STANDARDS OF PRACTICE

SECURITY, CUSTODY & RETENTION OF PATIENT HEALTH RECORDS

Name: Security, Custody & Retention of Patient Health Records
Date Approved: 09/30/2016
Date Updated: 09/30/2016, 03/15/2019, 03/08/2024
Date Effective: 10/15/2024
Number: SP-PM-7
Type: Practice Management Standards (PM)
Reference:

Professional Bylaws
(6.4) A member shall keep patient records in a systematic manner and shall retain each record for a period of at least six years after the date of the last clinical entry in a record. All records of pediatric patients shall be retained for two years past the age of majority or six years after the date they were last examined whichever may be the later date.

HIPA
16 Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
(a) protect the integrity, accuracy and confidentiality of the information:
(b) protect against any reasonably anticipated:
(i) threat or hazard to the security or integrity of the information;
(ii) loss of the information; or
(iii) unauthorized access to or use, disclosure or modification of the information; and
(c) otherwise ensure compliance with this Act by its employees.
Guide to HIPA website: https://oipc.sk.ca/assets/ipc-guide-to-hipa.pdf

03.08.2024 MOTION "To amend SP-PM-7 Security, Custody & Retention of Patient Health Records requirements as presented." CARRIED

Security of Patient Records

For all types of records, staff working in optometric offices where patient records are kept should:

- Shut and lock doors and cabinets as required
- Control access to fax machines and not leave records unattended there
- Query the status of strangers
- Know whom to tell if anything suspicious or worrying is noted
- Not tell unauthorized personnel how security systems operate
- Not breach security themselves - wear building passes/ID if issued
- Sign confidentiality agreements that outline penalties for inappropriately collecting, using, or disclosing personal information

- Keep health records on-site wherever possible. When records must be taken off-site, they should be kept secure at all times. Laptops and handheld computers should be password protected and the data should be encrypted whenever possible.

Paper records should be:

- Kept separate from general office document filing systems, i.e. generic intake forms, end-of-day balance sheets, company invoices, etc.
- Tracked if transferred; if a file is transferred to another entity, a note should be made of the date of transfer and location to which it was transferred
- Returned to the filing location as soon as possible after completion of treatment
- Stored securely within the office, arranged so that the record can be found easily if needed urgently
- Stored closed when not in use so that contents are not seen accidentally
- Inaccessible to members of the public and not left—even for short periods—where they might be looked at by unauthorized persons
- Held in secure storage with clear labeling

With electronic records, members and staff should:

- Be in compliance with all aspects of the Health Information Protection Act (HIPA)
- Log-out of computer systems or applications when not in use (whether leaving for the day or a few minutes)
- Protect the safety of the hardware from lightning strikes, power outages, water damage and theft
- Be diligent in maintaining current technology to protect the security of electronic patient data
- Ensure their electronic records are protected with a reliable backup system
- Not leave a terminal unattended and logged-in
- Keep computers away from public view and access
- Not share user IDs or passwords with other people. If other staff members have a need to access records, appropriate access should be organized for them—this must not be by using other users' IDs or passwords.
- Change passwords at regular intervals to prevent anyone else using them
- Ensure staff access to patient and government records are monitored and periodic and unscheduled compliance checks are conducted
- Not use short passwords or use names or words that are known to be associated with them (e.g. children's or pet names, birthdays). Passwords should never be written down.
- Revoke user IDs and passwords as soon as authorized users resign or are dismissed
- Always clear the screen of a previous patient's information before seeing another
- Use a password-protected log-out to prevent casual viewing of patient information by others
- Install firewall software where Internet access to computer systems exists
- Use audit trails to track when a record is accessed, by whom, and whether the accessing individual has the necessary authorization

- Ensure data backup intervals and methods, and disaster recovery plans, are in place and periodically reviewed
- For large computer systems, develop and implement rules on access levels for different users for different purposes

Storage

Ensure all records are secure and stored safely from environmental factors. When possible, files should be encrypted; however, they must be in a format that can be accessed.

Backups Including Storage

There are many advantages of electronic medical record over paper records; however, members must ensure they have backup protocols in place for secure storage and retrieval of records. Regardless of the backup provision, i.e. a third-party provider or a designated server, the member is responsible for confirming the backups are done successfully. Backups should be scheduled at regular intervals (minimum daily) and should be encrypted. Periodic testing of the backups should be done.

