

	<b>Règles d'entreprise</b>	<b>Page</b> 1 de/of 17
<b>TITRE /TITLE</b>		
<b><i>POLITIQUE DE PROTECTION DE LA VIE PRIVÉE</i></b>		
<b># VERSION /01</b>		

## TABLE DES MATIÈRES

<b>INTRODUCTION</b> .....	<b>2</b>
<b>1. DÉFINITIONS</b> .....	<b>2</b>
<b>2. OBJECTIFS</b> .....	<b>4</b>
<b>3. PORTÉE</b> .....	<b>4</b>
<b>4. RESPONSABILITÉS</b> .....	<b>4</b>
<b>5. COLLECTE DE RENSEIGNEMENTS PERSONNELS</b> .....	<b>4</b>
5.1 Source des Renseignements personnels .....	4
5.2 Fondement juridique pour la collecte .....	5
5.3 Informations à fournir au moment de la collecte .....	6
5.4 Principe de minimisation des Renseignements personnels .....	6
<b>6. UTILISATION DES RENSEIGNEMENTS PERSONNELS</b> .....	<b>7</b>
6.1 Fins.....	7
6.2 Utilisation pour le Traitement automatisé.....	7
6.3 Utilisation secondaire des Renseignements personnels au Québec .....	8
<b>7. DIVULGATION DE RENSEIGNEMENTS PERSONNELS</b> .....	<b>8</b>
7.1 Au sein de Theratechnologies .....	8
7.2 À des tiers.....	8
7.3 Divulgations spécifiques autorisées par la Loi sur le secteur privé du Québec.	9
7.4 Transfert de Renseignements personnels à l'extérieur de l'UE / de l'Espace économique européen (« EEE ») ou du Québec .....	10
7.5 Autres situations nécessitant une EFRVP .....	11
<b>8. CONSERVATION DES RENSEIGNEMENTS PERSONNELS</b> .....	<b>11</b>
<b>9. EXACTITUDE DES RENSEIGNEMENTS PERSONNELS</b> .....	<b>12</b>
<b>10. SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS ET VIOLATION DES DONNÉES</b> .....	<b>12</b>
10.1 Mesures générales de sauvegarde et de sécurité .....	12
10.2 Destruction sécurisée, archivage ou anonymisation .....	12
10.3 Incident de confidentialité .....	13
<b>11. DROITS DES INDIVIDUS</b> .....	<b>13</b>
<b>12. FORMATION</b> .....	<b>15</b>
<b>13. NOUS CONTACTER</b> .....	<b>15</b>
13.1 Coordonnées .....	15
13.2 Plaintes.....	16
<b>14. APPLICATION ET RÉVISION DE LA PRÉSENTE POLITIQUE</b> .....	<b>16</b>

## INTRODUCTION

La présente politique de protection de la vie privée (« **Politique** ») décrit les principes directeurs de Theratechnologies Inc. (y compris ses filiales Theratechnologies Europe Limited et Theratechnologies U.S. Inc. appelées collectivement « **Thera** ») concernant la collecte, l'utilisation, la divulgation et la protection des Renseignements personnels (tels que définis ci-dessous) et la façon dont ces Renseignements personnels peuvent être consultés et corrigés, le cas échéant.

Thera, une société biopharmaceutique de stade clinique axée sur le développement et la commercialisation de thérapies novatrices, s'engage à protéger la confidentialité et l'exactitude de tous les Renseignements personnels qu'elle recueillera, utilisera, divulguera ou conservera et à se conformer à toutes les Lois applicables en matière de protection de la vie privée (telles que définies ci-dessous).

Dans le cadre de ses activités, Thera, agissant en tant que responsable du traitement, sera en contact avec les Renseignements personnels des individus identifiables, incluant, mais sans s'y limiter, les clients, les visiteurs des sites web, les employés ou les patients ayant indirectement accès à l'un ou l'autre des produits de Thera.

