to the personal health information in order to fulfill their employment responsibilities should be provided access to it.

**Example:**
Dental hygienists do not require access to the health information of all patients in the practice; only to those of patients to whom they are providing care and treatment, and only the information required to conduct the treatment.

## Exception - Disclosure Without Consent:

The sharing of personal health information without consent can occur only in specific and limited cases, such as:

- to protect the mental or physical health and safety of a person, group of people or of the public;
- in an emergency situation;
- to comply with a subpoena, warrant, court order, etc.;
- to comply with the law or as required by law;
- to inform a relative or close friend of injury, illness or incapacity; or
- disclosing the information to the NBDS for the Society to fulfill is regulatory mandate.

NOTE: ***The dentist should maintain a written record of any disclosures including information about the date, reason for the release and to whom the information was released.***

# V. IF A PATIENT WANTS TO REVIEW AND/OR CHANGE INFORMATION IN THEIR FILE, WHAT DO I DO?

The *Act* provides individuals with a right of access to their personal health information and a right to require corrections to their information if it is inaccurate or incomplete. The right of access applies not only to information such as a dentist's recorded chart notes, but also to digital records, dental radiographs, impressions, etc.

Under the *Act* a patient can request:

1. to review the file in person; or
2. obtain a copy of the file (but not the original records).

Under the *Act* and pursuant to the NBDS Rules, the dentist's obligations are:

- to respond to a request within **30 days** (can extend for up to an additional 30 days in certain circumstances); and
- to ensure that the patient only gets access to his or her own personal health information as required by law.

***It is recommended that dentists post a notice to ensure patients are aware of the office file retention policy. See Section VIII regarding retention and destruction of patient files.***

Dental office staff can assist a patient with accessing their personal information, or changing information by asking the patient to indicate whether staff has consent to share the information with a spouse or parent. A note placed in the file to that effect can be re-confirmed at subsequent visits to ensure there has been no change, or where there is a change, to indicate the new consent now in effect. This small but effective technique in daily work can prove very effective when staff has to contact patients at home and/or leave messages and/or share information with another family member about the patient.

## Refusal of Access:

In extremely rare circumstances it is possible to refuse a patient's request to review personal health information. These rare circumstances include when:

- the release of personal health information could pose a danger to the person's health or safety, or to that of another person;
- the information could identify a person who provided information in confidence;
- access would reveal information prepared for a legal proceeding (solicitor-client privilege); or when
- **(Common to Dentistry) the information could reveal another person's personal health information (unless it can be removed or the practitioner has express consent to release it).**

# VI. WHAT ARE MY RESPONSIBILITIES?

Dentists have an obligation to safeguard patient health information in order to protect its confidentiality, integrity and availability. There are three broad categories of safeguards that may be applied to secure the information:

## Physical Safeguards:

- Ensure that records are held (or stored) in a secure physical building;
- Position computer screens and fax machines away from public sightlines to prevent viewing/access by unauthorized individuals. (e.g. other patients at the reception desk);
- Do not locate fax machines in areas of the office to which unauthorized individuals have access;
- Ensure that filing cabinets (containing patient records) and other storage areas are kept locked; and
- Institute "clean desk" policies in your clinic: documents containing personal information should never be left unattended.

## Administrative Safeguards:

- Employees should be required to sign an Oath of Confidentiality upon hiring, which is reviewed annually;
- Staff must be knowledgeable about the dental practice's privacy policies and procedures and be trained to implement them;
- Practitioners and staff should avoid discussions of patient information on cell phones and in public areas or where public attends (eg. coffee shops, restaurants, corridors, elevators, etc.);
- Staff must avoid talking about patient files, and especially when identifying information is discussed.
- Ensure regular confirmation of contact information (especially phone numbers and email addresses).
- Each dental office should appoint a staff person to be responsible for maintaining the Privacy protocols within the office.

## Technical Safeguards:

- Ensure strong passwords and encryption for computers, wireless networks and mobile devices;
- Contact your practice management software vendor to ensure that any electronic transmission of data is encrypted and secure;
- Utilize automatic log-offs and machine locking when devices are not in use;
- Maintain audit logs that show who accessed electronic patient charts;
- Ensure that appropriate access controls are in place to allow authorized users within the dental practice to have access only to the patient health information necessary for them to execute their employment responsibilities;
- Mobile dvices must be safely stored when not in use or when unattended;
- Protect electronic dental records systems against malicious software and arrange for system and software updates to be installed in a timely manner; and
- Hold only the minimal necessary patient health information on mobile media (e.g. CDs, back-up drives, laptops, USB flash drives and Smartphones).

**NOTE:**

***Dentists should ensure that staff members who are communicating with patients by telephone and leaving voice messages are trained to leave only the minimum necessary information on the message (e.g., "this message is for Mr. John Doe. Please call the dentist's office @ number"). No information should be left on a voice messaging system that relates to, or could reveal, the nature of the patient's health information that is the subject of the call.***

## Special caution: Social Media

While the use of social media may be viewed as an opportunity for a dental practice to promote its business, dentists need to be cognizant of the risks involved in using social media as a means of communicating with patients. The privacy of their patients and the security and confidentiality of the patient's personal health information **must** be maintained in the online environment and practitioners must not post any identifiable patient information.

# VII. MANDATORY DISCLOSURE OF PRIVACY BREACHES

A privacy breach may occur when personal health information is:

- Lost;
- Stolen;
- Collected, used, disclosed, or disposed of in an unauthorized manner or without consent; or
- Accessed by an unauthorized person.