Agreement with information management service provider

For the purposes of subsection 18(2) of HIPA, before providing personal health information to an information management service provider, a trustee must enter into a written agreement with the information management service provider that includes:

(a) a description of the specific service the information management service provider will deliver;

(b) provisions setting out the obligations of the information management service provider respecting the security and safeguarding of the personal health information;

(c) provisions for the destruction of the personal health information, if applicable;

(d) a requirement that the information management service provider not use, disclose, obtain access to, process, store, archive, modify or destroy personal health information received from a trustee except for the purposes set out in subsection 18(1) of the Act;

(e) a requirement that the information management service provider comply with the terms of the agreement entered into with the trustee; and

(f) a requirement that the information management service provider notify the trustee at the first reasonable opportunity of any breach of the agreement.

Destruction of Patient Files

Records should be stored securely in a retrievable, readable format, and useable for the purpose for which it was collected for the minimum time period according to professional bylaws, HIPA and CRA guidelines.

Per HIPA 17(1)(a), a written policy concerning the retention and destruction of personal health information must include:

(a) either:

(i) a requirement that personal health information be retained by a trustee for at least 10 years after the date of the last episode of care or until age 20 if the subject individual is a minor, whichever period is longer; or

(ii) a retention schedule that sets out:

(A) all legitimate purposes for retaining the information; and

(B) the retention period and destruction schedule associated with each purpose set out pursuant to HIPA

(b) measures to provide for the secure retention and destruction of records to minimize the risk of any unauthorized use or disclosure of, or unauthorized access to, personal health information; or

(c) a process to keep a record of:

(i) the name of each individual whose personal health information is destroyed;

(ii) a summary of what personal health information was destroyed;

(iii) the time period of the personal health information;

(iv) the method of destruction of the personal health information; and

(v) the name and job title of the individual responsible for supervising the destruction of the personal health information.

Using a Private Company for Destruction of Records

If hiring an outside agency to securely destroy (i.e. shred, burn, pulp, chemical destruction), the trustee needs to include confidentiality provisions into any contract and/or agreement with the contracted agency.

Refer to a sample agreement attached at the end of this policy.

Destruction of Devices Storing Patient Records

Devices such as servers, computers, laptops, fax machines and photocopies retain personal health information on their hard drives even after the user has deleted the information using the devices delete feature. To securely and permanently delete this information, the hard drive should be destroyed. It is recommended all members maintain an up-to-date list of all office and medical equipment that retains personal health information.

CONFIDENTIALITY AGREEMENT "SAMPLE"
BETWEEN OPTOMETRIC PRACTICE & A SERVICE PROVIDER

The service provider named below hereby agrees that it will not use or disclosure any identifiable patient information (whether received or created before or after the date of this agreement) except for the purposes necessary to perform services for the medical practice named below, as set out in the service contract entered into between the service provider and the medical practice before this date ("service agreement") or with the prior written consent of the medical practice in its sole discretion or as compelled by law.

The service provider represents that it has safeguards in place, equal or superior to the medical practice named below, to protect the security of patient information. The service provider agrees to securely dispose of identifiable patient information once it is no longer required for the purposes specified in the service contract and to notify the medical practice within a reasonable time thereafter that this has been done and how it has been done.

The service provider represents that it is aware of and fully compliant with Saskatchewan's Health Information Protection Act.

The service provider acknowledges and agrees that any breach of this agreement may result in termination of the service agreement and may be grounds for legal action by the optometric practice against the service provider.

Service Provider (please print): _____

Address: _____

_____

Authorized Signatory (please print): _____

X_____ _____
Authorized Signature Date (mm/dd/yyyy)

Optometric Office: _____

Witness _____

X_____ _____
Witness Signature Date (mm/dd/yyyy)

CONFIDENTIALITY AGREEMENT "SAMPLE"
BETWEEN OPTOMETRIC PRACTICE & A FILE DESTRUCTION FACILITY

The Contractor named below hereby agrees that it will destroy patient files and other confidential information provided by the optometric practice described below.

The Agreement

The Contractor agrees that it will, with respect to all documents provided by the optometric practice to it for destruction:

a) Shred all documents within 10 days of taking possession of those documents;
b) Not permit any agent or employee of the Contractor, or any other person, to read or copy any document;
c) Maintain all documents in a secure location until they are shredded;
d) Shred the documents in such a manner that they cannot be reconstructed;
e) Comply with all the requirements of The Health Information Protection Act and the regulations under The Health Information Protection Act respecting personal health information.

The Contractor acknowledges and agrees that any breach of this agreement may result in termination of the agreement for destruction of documents.

Contractor (please print): _____

Address: _____

_____

Authorized Signatory (please print): _____

X_____ _____
Authorized Signature Date (mm/dd/yyyy)

Optometric practice: _____

Witness

_____

X_____ _____
Witness Signature Date (mm/dd/yyyy)

CONFIDENTIALITY AGREEMENT FOR EMPLOYEES "SAMPLE"

I am aware that the optometric practice named below has policies and procedures regarding the privacy, confidentiality, and security of personal patient information and that it must comply with Saskatchewan's Health Information Protection Act. I understand that it is my responsibility to be familiar with the requirements outlined in these policies and procedures and I have read the current version of these policies and procedures.