## 1. DÉFINITIONS

- « **Autorités Réglementaires** » désigne toute autorité publique indépendante, établie par la loi, qui a compétence pour superviser les questions relatives à la protection de la vie privée et des Renseignements personnels;
- « **Délégué de la protection des données** » ou « **DPD** » a la signification qui lui est attribuée à l'article 13.1;
- « **Employés** » désigne tous les employés, c'est-à-dire les directeurs, les employés, les stagiaires et toute autre personne qui travaille à temps plein ou à temps partiel, de manière permanente ou temporaire, et qui est en droit de recevoir un salaire de Thera;
- « **Évaluation de l'impact du transfert** » ou « **EIT** » a la signification qui lui est attribuée dans la section 7.4(c);
- « **Évaluation des facteurs relatifs à la vie privée** » ou « **EFRVP** » a la signification qui lui est attribuée à la section 7.4(c);
- « **Fins** » a la signification qui lui est attribuée à la section 5.3;
- « **Incident de confidentialité** » a la signification qui lui est attribuée à l'article 10.3;
- « **Individu** » désigne une personne physique identifiée ou identifiable;
- « **Lois applicables en matière de protection de la vie privée** » désigne toute loi, tout règlement ou toute recommandation liés aux questions sur la protection de la vie privée et applicable à Thera, y compris notamment la *Loi sur la protection des renseignements personnels dans le secteur privé* (« **Loi sur le secteur privé du Québec** »), la *Loi sur la protection des renseignements personnels et les documents électroniques* (« **LPRPDE** ») et le *Règlement général sur la protection des données* (« **RGPD** ») de l'Union européenne (« **UE** »). Les lois applicables en matière de protection de la vie privée comprennent

également toute loi, tout règlement, toute recommandation ou toute orientation officiels remplaçant, ajoutant, modifiant, étendant, reconstituant ou consolidant l'une des lois susmentionnées;

- « **Mineur** » a la signification qui lui est attribuée à l'article 11;
- « **Politique** » a la signification qui lui est attribuée dans l'introduction;
- « **Principe de minimisation des données** » a la signification qui lui est attribuée dans l'article 5.4;
- « **Renseignements non personnellement identifiables** » ou « **RNPI** » sont des renseignements qui ne se rapportent pas à une personne physique identifiée ou identifiable. Les RNPI comprennent également les Renseignements personnels agrégés ou rendus anonymes de telle sorte qu'un Individu n'est plus identifiable;
- « **Renseignements personnels** » désigne toute information factuelle ou subjective, enregistrée ou non, concernant un Individu identifiable, telle que l'âge, le sexe, la date de naissance, la province de résidence, les préférences, les opinions, qui permet d'identifier directement cet Individu (par exemple le nom d'une personne), ou qui pourrait permettre d'identifier cet Individu une fois les renseignements combinés (par exemple les éléments d'une description physique). Les Renseignements personnels ne comprennent pas les renseignements qui ont été rendus anonymes ou agrégés de telle sorte qu'il n'existe aucune possibilité sérieuse qu'elles puissent être utilisées pour identifier un Individu, que ce soit en tant que telles ou en combinaison avec d'autres informations;
- « **Renseignements sensibles** » désigne tout Renseignement personnel qui, en raison de sa nature médicale, biométrique ou autrement intime, suscite une attente élevée en matière de respect de la vie privée. En vertu du RGPD, les Renseignements sensibles sont des Renseignements personnels révélant l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l'appartenance syndicale, et le traitement des données génétiques, des données biométriques, des données relatives à la santé ou des données relatives à la vie sexuelle ou à l'orientation sexuelle d'une personne physique;
- « **Responsable de la protection des Renseignements personnels** » est la personne identifiée à l'article 13.1;
- « **Thera** » a la signification qui lui est attribuée dans l'introduction;
- « **Traitement** » désigne toute opération effectuée sur des Renseignements personnels ou sur des ensembles de Renseignements personnels, que ce soit par des moyens automatisés ou non, telle que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition, l'alignement ou la combinaison, la restriction, l'effacement ou la destruction;
- « **Sites web** » a la signification qui lui est attribuée à la section 3 iv.

## 2. OBJECTIFS

La présente Politique définit un cadre spécifique en matière de protection de la vie privée et constitue la politique principale concernant la protection des Renseignements personnels chez Thera. Les objectifs de cette Politique sont notamment les suivants :

- Définir les principes de gouvernance, les rôles et les responsabilités au sein de Thera en ce qui concerne la protection des Renseignements personnels tout au long de leur cycle de vie;
- Fournir une procédure claire permettant aux Individus d'exercer leurs droits; et
- Définir la procédure de traitement des plaintes relatives à la protection de la vie privée.