The best way to prevent a privacy breach is to regularly review your office's *physical, administrative and technical* safeguards to protect the personal health information.

If a privacy breach does occur, the ultimate goal is to reduce the potential harm and prevent future breaches.

### The following steps should be considered:

## 1. Contain the breach

- ✓ This may involve contacting law enforcement in the event that patient health information has been stolen; or
- ✓ It may involve contacting an IT (information technology) security expert to conduct a forensic audit of your system if, for example, it appears that someone has "hacked" your electronic health system.

## 2. At first reasonable opportunity,

- ✓ Notify all persons affected by the breach (those to whom the information relates);
- ✓ Notify the Privacy Commissioner (mandatory under the *Act*); and
- ✓ Inform the New Brunswick Dental Society.

## 3. Implement corrective measures to prevent recurrence

- ✓ It is important to identify the cause of the breach in order to take the necessary steps to ensure that a similar breach does not reoccur and that personal health information is appropriately safeguarded on an ongoing basis.

# VIII. HOW LONG DO I NEED TO KEEP MY FILES?

In accordance with the provisions of the Act, custodians (i.e. dentists) must have a written policy for retention, storage, retrieval and secure destruction of personal health information. As a matter of course, you should share this policy with your patients.

In the context of New Brunswick's *Limitations of Actions* legislation, the New Brunswick Dental Society recommends that patient records be maintained for a minimum of 15 years as some legal proceedings may be commenced 15 years after the act or omission on which the claim was made took place. NBDS makes this recommendation to ensure dentists will be in a position to provide documents in defense of any such legal actions.

NOTE:

***Limitation periods under the Act do not start to run until a claimant reaches the age of 19. Dentists must consider the age of their child patients before any decision is made to destroy a file.***

***NBDS further recommends that you consult legal counsel in the development of a retention policy that is less than 15 years in duration.***

## Destruction of Patient Files

Before disposal, the *Act* requires that the dentist must keep records indicating:

- ✓ The names of patients whose personal health information was destroyed;
- ✓ A summary of the content of the destroyed records;
- ✓ The time period that the destroyed records encompassed (eg. 2004-2014);
- ✓ The method of destruction (e.g. secure shredding, disk wiping); and
- ✓ The name of the person who was responsible for supervising destruction.

# IX. RETIREMENT & RELOCATION

## I am retiring or closing my practice. What now?

A dentist's legal responsibility as custodian of patient health information does not end with retirement or relocation.

When an office is closed, attention must be paid to ensure that patient health information does not become "orphaned": patients must have the ability to access copies of their personal health information. If a dentist ceases to practice dentistry (either because they no longer maintain their certificate of registration or due to death), records should be retained for the periods outlined in the previous section unless:

1) Completed custody and control of the records has been transferred to another custodian (dentist) and each patient is informed of the transfer, or

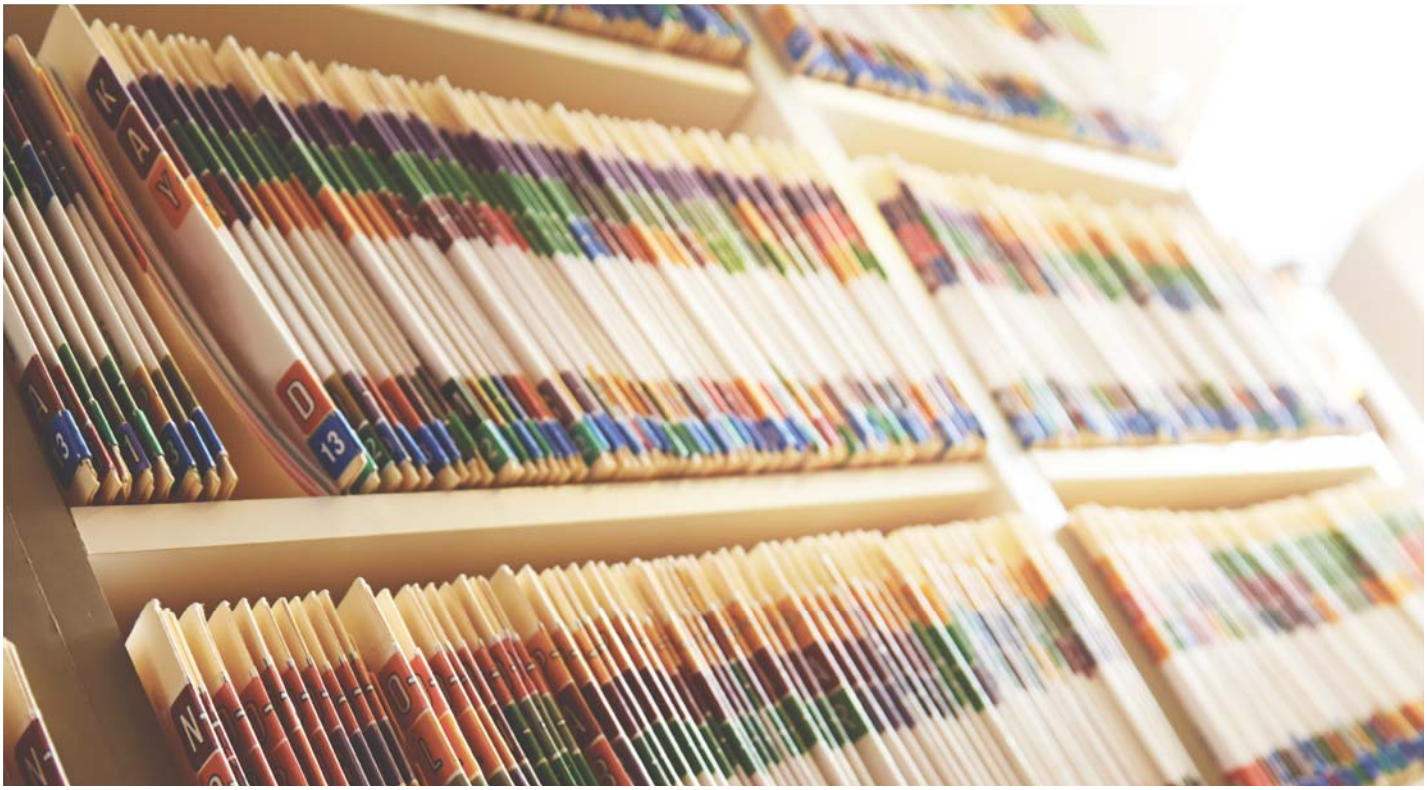
2) Each patient has been notified where their records are and when they will be destroyed following that notification, and in accordance with the NBDS recommended time period.

