

Politique de conservation et destruction des dossiers

Objectif

L'objectif de cette politique est de fournir des procédures de clôture, de conservation et de destruction des dossiers de client maintenus par l'organisme.

2. Définitions

2.1 Dans la présente politique :

« **date de clôture de dossier** » s'entend de la date à laquelle le responsable d'un dossier a déterminé que le dossier est terminé et à partir de laquelle il détermine la destruction du dossier.

« **date de destruction du dossier** » s'entend de la date à partir de laquelle un dossier est détruit.

3. Examiner et clore le dossier

3.1 La Fondation de l'Hôpital régional de Saint-Jérôme nomme un responsable de l'application de la présente politique. À défaut, la Direction générale de la Fondation de l'Hôpital régional de Saint-Jérôme est responsable de l'application de la présente politique.

3.2 Quand un dossier est terminé, le responsable du dossier détermine la date de clôture du dossier et sa date de destruction. Pour les dossiers concernant les donateurs et donateurs potentiels, il est convenu que le dossier doit être détruit après dix (10) ans de la date de son dernier don ou son dernier consentement à l'utilisation de ses renseignements personnels, la date la plus récente ayant préséance.

3.3 Avant de fermer le dossier et d'envoyer un document physique ou autre bien lié au dossier à un site d'entreposage externe ou à un service de déchiquetage, le responsable du dossier doit prendre des mesures pour retirer du dossier copies papier de documents qui ont été mis en images ou autrement sauvegardés dans la bibliothèque électronique de l'organisme.

3.4 L'organisme tient des registres identifiant les dossiers clos, y compris la date de clôture et le cas échéant, la date de destruction.

4. Conservation des dossiers fermés

4.1 Les dossiers fermés et non détruits sont entreposés dans un lieu physique pour maintenir la confidentialité des personnes concernées et pour les protéger contre les dommages ou la perte. Ils peuvent aussi être conservés sur notre réseau informatique SharePoint accessible seulement aux employés autorisés.

5. Destruction des dossiers

5.1 Quand le responsable du dossier ferme le dossier et si le dossier est prêt pour la destruction (voir article ci-dessous), la date de destruction est déterminée selon la norme de l'organisme tel que défini dans l'article 5.2 à moins que le responsable du dossier détermine qu'une autre date de destruction conviendrait mieux.

5.2 L'organisme conserve les dossiers fermés principalement pour satisfaire aux craintes concernant la gestion du risque. En conséquence, il est prudent de conserver le dossier fermé pendant une période déterminée selon les exigences légales qui seraient requises.

5.3 La date de destruction doit être suspendue dans les cas suivants se rapportant directement ou indirectement à : a) une réclamation réelle ou potentielle envers l'organisme, b) une demande de divulgation d'information concernant le dossier ou donateur concerné, c) audits et enquêtes gouvernementales. Cela peut être ordonné par le responsable du dossier.

5.4 La date de destruction de dossiers peut être reportée à tout moment au besoin (par exemple, si un nouveau consentement était accordé entre-temps).

5.5 Cette politique doit s'appliquer de manière à assurer le maintien de la confidentialité des renseignements personnels et le respect des lois fédérales et provinciales applicables en matière de protection des renseignements personnels.

5.6 L'organisme maintient un registre de dossiers détruits qui comprend le nom du donateur, le numéro de dossier, la date de clôture du dossier, la date de destruction du dossier et le nom du responsable du dossier.

L'organisme procède à la destruction des dossiers papiers et des dossiers électroniques notamment les renseignements et données électroniques comprennent notamment les courriels, les versions préliminaires de documents se trouvant sur un serveur ou un système de gestion des documents, les images de documents ou les documents numérisés, les télécopies (lorsqu'il n'existe pas de copie papier), la messagerie vocale, les métadonnées ainsi que les autres renseignements ou données relatifs à une affaire qui sont sauvegardés et entreposés en format électronique (par ex., sur des serveurs, des médias magnétiques, des systèmes magnéto-optiques, des disques compacts, des DVD).