## 3. PORTÉE

La présente Politique s'applique à tous les Renseignements personnels des Individus traités par Thera ou divulgués à Thera par des tiers, y compris, mais sans s'y limiter, les Renseignements personnels des :

- i. Individus recueillis dans le cadre de leurs interactions professionnelles avec les Employés de Thera ou les prestataires de services de Thera;
- ii. Membres du grand public qui contactent Thera pour se renseigner sur des services ou des produits;
- iii. Visiteurs entrant dans les locaux commerciaux de Thera; et
- iv. Visiteurs ou des utilisateurs des sites web et des services en ligne de Thera (collectivement, les « **Sites web** ») situés aux adresses suivantes :

(a) <https://www.theratech.com>

(b) <https://www.trogarzo.com>

(c) <https://www.egriftasv.com>

## 4. RESPONSABILITÉS

La protection de la vie privée des Individus relève de la responsabilité de chaque Employé, qui doit lire, comprendre et respecter la présente Politique. De manière plus précise, il incombe à chaque Employé de vérifier que toutes les mesures nécessaires pour satisfaire aux exigences énoncées dans la présente Politique sont en place avant de traiter des Renseignements personnels. Les Employés sont encouragés à contacter [privacy@theratech.com](mailto:privacy@theratech.com) pour obtenir de l'aide afin de confirmer que des mesures suffisantes ont été mises en place.

## 5. COLLECTE DE RENSEIGNEMENTS PERSONNELS

### 5.1 Source des Renseignements personnels

#### (a) Fournis par des Individus

D'une manière générale, les Renseignements personnels recueillis sont fournis par un Individu dans le cadre de son interaction avec Thera. Lorsqu'ils contactent ou sont contactés par Thera, les Individus peuvent être tenus de fournir des Renseignements personnels, notamment dans les cas suivants :

- En interagissant avec les Employés de Thera par le biais d'appels téléphoniques, de courriels, de formulaires web, de médias sociaux et d'autres méthodes de communication;
- En s'abonnant aux outils promotionnels de Thera;
- En entrant dans les locaux de Thera; et
- En visitant ou en utilisant les Sites web de Thera.

### **(b) Renseignements personnels obtenus légalement par des tiers**

Lors d'interactions avec des tiers, Thera doit seulement accepter la divulgation des Renseignements personnels qui ont été légalement recueillis ou autrement obtenus par ces tiers, lesquels doivent également avoir mis en place une politique de confidentialité régissant la protection des Renseignements personnels en conformité avec les Lois applicables en matière de protection de la vie privée.

Avant l'échange de Renseignements personnels, l'Employé de Thera doit obtenir une confirmation écrite de la part de la tierce partie indiquant : (i) qu'elle a légalement recueilli les Renseignements personnels; et (ii) qu'elle a le droit de divulguer ces Renseignements personnels à Thera.

### **(c) Renseignements personnels collectés automatiquement**

Thera peut également collecter des Renseignements personnels et RNPI sur les Individus, liés à leurs habitudes de navigation sur internet lorsqu'ils visitent ou utilisent les Sites web, les applications mobiles ou d'autres plateformes de médias sociaux de Thera. Pour plus d'informations, veuillez consulter notre [Politique sur les témoins navigateurs](#).

## **5.2 Fondement juridique pour la collecte**

### **(a) Consentement**

Mis à part lorsque des fondements juridiques alternatifs s'appliquent, Thera obtiendra toujours le consentement d'un Individu avant de procéder au Traitement de ses Renseignements personnels, et ce consentement sera documenté par écrit. Tout Employé qui recueille le consentement d'un Individu doit également noter la date à laquelle le consentement a été donné, ainsi que la nature du consentement recueilli (par exemple, en écrivant, en cochant une case, etc.).

Le consentement doit être manifeste, libre et éclairé et être donné pour une Fin (tel que défini à la section 5.3) précise. Cela signifie qu'un Individu doit comprendre ce à quoi il consent et qu'il doit être raisonnable de s'attendre à ce qu'il comprenne la nature, le but et les conséquences du Traitement de ses Renseignements personnels. Si le Traitement implique un transfert de Renseignements personnels à des tiers, Thera obtiendra le consentement de l'Individu pour un tel transfert et le consentement devra expressément inclure la juridiction dans laquelle les Renseignements personnels seront transférés.