In any event, patients must be provided with the opportunity to obtain their files. See Appendix D ("Checklist for Custodians in the Event of a Change in Practice.")

NOTE:

***NBDS requires that retiring and relocating dentists contact the NBDS office and provide information regarding the location of records so that the office staff can efficiently address patient inquiries. (See Appendix B: Rule 7.)***

***It is recommended that files be kept for the longer periods not only for the patient's needs but to ensure that dentists have relevant information if there is a civil action within the relevant Limitation of Actions period.***



# IX. FEES RELATED TO PROVIDING COPIES OF FILES TO PATIENTS

The *Personal Health Information Protection and Access Act* of New Brunswick contains provisions regarding the fees that may be charged to a patient for providing the patient with requested personal health information.

A patient may view the file on site for free OR may be asked to pay set fees to obtain a copy of the file as outlined below:

| SEARCH AND PREPARATION | COPYING | DATA PROCESSING | MAIL AND COURIER |
|---|---|---|---|
| *Charge only for a file that takes longer than 2 hours to prepare.* | *If the requested information can be printed or copied, fees are 25 cents per page.* | *Can charge $10 for every 15 minutes to process electronic data.* | *No fee if sending copies in regular mail.* |
| *$15 for each additional 30 minutes.* | *Or, charge actual cost of service.* | *Or actual cost incurred.* | *May charge actual cost of courier service.* |

Dentists may waive all or a portion of fees where imposing fees would cause financial hardship.

NOTE:

***USC&LS codes 93211 and 02911-02919 in the NBDS Fee Guide address the copying of records and the duplication of radiographs; (code 04912) for duplication of models. The NBDS does not endorse "administration fees" as the patient should not be required to incur costs over and above the direct costs associated with the copying, duplicating, and transfer of their Records.***

# APPENDIX A

For further information and inquiries, please contact either of the following:

**New Brunswick Dental Society**
520 King Street, HSBC Place #820
P.O. Box 488, Stn "A"
Fredericton, NB E3B 4Z9
Telephone: 506-452-8575
Fax: 506-452-1872
Email: nbds@nb.aibn.com
Website: www.nbdental.com

**Office of the Access to Information and Privacy Commissioner**
230-65 Regent Street
Fredericton, NB E3B 7H8
Telephone: 506-453-5965
Toll Free: 1-877-755-2811
Fax: 506-453-5963
Email: access.info.privacy@gnb.ca
Website: www.info-priv-nb.ca

**Personal Health Information, Privacy and Access Act for NB (PHIPAA)**
http://www.gnb.ca/0051/acts/legislation-e.asp

**Personal Information Protection and Electronic Documents Act (PIPEDA)**
http://www.priv.gc.ca/information/guide_e.asp

# APPENDIX B

## RULE 7

## DESIGNATED CUSTODIAN OF PATIENT DENTAL RECORDS

Any practicing dentist who no longer maintains a license for any reason, including leave of absence, changing jurisdiction, or retirement, is required to contact the NBDS and provide written confirmation as to who is the designated custodian of the patient dental records for the departing dentist.

Failure to designate a custodian for dental records as required in this Rule will be subject to a Complaint by the Registrar as an act of Professional Misconduct.

# APPENDIX C

## Privacy and Security Checklist

| A. CLINIC POLICIES AND PROCEDURES | YES | NO | Comments |
|---|---|---|---|
| Do you have an office privacy policy that deals with confidentiality of personal health information including printing, transfer, storage, and secure disposal of patient records? | | | |
| Are procedures in place for dealing with actual and suspected privacy and security incidents and breach investigations? | | | |
| Are processes in place to securely dispose of paper documents and old electronic devices (such as data storage, computers, etc.) that may contain confidential data? | | | |

| B. STAFF | YES | NO | Comments |
|---|---|---|---|
| Have you appointed an individual (and delegated) responsible for privacy and security? This person would be responsible for answering questions (e.g., from patients), but also responding to complaints, incidents, breaches, audits, and making sure that staff are trained and policies/procedures are up-to-date. | | | |
| Have staff members signed a confidentiality agreement? | | | |
| Have staff members been trained about how to maintain privacy and confidentially of personal health information? | | | |
| Do you have ongoing annual privacy and security awareness training that includes how users must safeguard their user IDs and passwords, keys, tokens, and other access credentials? | | | |

| C. PARTNERS | YES | NO | Comments |
|---|---|---|---|
| Do contracts with third parties (e.g., paper-shredding service) include privacy and confidentiality clauses? | | | |

| D. PATIENTS | YES | NO | Comments |
|---|---|---|---|
| Is a patient privacy notice or other communication materials that inform patient about privacy and information practices available? | | | |
| Are procedures available for dealing with patient requests for information, corrections, and complaints? | | | |

