2. Checklist for Compliance with HIPAA

Chiropractors should consider the following checklist to evaluate their compliance with privacy legislation:

1. Patients should know what information is being collected, used and/or disclosed about them and for what reason.
   - A poster, sign or brochure should be freely available in the clinic that states:
     - how and why the patient health information may be collected, used and disclosed;
     - patients’ right to request access to the information in their records;
     - patients’ right to request amendments to their records.
   - Information collected, used or disclosed should be limited to that which is necessary for the care of the patient and for registration and billing purposes.

2. There should be a process for appropriate patient consent to collection, use and disclosure of information.
   - Consent must be informed and voluntary.
   - Implied consent or deemed consent is generally sufficient for the ongoing care of the patient after the original presentation, including referrals to other caregivers. Release of information within the care team should be on a need-to-know basis.
     - Implied consent generally means the patient understands how their information may be collected, used or disclosed, but has not signed a consent form and has the option to opt out of the consent.
     - Deemed consent means the patient has not given consent, or doesn’t know their personal health information is being shared such as in the case of an unconscious patient undergoing care in the Emergency Department. Deemed consent should never be invoked casually or as a default approach to dealing with patients and their wishes.
   - Express (usually written) consent should be obtained for the collection, use and disclosure of information for any purpose other than the original purpose for its collection.
   - Patients have the right to limit consent. Patients can withdraw consent at any time. The consequences of withdrawal of consent should be discussed explicitly with the person and documented.
• All verbal consent should be documented.

3. The office must have a process to permit patient access to personal health information.
   • Patients must be permitted to see information in their records and to have copies of the records upon request. The chiropractor should retain original documents.
   • There are limited circumstances in which patients may be refused access to all or part of their record. Generally this is limited to circumstances in which disclosure:
     o is likely to endanger the mental or physical health or safety of the patient or another person,
     o would disclose confidential information about someone other than the patient, or
     o would identify a third party who provided information to the chiropractor in confidence.
   • Chiropractors have a duty to assist patients in accessing information in their records, upon receipt of a written request for access. Chiropractors must respond to such a request within 30 days.
   • Prudent chiropractors will ensure that patient access to records is supervised and that they are available to answer any questions the patient may have about the information in their record.
   • Chiropractors may charge a reasonable fee for providing access and/or copies of the patient file.
   • Patients who feel the fee is excessive can appeal to the Office of the Information and Privacy Commissioner of Saskatchewan (OIPC).

4. There should be a mechanism to update and correct information in personal health records.
   • Registration and billing data must be updated as required.
   • Clinical records should be complete and accurate. Amendments to the clinical record should not erase any previous entries to the chart, should be dated and should indicate clearly that an addition or amendment is being made. The source of the amendment should also be documented.
• Corrections can be made to inaccurate or incomplete factual information. A chiropractor is not required to make an amendment to a patient record merely because a patient disagrees with the chiropractor’s diagnosis or opinion.

• Chiropractors who use electronic medical records should ensure that their medical record software tracks additions and amendments.

5. All personal health information (registration data, billing data, health records, and staff/employee record, etc) should be kept appropriately secure.

• Consider locks, alarms, and other physical security devices.

• Electronic records should be password protected, and electronic systems should have appropriate firewalls, encryptions and other electronic security mechanisms. Consider handcuffing (limiting access to portions of the electronic record to defined users).

• Office policies and procedures should ensure that records are kept secure, that written information cannot be seen by unauthorized persons, that conversations cannot be overheard, and that all physicians and employees understand the importance of complete confidentiality.

• Restrict access to areas where personal health information is kept.

• If an information manager (computer support person, offsite storage company, etc), has access to patient information, a written agreement should be in place whereby the information manager agrees to ensure confidentiality and limit access to the records.

• All documents must be stored securely until they are cross-shredded by a file destruction company. Signed agreements must be in place as to the security and confidentiality of the files.

• Information must be retrievable for the duration of the retention period.