Les Individus peuvent, à tout moment, modifier ou retirer leur consentement. Les Employés qui recueillent des Renseignements personnels doivent fournir aux Individus concernés la procédure complète afin d'exercer leur droit de rétractation, conformément à la section 11 ci-dessous.

## **(b) Fondements juridiques alternatifs en vertu du RGPD**

Lorsqu'il est applicable, le RGPD permet à Thera de s'appuyer sur des fondements juridiques autres que le consentement pour le Traitement des Renseignements personnels.

Les fondements juridiques alternatifs pour le traitement des Renseignements personnels des résidents de l'UE, tels que définis dans la présente Politique, sont les suivants :

- Lorsque l'utilisation des Renseignements personnels est nécessaire à l'exécution des obligations de Thera en vertu d'un contrat avec un résident de l'UE (par exemple : lorsque le résident de l'UE utilise les Sites web);
- Lorsque l'utilisation des Renseignements personnels est nécessaire aux intérêts légitimes de Thera ou aux intérêts légitimes d'autres Individus (par exemple, pour assurer la sécurité du site web de Thera ou pour prévenir la fraude liée à l'un des produits ou services de Thera). Dans une telle situation, Thera tiendra compte des droits des Individus en vertu du RGPD et les mettra en balance avec les intérêts légitimes de Thera; et
- Lorsque l'utilisation des Renseignements personnels est nécessaire pour se conformer aux exigences légales ou défendre les droits légaux de Thera.

### **5.3 Informations à fournir au moment de la collecte**

L'objectif commercial légitime et spécifique au Traitement (« **Fin** ») doit toujours être identifiée par Thera avant ou au moment de la collecte de ces Renseignements personnels. Thera doit toujours limiter la collecte des Renseignements personnels à ce qui est strictement nécessaire pour atteindre la Fin identifiée.

Outre l'identification de la Fin, il convient de répondre aux questions suivantes et de les communiquer à l'Individu concerné avant la collecte de ses Renseignements personnels :

- Quels sont les Renseignements personnels collectés?
- Pourquoi sont-ils collectés?
- Comment sont-ils collectés?
- Où sont-ils conservés?
- Comment sont-ils sécurisés?
- Qui y a accès ou les utilise?
- Avec qui sont-ils partagés?
- Le cas échéant, Thera utilise-t-elle une technologie qui comprend des fonctions permettant d'identifier, de localiser ou de profiler les personnes et, dans l'affirmative, quels sont les moyens offerts pour activer/désactiver ces fonctions?
- Quand sont-ils éliminés?

### **5.4 Principe de minimisation des Renseignements personnels**

Sauf s'il est autrement autorisé par la présente Politique, Thera traitera toujours le minimum des Renseignements personnels nécessaires à la réalisation des Fins pour lesquelles ils ont été recueillis (le « **Principe de minimisation des données** »).

### (a) Application du Principe de minimisation des données

Le Principe de minimisation des données s'applique à tous les services et activités de Thera impliquant le Traitement des Renseignements personnels.

### (b) Procédure générale de mise en œuvre du Principe de minimisation des données

- **Mise en œuvre de mesures techniques et organisationnelles.** Thera mettra en œuvre, tant au moment de la détermination des moyens de Traitement qu'au moment du Traitement lui-même, les mesures techniques et organisationnelles appropriées afin de se conformer au Principe de minimisation des données. Par exemple :
  - **Personnes ayant accès.** Le Responsable de la protection des Renseignements personnels de Thera (tel qu'identifié à la section 13) identifiera un nombre limité d'Employés qui seront autorisés à traiter les Renseignements personnels.
  - **Identification des Fins du Traitement.** Avant de Traiter des Renseignements personnels, l'Employé identifiera les Fins du Traitement.
  - **Limitation de l'accès et du Traitement des Renseignements personnels.** Thera fournira à l'Employé autorisé l'accès aux Renseignements personnels et cet accès sera limité à ce qui est nécessaire pour atteindre les Fins identifiées.

