DENTAL RECORD RETENTION AND DESTRUCTION POLICY

The College of Dental Surgeons of Saskatchewan

1.01 PURPOSE AND SCOPE

This template outlines the requirements for the retention and destruction of personal health information ("PHI") to help ensure compliance with The Health Information Protection Act (the "Act") and The Health Information Protection Regulations, 2023 (the "Regulations").

Your organization may wish to adapt and modify this template to develop its written policy concerning the retention and destruction of personal health information, as required under the Act. Prior to drafting this policy, it is important to review the Act and Regulations to ensure your organization's policy is in compliance with the most current versions in force.

1.02 RETENTION PERIOD

Your organization's written policy must include either:

a) A requirement that PHI must be retained for at least 10 years after the date of the last episode of care or until the individual reaches the age of 20 if the subject individual is a minor, whichever is longer; or,
b) A retention schedule that (a) sets out all legitimate purposes for retaining the information, and (b) the retention period and destruction schedule associated with each purpose set out in connection with (a).

In addition to complying with the retention timelines in the Act, consideration must be given to appropriate retention periods under other application legislation - patient records can be destroyed once the appropriate retention period has expired, determined with reference to other applicable legislation.

1.03 SECURITY AND CONFIDENTIALITY OF PHI

Your organization's written policy must describe how PHI will be security retained and held confidential to minimize the risk of unauthorized access, use or disclosure. Administrative, technical and physical measures should be adopted to maintain the security and confidentiality of PHI, and these measures should be detailed in your written policy.

a) Administrative Measures
    i) Provide training and ongoing education to provided employees on the importance of PHI security and confidentiality.
    ii) Require employees sign confidentiality agreements acknowledging their understanding of their obligations and consequences of breaches. This requirement is separately set out in the Act.
b) Technical Measures
    i) Implement access controls to ensure that only authorized personnel can access PHI. Access controls include using encryption for PHI stored electronically to protect against unauthorized access, and regularly updating and patching office software to protect against security vulnerabilities.
c) Physical Measures:
    i) Store paper records in locked, secure areas accessible only to authorized personnel.
    ii) Use secure containers for the disposal of paper records to be destroyed.
    iii) Implement monitoring to detect and prevent unauthorized access to areas where PHI is stored.

1.04 DESTRUCTION OF RECORDS

Your organization's written policy must outline the process by which PHI is destroyed. In connection with destroying PHI, your organization must maintain a destruction log.

a) Destruction Process
    i) Your organization should designate an individual who is tasked with approving the destruction PHI. This individual's approval should come after their consultation with and receipt of approval from the relevant health care providers.
b) Destruction Log: In connection with the destruction of PHI, a destruction log must be completed. Destruction logs should be kept permanently in a safe location. Destruction logs must contain the following information:
    i) The name of each individual whose PHI was destroyed;
    ii) A summary of what PHI was destroyed;
    iii) The time period of the PHI;
    iv) The method of destruction of the PHI; and,
    v) The name and job title of the individual responsible for supervising the destruction.
c) Destruction Methods
    i) Paper Records: Use cross-cut shredding or incineration to ensure that paper records are completely destroyed and cannot be reconstructed.
    ii) Electronic Records: Use software that ensures the complete and irretrievable deletion of electronic records. Physically destroy electronic storage media (e.g., hard drives) that are no longer in use.

1.05 REVIEW AND UPDATES

Ensure that your organization's policy will be reviewed annually and updated as necessary to ensure continued compliance with legislative requirements and best practices.