*Checklist used with permission of the BC Medical Association.*

## ADDITIONAL CONSIDERATIONS, IF USING COMPUTERS, FAXES, AND ELECTRONIC DEVICES

| E. ELECTRONIC RECORDS MANAGEMENT & BUSINESS CONTINUITY | YES | NO | Comments |
|---|---|---|---|
| Have you appointed an individual responsible for ongoing electronic records account management (new user set-up, changes to user privileges, deactivation of old user accounts)? | | | |
| Has a unique user ID and strong password been assigned to each individual user accessing the electronic records? | | | |
| Are appropriate access controls in place to ensure that only those authorized users within the dental practice have access to the patient health information necessary for them to execute their employment responsibilities and that such access is characterized as "read", "write" and/or "modify" as required for these responsibilities? | | | |
| Has the systems audit trail functionality been enabled? | | | |
| Do you have an audit schedule and procedures in place for a designated individual to routinely and periodically (i.e., spot-audits) monitor audit trails? | | | |
| Is there is a business continuity and disaster recovery plan in place in the event of catastrophic system failure due to environmental and/or other hazards? | | | |

| F. HARDWARE, SOFTWARE AND PERIPHERALS | YES | NO | Comments |
|---|---|---|---|
| Do your policies address fax and email use? | | | |
| Are peripheral devices (printers, fax machines) located in secure areas to prevent unauthorized access? | | | |
| Are computer monitors situated in a manner that prevents unauthorized viewing? | | | |
| Is any patient data stored on desktop computers, laptops, or mobile storage (e.g., memory keys) encrypted? | | | |
| Are procedures and technical controls (e.g., application time-out) in place to prevent screens from being viewed if the computer user leaves the computer? | | | |
| Has up-to-date antivirus protection been installed on all workstations and are anti-virus controls always on, enabled and updated in a timely manner? | | | |
| Are firewalls installed on computers with access to the Internet? | | | |
| Does your diagnostic software meet Health Canada Requirements in the rules under the Medical Devices Regulation? | | | |

| G. LOCAL AREA NETWORK (LAN) AND WIRELESS | YES | NO | Comments |
|---|---|---|---|
| Does your office employ a secure email service with strong encryption in order to meet your obligations to secure a patient's health information? | | | |
| Is information communicated to patients or colleagues through wireless devices, either email or text, strongly encrypted or de-identified? | | | |
| Have appropriate controls been set up to secure the Local Area Network (LAN), if you have one? | | | |
| Have wireless security settings been appropriately configured and enabled (e.g., restrict wireless transmission, firewalls, encryption is used, etc.), if they are in place? | | | |
| Have appropriate controls been set up to secure the Virtual Private Network (VPN), if you have one? | | | |

# Checklist for the Protection of Personal Health Information in New Brunswick

## For Use by Custodians in the Event of a Change in Professional Practice

On September 1st, 2010, the *Personal Health Information Privacy and Access Act* ("the *Act*") was proclaimed to provide access rights to one's personal health information, to provide rules on the use, collection and disclosure of such private information, and to protect the confidentiality of personal health information and the privacy of the individuals to whom it belongs. This new legislation also permits the Office of the Access to Information and Privacy Commissioner to play an oversight role to ensure compliance with the *Act* in all respects. In summary, the *Act* is reflective of the Province's new approach to providing overall a better public health care system and has resulted in changes for many health care professionals, i.e., custodians, in the way they protect personal health information.

To assist in the implementation of the new rules found in the *Act*, the Office of the Access to Information and Privacy Commissioner has devised useful **CHECKLISTS FOR CUSTODIANS**. These checklists guide custodians through easy steps which are designed to check that the health care records of patients or clients remain safe in all situations involving a change in their professional practice. Custodians need to be mindful that they continue to be responsible for the records of their patients/clients until those records are passed to another custodian, or until they are passed to another person who is legally authorized to hold them, or until they are destroyed in accordance with the rules found in the *Act*. Before going through the **CHECKLISTS FOR CUSTODIANS** below, all custodians must be reminded of an essential obligation of the *Act*: to establish a **WRITTEN POLICY** for the retention, secure storage, access, and secure destruction of health care records in their custody. This written policy will serve to protect the personal health information of your patients from being stolen, lost, inadvertently disposed, or disclosed to or accessed by unauthorized individuals.

The present **CHECKLISTS FOR CUSTODIANS** has been developed to be used whenever custodians contemplate a change in their professional practice involving:

A) the TEMPORARY closure of the office (ex. sabbatical leave, illness, etc.); or
B) the PERMANENT closure of the office or practice such as the sale of the practice, the transfer of the practice to another custodian, or when the custodian moves to another location in or outside New Brunswick.

Depending on the change of the professional practice, please refer to either CHECKLIST A for the TEMPORARY CLOSURE of the office or practice; Checklist B is for the PERMANENT CLOSURE of the office or practice.

## Checklist A: Temporary Closure of the office/practice

- ❑ STEP 1: Be aware of ALL records in your care and control (including all active and inactive files).

- ❑ STEP 2: Create a list of all records identified in Step 1.