## 6. UTILISATION DES RENSEIGNEMENTS PERSONNELS

### 6.1 Fins

Les Renseignements personnels ne doivent être utilisés que (i) pour les Fins identifiées par Thera lorsque le consentement a été obtenu conformément à la présente Politique; ou (ii) pour des Fins conformes au fondement juridique alternatif en vertu du RGPD. Les objectifs susmentionnés peuvent inclure :

- Le Traitement des commandes de services et/ou de produits de Thera;
- L'envoi de matériel promotionnel, de bulletins d'information, d'offres ou d'autres informations;
- Le Traitement et la réponse aux plaintes et aux demandes de renseignements;
- Le respect des exigences légales ou réglementaires; et
- Tout autre objectif mentionné dans d'autres politiques internes.

### 6.2 Utilisation pour le Traitement automatisé

Si Thera utilise des Renseignements personnels pour prendre une décision fondée exclusivement sur un Traitement automatisé de ces renseignements, Thera doit en informer l'Individu concerné au plus tard au moment où elle l'informe de la décision. Sur demande, Thera doit également fournir les éléments suivants :

- i. Les Renseignements personnels qui ont été utilisés pour rendre la décision;
- ii. Les raisons et les principaux facteurs et paramètres qui ont mené à la décision; et

- iii. Le droit de l'Individu concerné de faire corriger les Renseignements personnels utilisés pour prendre la décision.

L'Individu concerné doit avoir la possibilité de présenter ses observations en s'adressant à [privacy@theratech.com](mailto:privacy@theratech.com).

### **6.3 Utilisation secondaire des Renseignements personnels au Québec**

La *Loi sur le secteur privé du Québec* permet aux entreprises d'utiliser des Renseignements personnels à une autre Fin sans le consentement de l'Individu concerné dans les situations spécifiques suivantes :

- Lorsque l'utilisation est conforme à l'objectif initial pour lequel les renseignements ont été traités (les objectifs conformes n'incluent pas la prospection commerciale ou philanthropique);
- Lorsque l'utilisation est clairement dans l'intérêt d'un Individu;
- Lorsque l'utilisation est nécessaire à la prévention et/ou à la détection de la fraude ou à l'évaluation et à l'amélioration des garanties et des mesures de sécurité;
- Lorsque l'utilisation est nécessaire pour fournir ou livrer un produit ou un service demandé par un Individu; et
- Lorsque l'utilisation est nécessaire à des fins d'étude, de recherche ou de statistique et les renseignements sont dépersonnalisés.

Lorsque l'utilisation secondaire envisagée concerne des Renseignements sensibles, Thera doit obtenir expressément le consentement de l'Individu concerné.

## **7. DIVULGATION DE RENSEIGNEMENTS PERSONNELS**

### **7.1 Au sein de Theratechnologies**

Les Renseignements personnels traités au sein de Thera ne seront accessibles ou divulgués qu'aux Employés identifiés par le Responsable de la protection des Renseignements personnels qui ont besoin de connaître ces renseignements pour exercer leurs fonctions comme l'exige leur poste, le tout conformément aux Fins identifiées au moment du Traitement des Renseignements personnels.

### **7.2 À des tiers**

Thera peut communiquer des Renseignements personnels à des tiers qui ont besoin de les connaître pour aider Thera à atteindre les Fins identifiées définis au moment où le consentement a été donné.

Lorsque Thera transfère des Renseignements personnels à des tiers en vue de leur traitement, ils ne peuvent être utilisés qu'aux Fins pour lesquels le consentement a été donné à l'origine. En outre, le tiers doit fournir un niveau de protection adéquat qui peut être comparé au niveau de protection dont les Renseignements personnels auraient bénéficié s'ils n'avaient pas été transférés. Un niveau de protection adéquat comprend :

- (a) ***Une entente écrite*** définissant les rôles et les responsabilités des parties en ce qui concerne les Renseignements personnels, en particulier les mesures mises en place par le tiers pour :

- Protéger la confidentialité des Renseignements personnels fournis;
- Veiller à ce que les Renseignements personnels ne soient utilisés qu'aux Fins précisés dans l'entente; et
- Veiller à ce que les Renseignements personnels ne soient pas conservés après l'expiration ou la résiliation anticipée de l'entente.

De plus, l'entente doit stipuler que :

- Le tiers doit informer sans délai le Responsable de la protection des Renseignements personnels de Thera de toute violation ou tentative de violation des obligations de confidentialité contenues dans l'entente; et
- Thera se réserve le droit de procéder à tout audit relatif aux mesures de confidentialité mises en œuvre par le tiers.

