College of Dental Hygienists of Ontario

Protecting your health and your smile

Retention and Safeguarding Policy for Records Containing Personal Information

The College is committed to using, disclosing and retaining personal information in a secure and confidential manner. In addition, the College ensures that documents containing personal information are not retained unnecessarily and are disposed of within a reasonable time frame. Due to the regulatory nature of the College's mandate, records containing personal information are retained according to the following guideline. Unless otherwise stated in this policy, a registrant's permanent file is kept indefinitely. Archives of all Committee material are retained indefinitely in a secure location and may be retained either electronically or in paper form. The guidelines below relate to materials other than that which is contained in the Committee materials.

If there are special circumstances, senior staff may decide to retain a particular file for a longer period. Unless otherwise indicated, the retention period commences with the last entry in a file. These retention policies apply to both written and electronic records.

Discipline, Fitness to Practise, Requests for Funding, and ICRC:

The file, with the exception of the initial complaint/concern, the decision and follow-up requirements, if applicable, is destroyed upon completion of the proceeding or conclusion of the appeal period. Investigator's notes are retained for a period of five (5) years after the file has been closed. Dental records are returned to the practitioner on the conclusion of the investigation. Dental charts/records that cannot be returned will be destroyed after 10 years.

Unauthorized Practice, Civil and Holding Out Proceedings:

The file is retained for a period of 25 years.

Registration:

The initial letter of inquiry is destroyed after one year if the individual does not pursue an application for registration. Incomplete applications containing original documentation relating to the course of study are retained for one year. An attempt is then made to contact the applicant to see if they would like their documents returned. If the applicant does not respond or request the return of the documents, the documents are destroyed. Appeal decisions are kept for an indefinite period of time. A list of closed files is kept indefinitely.

Registrants' Permanent Files:

Permanent files are kept in a secure location and destroyed 10 years following the death of the registrant or 10 years after the person is no longer a member of the College so long as it is at least 75 years from the person's birth.

Renewal Forms:

Renewal forms will be destroyed three (3) years after the date on which they were due. This includes both paper and electronic files.

General Files:

The types of general files that contain personal information may include, but are not limited to, Council/non-Council member files and applications from consultants. These files will be retained for two (2) years following the final day of their respective terms or retainer or correspondence.

Quality Assurance:

Professional portfolios in hard copy will be retained until the applicant meets the assessment guidelines. Electronic copies will be retained on the College system for three (3) years after which they will be transferred to a CD ROM for permanent storage.

Human Resources Files:

Employment records would be retained for five (5) years following the last day of employment.

CDHO Policy for Safeguarding Personal Information (includes Council and Non-Council Members)

The College ensures that personal information it holds is secure by:

- Storing sensitive files in secure locations that are under lock and key or in a supervised area.
- Ensuring that sensitive files in use are within a supervised area.
- Restricting access to personal information to authorized personnel.
- Transporting paper information through sealed, properly addressed envelopes or containers by reputable companies.
- Password protecting electronic files.
- Transmitting electronic information, including faxes, either through a direct line or anonymizing or encrypting the information.
- Frequently reviewing the three-level Internet security system.
- Providing employees of the College with an orientation including the importance of confidentiality and ongoing training regarding the information safeguards required for personal information and their importance.
- Ensuring that external consultants and agencies with access to personal information provide satisfactory assurances of privacy including the signing of confidentiality statements where appropriate.
- Disposing of personal information that is no longer required to be retained in a confidential and secure fashion (i.e. shredding).
- Reviewing its security measures annually to ensure that all personal information is secure.

August 2004

Updated May 2006; October 2009
Reviewed December 2010
Reviewed and updated March 2012
Regulation/Privacy Code March 2011