- ❑ STEP 3: Identify the secure location where the records which must be retained will be stored. Remember that as a custodian, you remain responsible for the protection of your patients/client's files even while they are in storage. A secure location means one which has proper security safeguards.

- ❑ STEP 4: Notify all individuals whose records you hold (patients, clients) of the temporary closure of your office or practice, and of the anticipated period of time of the office closure.

  This will permit those who need a copy of their record to request a copy. Notification should include to whom the patient/client can make a written request to access his or her record, and that the record belonging to that individual will be retained until the re-opening of the office or until another notice from your office is issued.

- ❑ STEP 5: Identify which records need to be retained and which can be destroyed. Please verify with your professional Association for the suggested retention schedules (period of time to retain) for the records in your custody.

  *For example, College of Physicians and Surgeons Guidelines suggest the following retention schedule:*
  - *Files of patients: 10 years after last seen*
  - *Files of minors: 10 years after last seen or until the minor reaches the age of 21, whichever is longer*
  - *Files of deceased patients: 2 years after date of death*

- ❑ STEP 6: Destroy records that need no longer be retained and do so in a secure fashion (ex. secure shredding, disk wiping, etc.). When you proceed to the destruction of records, you must write down the following:

  a) Names of individuals whose records will be destroyed;
  b) Brief summary of the content of each record destroyed;
  c) Time period of each record destroyed;
  d) Method of destruction used (ex. secure shredding or incineration by company X); and
  e) Name of the person who supervised the destruction.

Please use the attached **Appendix – Sample Chart for Records Securely Destroyed** to assist you in keeping track of the information obtained in STEP 6.

## Checklist B: Permanent Closure of the office/practice

- ❑ STEP 1: Be aware of ALL records in your care and control (including all active and inactive files).

- ❑ STEP 2: Create a list of all records identified in Step 1.

- ❑ STEP 3: Identify which records need to be retained and which can be destroyed. Please verify with your professional Association for the suggested retention schedules (period of time to retain) for the records in your custody.

  *For example, College of Physicians and Surgeons Guidelines suggest the following retention schedule:*
  - *Files of patients: 10 years after last seen*
  - *Files of minors: 10 years after last seen or until the minor reaches the age of 21, whichever is longer*
  - *Files of deceased patients: 2 years after date of death*

- ❑ STEP 4: Destroy records that need no longer be retained and do so in a secure fashion (ex. secure shredding, disk wiping, etc.). When you proceed to the destruction of records, you must write down the following:

  a) Names of individuals whose records will be destroyed;
  b) Brief summary of the content of each record destroyed;
  c) Time period of each record destroyed;
  d) Method of destruction used (ex. secure shredding or incineration by company X); and
  e) Name of the person who supervised the destruction.

  Please use the attached **Appendix – Sample Chart for Records Securely Destroyed** to assist you in keeping track of the information obtained in STEP 4.

- ❑ STEP 5: Identify the secure location where the records which must be retained will be stored. Remember that as a custodian, you remain responsible for the protection of your patients/client's files even while they are in storage. A secure location means one which has proper security safeguards.

- ❑ STEP 6: Notify all individuals whose records you hold (patients, clients) of the closure of your office or practice.
  This will permit those who would like to receive a copy of their record to do so.
  Notification to patients/clients should include the name of a contact person, i.e., to whom a patient/client can make a written request to access his or her record. Notification should also indicate the length of time you will retain the file belonging to the individual before it is destroyed (in accordance with your retention schedules).

**Appendix – Sample Chart for Records Securely Destroyed**

| Name of individual (patient/client) | Summary of the content in each record | Time period of each record | Method of destruction | Person responsible for the destruction of files | Date of destruction |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# Guidelines for Custodians
## – to assess compliance with the *Personal Health Information Privacy and Access Act (PHIPAA)*

This document is designed to help custodians evaluate readiness for compliance with PHIPAA and to help identify where policies or practices may need to be developed and/or changed to ensure compliance. It is intended to complement the document entitled: *Preparing for the Personal Health Information Privacy and Access Act (PHIPAA): a checklist for custodians.*

*NOTE: This document is a guide only; it is not intended to provide a complete statement of your organization's legal obligations and as such it should not be construed as legal advice. Reference should always be made to the official text of PHIPAA and its regulations for a complete statement of the law and for further information about the points presented here. The relevant sections of the Act are referenced in parentheses throughout the document to assist you.*

## 1. Are you a "custodian" as defined by PHIPAA? *(Section 1)*

*PHIPAA applies to personal health information that is collected, used or disclosed by a custodian or that is in the custody or control of the custodian. "Custodian" means an individual or organization that collects, maintains or uses personal health information for the purpose of providing or assisting in the provision of health care or treatment or the planning and management of the health-care system or delivering a government program or service and includes:*

(a) public bodies,
(b) health-care providers,
(c) the Minister,
(d) the following organizations or agencies:
- *(i) Ambulance New Brunswick Inc.,*
- *(ii) the New Brunswick Health Council,*
- *(iii) FacilicorpNB Ltd.,*
- *(iv) regional health authorities,*
- *(v) WorkSafeNB*
- *(vi) Canadian Blood Services,*

(e) information managers,
(f) researchers conducting a research project approved in accordance with this Act,
(g) health-care facilities,
(h) a laboratory or a specimen collection centre,
(i) nursing homes and operators as those terms are defined in the Nursing Homes Act, and
(j) a person designated in the regulations as a custodian.

| **Yes** | **No** | |
|---|---|---|
| ☐ | ☐ | Are you (or is your organization) a custodian as defined above? |

## 2. Do you collect, use, disclose or maintain personal health information that may be subject to PHIPAA? *(Sections 1 and 3)*

*PHIPAA applies to personal health information that is collected, used, maintained or disclosed by a custodian or that is in the custody or control of the custodian. Personal health information is defined in part as identifying information about an individual pertaining to that person's mental or physical health, family history or health care history. This includes:*

- genetic information;
- registration information, including the Medicare number of the individual;
- information about payments or eligibility for health care or health-care coverage;
- information pertaining to a donation by the individual of any body part or bodily substance;
- information derived from the testing of a body part or bodily substance of the individual; and
- information that identifies the individual's health-care provider or substitute decision maker.