**(b) Politiques** régissant le Traitement des Renseignements personnels.

En outre, les Renseignements personnels peuvent être divulgués à des tiers dans les situations suivantes :

- Tel que permis par les Lois applicables en matière de protection de la vie privée. Dans ce cas, Thera s'efforcera de ne pas divulguer plus de Renseignements personnels que ce qui est légalement requis;
- Pour se conformer à des procédures légales valides, telles que les mandats de perquisition, les citations à comparaître ou les ordonnances des tribunaux;
- Lors de situation d'urgence ou lorsque cela est nécessaire pour protéger la sécurité d'une personne ou les locaux ou les actifs de Thera; ou
- Lorsque les Renseignements personnels sont déjà accessibles au public au moment de leur divulgation.

### **7.3 Divulgations spécifiques autorisées par la Loi sur le secteur privé du Québec**

Thera peut, sans le consentement d'un Individu, communiquer les Renseignements personnels comme suit :

- À une personne ou un organisme ayant le pouvoir d'exiger la divulgation de Renseignements personnels et qui a en a besoin dans l'exercice de ses fonctions;
- À une personne qui doit recevoir les Renseignements personnels en raison d'une situation d'urgence menaçant la vie, la santé ou la sécurité d'un Individu, ou à qui Thera peut divulguer les renseignements pour prévenir un acte de violence, y compris un suicide, s'il y a un risque sérieux de décès ou de blessure grave pour un Individu;
- À toute personne si les Renseignements personnels datent de plus de 100 ans ou si l'Individu concerné est décédé depuis plus de 30 ans;
- À une personne ou une organisation dans le cadre d'un mandat ou d'un contrat de service ou d'un contrat d'entreprise;
- À l'autre partie dans le cadre d'une transaction commerciale si la divulgation est nécessaire pour mener à bien la transaction;
- À une personne qui peut l'utiliser à des fins d'études, de recherche ou de statistique ou à une personne autorisée par la *Commission d'accès à l'information* à l'utiliser;
- À une personne autorisée par la loi à recouvrer des créances pour autrui et qui en a besoin à cette fin dans l'exercice de ses fonctions; et
- À une personne si les Renseignements personnels sont nécessaires au recouvrement d'une créance de Theratechnologies.

Thera tiendra un registre des divulgations de Renseignements personnels susmentionnés.

#### **7.4 Transfert de Renseignements personnels à l'extérieur de l'UE / de l'Espace économique européen (« EEE ») ou du Québec**

Le transfert de Renseignements personnels à l'extérieur de l'UE/EEE ou du Québec, au sein de Thera ou à tiers, est acceptable :

- (a) Si aux États-Unis, le tiers qui reçoit les Renseignements personnels fait partie du cadre de protection des données UE – États-Unis. Pour une liste complète des entreprises participantes, veuillez consulter : <https://www.dataprivacyframework.gov/s/participant-search>.
- (b) Si en dehors du Canada ou des États-Unis, le pays a été reconnu par la Commission européenne comme offrant un cadre juridique adéquat en matière de protection de la vie privée. Pour obtenir la liste complète des pays offrant un cadre juridique adéquat en matière de protection de la vie privée, veuillez consulter : [https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_fr](https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_fr) et <https://www.cnil.fr/fr/maitriser-mes-donnees>.
- (c) Lorsque le cadre juridique en matière de protection de la vie privée d'un pays n'est pas considéré comme adéquat, une évaluation des incidences du transfert (« EIT ») en vertu du RGPD ou une évaluation des facteurs relatifs à la vie privée (« EFRVP ») en vertu de la *Loi sur le secteur privé du Québec* doit être effectuée avant le transfert des Renseignements personnels.
  - Une ETI ou EFRVP visent essentiellement à évaluer l'impact qu'un transfert vers un pays hors de l'UE/EEE ou hors du Québec peut avoir sur la protection et la sauvegarde sécuritaire des Renseignements personnels ainsi que sur le droit à la vie privée des Individus.
  - La première partie de l'évaluation comprend une analyse des lois, des pratiques et des autorités publiques en place dans la juridiction destinataire afin de déterminer si un élément de cette juridiction pourrait avoir un impact négatif sur l'efficacité des mesures prises pour assurer la protection des Renseignements personnels.
  - La deuxième partie de l'EIT ou de EFRVP comprend une analyse de la nature des Renseignements personnels transférés (en particulier, s'il s'agit de Renseignements sensibles ou non) et des mesures de sécurité mises en place. Les mesures auxquelles il est fait référence ici sont par exemple, en vertu de du RGPD, les clauses contractuelles types (« CCT ») de la Commission européenne.
  - Si l'EIT ou EFRVP révèle qu'il n'y a pas de risque pour les Renseignements personnels des Individus, le transfert peut avoir lieu avec des mesures appropriées telles que les CCT susmentionnées ou un accord écrit au Québec, le cryptage des Renseignements personnels et l'application du Principe de minimisation des données.
  - Si la conclusion de l'EIT ou EFRVP est que la sécurité des Renseignements personnels ne serait pas garantie, le transfert ne doit pas avoir lieu.