• When files are transferred to a file destruction facility, a written agreement should be in place whereby the file destruction facility agrees to ensure the security and confidentiality of the records until they are destroyed.

6. The office must designate an individual (ideally a chiropractor) to act as the Privacy Officer to oversee management of personal information.
• The Privacy Officer should be familiar with the obligations under HIPA.
• The Privacy Officer should monitor the tools and recommendations of the OIPC.
• This individual should develop and implement the privacy policies for the clinic and provide clinic staff with advice regarding HIPA compliance.
• All employees should know who the Privacy Officer is. The name and contact information of the Privacy Officer should be posted in the clinic for the public to see.

7. All staff should understand what types of information may be disclosed, to whom, and under what conditions.
• Disclosure among health care professionals in the course of providing patient care does not generally require express consent.
• HIPA allows disclosure without consent in a limited number of other situations (e.g., to a proxy for the patient in the case of advanced care directives, to a quality of care committee, for professional review/audit, to minimize danger to the health and safety of an individual). Disclosures of this type should be well documented and overseen by the clinic’s Privacy Officer.
• The office should have explicit policies that define whether staff may respond to requests for information about patients.
• Where information is shared among trustees, consideration should be given to formal data sharing agreements signed by both parties. Data sharing agreements may be particularly important when data are shared electronically. Such agreements should bind both parties to comply with privacy requirements.
• The default position should always be to require express consent from the patients prior to any disclosure.
• When in doubt, staff should forward requests for information to the Privacy Officer in the clinic.

8. Clinics should have a specific written office policy for information management. This should be readily accessible to staff. All staff members should receive training about the policy and sign confidentiality agreements.
• Staff policies and procedures should contain an explicit privacy policy. Non-compliance with the privacy policy should be grounds for disciplinary action.
• Staff should receive regular in-service training on issues related to information handling. This training should cover the following:
  o The privacy legislation under which your practice operates.
  o Key highlights of your practice’s privacy and security policies.
  o Privacy and security procedures, such as when to get explicit patient consent and managing patient complaints, privacy breaches and consent directives.
  o Staff responsibilities for protecting patient information.
  o Privacy and security best practices, such as not sharing user account information and how to create a secure, complex password.
  o Consequences for breaching privacy.

• Staff should be required to sign a confidentiality agreement at the time of hiring. Consider annual renewals of the agreement. The Agreement should state that:
  o The employee is familiar with the office privacy policies,
  o The employee will not read, collect, use or disclose information in any patient record unless required for patient care, or to fulfill their job responsibilities.
  o The employee will not disclose any patient information to anyone except in accordance with the clinic’s policies or as directed by the clinic’s Privacy Officer.

• The clinic’s privacy policy should be available to patients upon request.

9. The office should follow accepted guidelines for the retention and destruction of personal information.

  • According to CAS Policy X-1, patient files must be retained for a period of 15 years.
  • Destruction of personal health information should always be by a method that removes personal identifiers and minimizes the chance of any inadvertent disclosure of information.
  • Destruction of personal health information should be done by cross shredding or incineration.
  • If the office utilizes a third party to store or destroy records, there should be a signed agreement in which the third party agrees to maintain confidentiality with
respect to the information in those records. The agreement should include the process by which the information will be stored or destroyed.

- Storage of files by a third party should protect against theft, loss, damage and limit access. Documents must also be retrievable with a written request.

10. A process should be in place of handling complaints about management of personal health information.

- The process should be defined in the office privacy policy, and usually should be handled by the Privacy Officer.
- In the event that a complaint cannot be resolved, the Privacy Officer or designated individual should know the mechanisms for referral of the complaint to the Chiropractors’ Association of Saskatchewan or to the Office of the Information and Privacy Commissioner.

Chiropractors’ Association of Saskatchewan
3420A Hill Avenue
Regina, SK S4S 0W9
(306) 585-1411

The Office of the Information and Privacy Commissioner
#503 – 1801 Hamilton Street
Regina, SK S4P 4B4
(306) 787-8350