*Certain records and information containing personal health information may not be subject to PHIPAA. Please refer to Question 3 and also consult the Act for more information.*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Do you have records containing personal health information? |

## 3. Do the exceptions defined in PHIPAA, which exclude personal health information from the application of PHIPAA, apply to the personal health information in your custody or control? *(Sections 3 and 4)*

*The Act provides for certain instances whereby personal health information will be excluded from the application of PHIPAA and the Act will not apply. For example, the Act does not apply to:*

- an individual or organization that collects, maintains or uses personal health information for purposes other than health care or treatment and the planning and management of the health-care system, or for delivering a government program and service including: employers (public and private), insurance companies, regulatory bodies of health-care providers, licensed or registered health-care providers who do not provide health care, and certain other individuals or organizations prescribed by regulation;
- personal health information in a record created 100 or more years ago or where 50 or more years have passed since the death of the individual;
- information in a court record, such as a record of support services provided to a judge or court official;
- a record created or information held by a person under the provisions of certain other Acts of the Legislative Assembly, including the *Family Services Act,* the *Mental Health Act,* and any other Act of the Legislative Assembly prescribed by regulation.

*Consult the Act and regulations for more information on instances where PHIPAA may not apply.*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Check "yes" if there are exceptions that may exclude the personal health information in your custody or control from the application of PHIPPA. |

*Your answers to Questions 1, 2, and 3 may be used to assess whether PHIPAA will apply to all or some of the personal health information in your custody or control. For a more comprehensive assessment of the application of PHIPAA in your specific circumstances, consult the Act and regulations.*

# 4. Rights of the individual

## *4.1. Obtaining consent* *(Sections 17, 18, 19)*

### *4.1.1 General considerations regarding consent*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Have you obtained consent from the individual for the collection, use or disclosure of personal information unless otherwise required or permitted by the Act or by law? |
| ☐ | ☐ | Is consent knowledgeable? *(for consent to be knowledgeable, individuals must be informed (by way of a readily available notice or similar means) in laymen's terms about the purpose of the collection, use or disclosure of their information both within and outside of the circle of care and informed of their right to withhold or withdraw their consent)* |
| ☐ | ☐ | Is consent specifically related to the personal health information collected and the purpose(s) for which it will be used? |
| ☐ | ☐ | Is consent voluntary *(consent may not be coerced)*? |

### *4.1.2 Express consent*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Where applicable, have you obtained express consent for the collection, use or disclosure of personal health information? *(Where consent is required by the Act, it must be express unless the Act specifically permits an implied consent – see 4.1.3 below).* |

Express consent will generally be required when information is being disclosed to any of the following (unless otherwise provided in the Act):

√ the media;

√ a person for the purpose of fund-raising;

√ a visitor to a health-care facility;

√ a person for a non-health care related purpose (for example, information disclosed to an insurance company);

√ a person outside of New Brunswick (some exceptions apply – refer to Section 47); and

√ a person for the purpose of research (some exceptions apply – refer to Section 43).

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Will you ensure the express consent is obtained in writing from the individual or his or her substitute decision-maker? |
| ☐ | ☐ | Have the general considerations for consent outlined in 4.1.1 been met? |

### 4.1.3 Implied consent

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Is there implied knowledgeable consent of the individual to share his/her personal health information within the circle of care for providing health care to that individual? *(For implied knowledgeable consent to exist, it must be reasonable to assume that the individual understands the purpose for the collection, use or disclosure of his or her personal health information within the circle of care and the implications of providing or withdrawing consent).* |
| ☐ | ☐ | Have the general considerations for consent outlined in 4.1.1 been met? |

### 4.1.4 Consent not required

| Yes | No | |
|---|---|---|
| ☐ | ☐ | If you will collect, use or disclose personal health information without consent, has the authority under the Act to do so been documented and confirmed? |
| ☐ | ☐ | Do you have a process in place to ensure there is a record of all personal health information disclosed without consent under the Act as required by Section 46? |

### 4.2. Consent Directives *(Section 22)*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Where consent has been obtained, are there procedures in place to address an individual's request to withdraw consent to the collection, use or disclosure of his or her personal health information? |
| ☐ | ☐ | Are procedures in place to control and monitor situations where a custodian may be required to override an individual's consent directive in accordance with the Act (for example, for health and safety reasons)? *(procedures should include, but not be limited to: logging, monitoring and auditing consent directive overrides to ensure that they are documented and authorized by the Act).* |
| ☐ | ☐ | If information networks are used, is a process in place to inform individuals about how they can exercise their right to prevent access to or disclosure of their personal health information contained in an information network? *(note, however, that an individual may not withhold his or her consent for the collection of personal health information by a custodian for creating and maintaining an information network).* |