Les Employés de Thera qui envisagent de transférer des Renseignements personnels doivent toujours consulter [privacy@theratech.com](mailto:privacy@theratech.com) avant de procéder à un tel transfert.

## **7.5 Autres situations nécessitant une EFRVP**

Sous la supervision du Responsable de la protection des Renseignements personnels, Thera devra procéder à une EFRVP, entre autres, lors des situations suivantes :

- Avant d'entreprendre tout projet d'acquisition, de développement ou de refonte d'un système d'information ou d'un système de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de Renseignements personnels; et
- Avant de divulguer des Renseignements personnels sans consentement à un Individu ou un organisme qui souhaite les utiliser à des Fins d'étude, de recherche ou de production de statistiques. Dans cette situation particulière, la demande doit être soumise au Responsable de la protection des Renseignements personnels de Thera. Si la conclusion de l'EFVRP est que les Renseignements personnels peuvent être divulgués pour les Fins susmentionnées, Thera doit conclure une entente écrite et cette entente doit inclure le contenu obligatoire de la législation (comme mentionné à l'article 7.2 (a)) et toute mesure de protection additionnelle identifiée dans l'EFVRP.

Lors de la réalisation de l'EFVRP, Thera examinera si les Renseignements personnels à Traiter sont sensibles ou non, les Fins pour lesquelles ils seront utilisés, la quantité, les moyens de distribution et le support de conservation des Renseignements personnels.

La réalisation de l'EFVRP permet de démontrer que Thera a pris les mesures nécessaires afin d'assurer une protection efficace des Renseignements personnels.

## **8. CONSERVATION DES RENSEIGNEMENTS PERSONNELS**

Les Renseignements personnels seront toujours conservés conformément aux Lois applicables en matière de protection de la vie privée et à toute autre loi applicable (y compris dans le but de satisfaire à toute exigence ou obligation légale, comptable ou autre ou dans le but d'établir ou de défendre des réclamations juridiques potentielles), tel qu'indiqué dans le calendrier de conservation de Thera.

Sauf lorsque la loi le permet, Thera ne conservera les Renseignements personnels qu'aussi longtemps que nécessaire pour atteindre les Fins pour lesquelles ils ont été recueillis.

Une fois la Fin du Traitement des Renseignements personnels atteinte, Thera détruira ou archivera les Renseignements personnels ou, s'il existe une raison sérieuse et légitime de le faire, rendra les Renseignements personnels anonymes conformément aux Lois applicables en matière de protection de la vie privée. Les Renseignements Personnels rendus anonymes seront conservés dans une base de données distincte, créée au besoin, et ne seront accessibles que si nécessaire, et en rapport avec les Fins initiales du Traitement. Les Renseignements personnels qui présentent encore un intérêt administratif pour les départements concernés (par exemple, les services juridiques) seront sauvegardés sur un logiciel de gestion de serveur de fichiers. Ces Renseignements personnels doivent être accessibles seulement aux Employés qui ont un besoin d'en prendre connaissance et être conservés aussi longtemps que le prévoit le calendrier de conservation de Thera. Seuls les Renseignements personnels présentant un intérêt historique, scientifique ou statistique justifiant leur conservation peuvent être conservés pour une durée indéterminée dans une base de données distincte. Tout Employé souhaitant rendre anonymes des Renseignements personnels doit en faire la demande auprès de [privacy@theratech.com](mailto:privacy@theratech.com).