As an employee of the optometric practice named below, I agree to observe and comply with all policies and procedures of the optometric practice with respect to privacy, confidentiality, and security of patient information. Except when I am legally authorized or compelled to do so, I will not use or disclose personal patient information that comes to my knowledge or possession by reason of my employment with this medical practice.

I understand that any breach of the policies and procedures, including misuse or inappropriate disclosure of patient information, may be just cause for the termination of my employment.

Employee name (please print): _____

X_____ _____

Employee Signature Date (mm/dd/yyyy)

Optometric practice: _____

Witness

_____

X_____ _____

Witness Signature Date (mm/dd/yyyy)

CONFIDENTIALITY AGREEMENT "SAMPLE"
BETWEEN OPTOMETRIC PRACTICE & FILE STORAGE FACILITY

The file storage facility named below hereby agrees that it accepts for storage patient files provided by the optometric practice described below.

The file storage facility agrees that it will not allow its representatives, agents or employees to read, use or disclose any patient information contained within the files provided to it.

The file storage facility agrees that it will maintain complete confidentiality with respect to all patient information (whether received or created before or after the date of this agreement).

The file storage facility agrees that, upon receiving a request from the optometric practice, it will deliver the requested files to the optometric practice on a timely basis.

The file storage facility represents that it has safeguards in place, to protect the security of patient information.

The file storage facility represents that it is aware of and fully compliant with Saskatchewan's Health Information Protection Act

The file storage facility acknowledges and agrees that any breach of this agreement may result in termination of the service agreement and may be grounds for legal action by the medical practice against the service provider.

File Storage Facility (please print): _____

Address: _____

_____

Authorized Signatory (please print): _____

X _____ _____
Authorized Signature Date (mm/dd/yyyy)

Optometric practice: _____

Witness _____

X _____ _____
Witness Signature Date (mm/dd/yyyy)

REQUEST FOR ACCESS TO PERSONAL INFORMATION

The information on this form will be used to respond to your request for your personal information or the personal information of someone whom you are legally entitled to represent.
Whose information do you want access to?

- My own personal information.
- Another person's personal information.

Please complete the "Patient Information" and "Authorized Representative's Contact Information" sections below, and attach proof that you can legally act on behalf of that individual.

Patient information:

Mr / Mrs / Ms (please circle) Last Name: _____

First Name: _____

Street address: _____

City /town: _____ Prov._____ Postal Code: _____

Health Card number: _____ Tel (home): _____

Daytime Tel: _____

Fax: _____

Date of birth (mm/dd/yyyy): _____ Email address: _____

Please describe, in as much detail as possible, the information you want access to. Indicate if you also want access to records about the disclosure of your information, or information of the person you are representing. Be sure to give previous names, if any.

_____
_____
_____

Please indicate if you wish to:

- Receive a photocopy of the record.
- Have the material *faxed/or mailed* (circle appropriately) or I will collect it from the office.
- Please note that a base fee of $_____ per page applies for each page copied. For convenience, you may enclose this fee with your request. A deposit of the fee(s) may be required. You will be provided with an estimate of any additional costs.
- View the original record, without receiving a copy.
- Please ask for an estimate of the fee you will be charged for:
- Review of the original by the optometrist and/or
- Supervision by optometrist or designated staff person for your review

X_____ _____

Patient Signature Date (mm/dd/yyyy)

REQUEST TO AMEND PERSONAL INFORMATION "SAMPLE"

The information gathered on this form will be used to respond to your request to amend your personal information or the personal information of someone you are legally entitled to represent.

Whose information do you want to amend?

- My own personal information.
- Another person's personal information.

Please complete the "Patient Information" and "Amendments by Authorized Representative" sections below, and attach proof that you can legally act on behalf of that individual.

Patient information

Mr / Mrs / Ms (please circle) Last name: _____

First name: _____

Street address: _____

City/town: _____ Prov._____ Postal Code: _____

Health card number: _____ Tel (home): _____

Daytime Tel: _____

Fax: _____

Date of birth (mm/dd/yyyy): _____ Email address: _____

Please describe, in as much detail as you can, the information you want amended. Be sure to give the complete patient name that is in the records if it is different from the name given above. If you need more space, please attach a separate sheet of paper.

_____
_____
_____
_____

What amendment do you want to make and why? Please attach any documents that support your request.

_____
_____
_____
_____

X_____ _____

Patient Signature Date (mm/dd/yyyy)