### 4.3 Right to be informed *(Section 31)*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Have you taken reasonable steps to directly inform individuals whose personal health information is being collected directly of the purpose (including anticipated uses and disclosures) for which the information is being collected before or as soon as practical after it is collected? *("Reasonable steps" may include, for example, creating a poster or a privacy notice and making it available on the custodian's website or as a handout; notifying individuals either verbally or in writing about how they may obtain a copy of the organization's privacy notice; and describing the purpose of collection on forms used to collect personal health information.).* |

## 4.4. Collecting the Medicare number *(Section 48)*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Are individuals only required to produce their Medicare number for reasons connected to health services? |
| ☐ | ☐ | If you require the Medicare number for non-health purposes, is the collection authorized by an Act or regulation? *(If not, collection can be voluntary, but cannot be made as a condition of receiving a service. Individuals must have the option of using other identification).* |

## 4.5. Individual's right to complain to the Access to Information and Privacy Commissioner regarding an action/decision of a custodian *(Part 6)*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Are individuals informed of their right to contact the Access to Information and Privacy Commissioner to request a review of an action taken or a decision made in the event that you cannot resolve a concern regarding their personal health information? |

## 4.6. Individual's ability to designate a substitute decision-maker *(Sections 25,26)*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Do you have procedures to process an individual's written request to designate another individual to act on his or her behalf regarding his or her rights pertaining to his or her personal health information? |
| ☐ | ☐ | If an individual is not able to act on his or her behalf; do you ensure that the designated person meets one of the circumstances identified in Section 25 of the Act? |

## 4.7. Requests for access to personal health information *(Part 2, Division A)*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Have you established procedures to receive requests for, and provide access to records containing personal health information? |
| ☐ | ☐ | Will you charge a fee for providing access? If so, is it consistent with the regulations under PHIPAA? |
| ☐ | ☐ | When responding to requests for disclosure of personal health information do you have procedures in place to uniquely identify the individual to whom the information relates before granting access to the information? |

## 4.8. Requests to correct personal health information

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Have you established procedures to correct records of personal health information when required by the individual about whom the information pertains; or to place a statement of disagreement on the records of the individual's personal health information? |

## 5. Protection of personal health information

### *5.1. Duty to protect* (Section 50)

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Have you developed a security policy and supporting procedures that outline how your organization will ensure that reasonable safeguards are in place to protect the *confidentiality, security, accuracy and integrity* of the personal health information in your custody or control? |
| ☐ | ☐ | Has a review been conducted to ensure that information practices and policies conform with industry standard (national or jurisdictional) information technology security standards and processes appropriate for the level of sensitivity of the personal health information to be protected? |
| ☐ | ☐ | Have you implemented reasonable physical safeguards such as locked cabinets and use of access cards to control entry to storage areas that contain personal health information? |
| ☐ | ☐ | Have you implemented reasonable administrative safeguards such as background checks, mandatory employee training and appropriate privacy and security policies to protect personal health information against risks such as unauthorized access, use, disclosure or modification? |
| ☐ | ☐ | Have you implemented reasonable technical safeguards such as appropriate encryption of personal health information, strong passwords, anti-virus protection and firewalls to protect personal health information against unauthorized access, use, disclosure or modification? |
| ☐ | ☐ | Are the policies and procedures described above designed to protect information in all forms including, but not limited to paper records; computer records including databases, e-mail, electronic forms; and microfilm/fiche? |

### *5.2. Retention, storage and secure destruction* (Section 55)

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Do you have written policies for the retention, archival storage, access and secure destruction of personal health information in your custody and/or control? |
| ☐ | ☐ | Do your existing procedures enable compliance with such policies? |
| ☐ | ☐ | Do retention policies comply with any applicable legislative requirements? |
| ☐ | ☐ | Do the above policies apply to records in all formats (for example,. paper, electronic databases, e-mail, microfilm/fiche) regardless of media? |
| ☐ | ☐ | Are there policies or procedures that ensure personal health information is securely destroyed when no longer required? *(Policies should mitigate risks such as records containing personal health information thrown in a garbage can or electronic records not completely removed from a hard drive sold for salvage).* |
| ☐ | ☐ | Do you have a formal /secure system and process to backup electronic data contained on all computer systems that store personal health information? |
| ☐ | ☐ | Are backup tapes securely stored and appropriately destroyed once they have reached the end of their useful life? |

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Do you ensure paper records are safely stored where they will not suffer damage from risks such as flooding/water damage? |
| ☐ | ☐ | Do you keep a formal record of the contents of all records containing individuals' personal health information destroyed in accordance with the retention and/or destruction policy? |
| ☐ | ☐ | Is personal health information in the organization's custody or control stored outside Canada only for authorized purposes *(storage outside of Canada is not permitted unless the individual has consented or unless such storage is specifically authorized under the Act)?* |

### *5.3. Information Management Service Provider agreements* (Section 52)

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Have you identified all "information managers" (for example, paper shredding services, IT service providers) engaged by your organization in delivering programs and services? |
| ☐ | ☐ | Do you have written agreements with all information managers that contain appropriate privacy and security clauses including:<br>• a description of how the personal health information will be protected against risks such as unauthorized access to or use or disclosure of the information, unsecure destruction or alteration;<br>• the requirement for the information manager to comply with the PHIPAA and regulations;<br>• the requirement that information managers do not store personal health information outside of Canada except in the case of maintenance and technical support provided for personal health information systems or unless otherwise provided for in the Act. |

### *5.4. Duty to collect accurate information* (Section 53)

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Do you take reasonable steps to ensure that the personal health information you collect is accurate and complete? |

## 6. Collection, use and disclosure

### *6.1. Limitations on collection* (Section 29)

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Do you take steps to limit the personal health information that is collected, used or disclosed to only what is necessary to satisfy the purpose of the collection, use or disclosure? |
| ☐ | ☐ | Do you use or disclose de-identified personal health information if it will serve the purpose as identifiable information? |

## 6.2. Manner of collection *(Section 28)*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Do you only collect personal health information directly from the individual about whom that information pertains? |
| ☐ | ☐ | If personal health information is collected indirectly from other sources, has the individual consented to collection by the other means or does the collection fall under one of the exceptions specified in Section 28 of the Act? |
| ☐ | ☐ | When collecting personal health information from other sources, do you take reasonable steps to verify the accuracy of the information? |

## 6.3. Restrictions on use and disclosure *(Sections 32-45)*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Do you have policy or procedures to limit the use and disclosure of personal health information to the minimum amount of information necessary to accomplish the purpose for which it is to be used or disclosed? |
| ☐ | ☐ | Do you have policy or procedures to restrict access to or disclosure of an individual's personal health information by persons such as employees, volunteers and others who do not need to know the information to perform their jobs? |
| ☐ | ☐ | Do you have consent from individuals for every use of their personal health information? |
| ☐ | ☐ | If you do not always have consent to use an individual's personal health information, does the use meet one of the criteria outlined in Section 34 of the Act ? |
| ☐ | ☐ | Do you take steps to ensure that consent is obtained prior to disclosing personal health information unless the disclosure is specifically authorized by the Act? |
| ☐ | ☐ | If you do not have consent to disclose an individual's personal health information, is the reason for disclosure one of the circumstances identified in Section 37(6) and Sections 38-45 of the Act? (*These sections allow limited disclosure without consent.)* |
| ☐ | ☐ | Do you inform non-custodians that they can only use personal health information for the purpose(s) for which you are disclosing it to them and for no other reason, except where permitted by the Act? |
| ☐ | ☐ | Do you have a policy requiring that personal health information be de-identified in circumstances where consent for use or disclosure has not been obtained and where the use or disclosure of personal health information is not authorized by the Act? |
| ☐ | ☐ | In the case where de-identified information will be used or disclosed, do you have procedures in place to provide reasonable assurance that the information cannot be used either alone or in combination with other information to re-identify an individual or individuals whose personal health information is contained in the data set? |

### *6.4. Use or disclosure for research* (Section 43)

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Will personal health information be used or disclosed for research? |
| ☐ | ☐ | If personal health information is to be used or disclosed for research, has the project been approved by an authorized research review body having met all of the requirements of the Act? |

## 7. Other things to consider – general privacy practices

### *7.1. Responsibility for privacy*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Have you designated one or more individuals who will be responsible for implementing and overseeing compliance with PHIPAA? *(individual(s) should be appropriately trained and be provided with adequate resources to do the job)* |

### *7.2. Privacy policy – development and compliance*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Do you have a written privacy policy intended to ensure compliance with the Act within your organization? |
| ☐ | ☐ | Are staff and contractors familiar with the privacy policy, and are they periodically reminded of their responsibilities for compliance with the policy? |
| ☐ | ☐ | Are staff and contractors required to sign confidentiality agreements that contain a written requirement for them to comply with PHIPAA and the organization's privacy policies? |
| ☐ | ☐ | Are procedures in place to monitor and ensure agents' (for example, employees', contractors', volunteers') compliance with the organization's privacy and security policies? |

### *7.3 Privacy Notice*

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Have you developed a publicly displayed privacy notice for your organization that will provide individuals with reasonable notice of your organization's privacy practices? |

*(A privacy notice may be made available, for example, on the organization's website, incorporated within posters and brochures, or by way of voice recording). A privacy notice is a communication tool that is different than (but must be consistent with) the organization's privacy policy. The privacy policy is an internal document that outlines employees' and agents' responsibilities for privacy under the legislation.*

| | | |
|---|---|---|
| ☐ | ☐ | Have you reviewed the organization's forms, applications, etc., that are used to collect personal health information to ensure that individuals are appropriately informed about the purposes for the collection of the information at the time it is provided? This may be done either by incorporating an explanation of the purpose directly within the forms or by a short statement explaining how the individual may obtain a copy of the privacy notice or obtain more information about the purpose of the collection. |

## 7.4. Privacy training and awareness

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Do you have a plan in place to regularly deliver mandatory privacy training to all employees and contractors to reinforce their obligations under PHIPAA and the organization's privacy policies? |
| ☐ | ☐ | Do you have a plan in place to communicate the organization's privacy policies to employees and to assist employees/managers develop procedures that support alignment with the policies? |

## 7.5. Privacy inventory and gap analysis

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Have you completed an inventory of your organization's information holdings and identified the various purposes for which you collect, use and disclose personal health information? |
| ☐ | ☐ | Have you conducted a gap analysis based on the inventory to determine areas of risk and non-compliance? |

## 7.6. Investigation of privacy incidents and breaches

| Yes | No | |
|---|---|---|
| ☐ | ☐ | Do you have a process for receiving and investigating privacy complaints in a timely manner? |
| ☐ | ☐ | Have you developed a privacy incident response policy and procedures to manage and contain a privacy breach should it occur? |
| ☐ | ☐ | Have you developed a process for reporting a privacy breach to the Access to Information and Privacy Commissioner and for notifying the affected individual(s)? |