## 9. EXACTITUDE DES RENSEIGNEMENTS PERSONNELS

Les Renseignements personnels utilisés par Thera sont tenus aussi exacts et complets que possible de le faire afin de réduire au minimum la possibilité qu'une décision touchant un Individu soit prise sur la base de renseignement inexact. Si l'utilisation de Renseignements personnels peut nuire à un Individu ou à Thera, il est essentiel que des mesures visant à vérifier l'exactitude et l'exhaustivité de ces Renseignements personnels soient mises en œuvre avant leur utilisation ou leur divulgation.

Si les Renseignements personnels sont susceptibles d'être inexacts ou obsolètes, les Employés doivent prendre note de la possibilité d'inexactitude et informer toutes autres personnes susceptibles d'utiliser ces Renseignements personnels. Dans la mesure du possible, Thera prendra des mesures appropriées pour s'assurer que les Renseignements personnels sont mis à jour afin de respecter la norme d'exactitude susmentionnée, par exemple en procédant à un examen annuel de la base de données.

Les Individus qui ont fourni des Renseignements personnels sont encouragés à informer Thera de toute mise à jour nécessaire concernant leurs Renseignements personnels.

Il incombe à chaque Employé de veiller à ce que les Renseignements personnels à son sujet qui sont traités par Thera soient exacts en tout temps.

## 10. SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS ET VIOLATION DES DONNÉES

### 10.1 Mesures générales de sauvegarde et de sécurité

(a) **Norme de sécurité.** Thera doit mettre en œuvre et maintenir des mesures de sécurité pour protéger les Renseignements personnels, quel que soit le format dans lequel ils sont conservés, contre la perte, le vol ou la collecte, l'utilisation ou la divulgation non autorisée (y compris l'accès, la copie ou la modification non autorisés). Ces mesures de sécurité doivent être adaptées à la nature, à la quantité, aux moyens de distribution, au format et à la méthode de conservation des Renseignements personnels.

(b) **Méthodes de sécurité.** Les méthodes de protection comprennent :

- i. Des mesures physiques, par exemple la restriction de l'accès aux locaux et aux systèmes informatiques de Thera;
- ii. Des mesures organisationnelles, par exemple la limitation de l'accès sur la base du « besoin de savoir »; et
- iii. Des mesures technologiques, par exemple l'utilisation de mots de passe et le cryptage, la protection contre des logiciels malveillants, l'utilisation d'un logiciel de gestion de serveur de fichiers pour fournir des pistes d'audit de tout accès.

### 10.2 Destruction sécurisée, archivage ou anonymisation

(a) **Norme de destruction.** Une fois la période de conservation des Renseignements personnels écoulée (conformément au calendrier de conservation de Thera), Thera détruira, archivera ou rendra anonymes les Renseignements personnels conformément à l'article 8 de la présente Politique.

(b) **Méthodes de destruction.** Thera appliquera les principes suivants en ce qui concerne la destruction et l'effacement des Renseignements personnels :

- i. Les Renseignements personnels en format papier seront détruits par déchiquetage transversal;
- ii. Les documents contenant des Renseignements personnels ne seront pas placés au rebut, à moins que ces déchets ne soient ensuite déchiquetés et que les renseignements ne soient protégés contre tout accès non autorisé en attendant leur destruction; et
- iii. Les supports de stockage électroniques seront soumis à un logiciel ou à des techniques de suppression sécurisée conformes aux normes de l'industrie.

### **10.3 Incident de confidentialité**

Une violation de données ou un « **Incident de confidentialité** » est toute violation (potentielle) de la sécurité entraînant la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé ou illégal à des Renseignements personnels traités par Thera, ainsi que toute autre violation de la protection de ces renseignements.

La prévention d'un Incident de confidentialité relève de la responsabilité de tous les Employés. Tout Employé qui soupçonne une violation de la présente Politique ou une irrégularité relative aux activités de Traitement des Renseignements personnels doit en informer sans délai son superviseur et le Responsable de la protection des Renseignements personnels à l'adresse [privacy@theratech.com](mailto:privacy@theratech.com).

**Obligations contractuelles.** À des fins d'assurance, Thera peut être soumise à des obligations contractuelles concernant la manière dont elle doit répondre à un Incident de confidentialité qui implique des Renseignements personnels d'un Individu, notamment, qui doit être avisé et comment l'avis doit être donné; ces exigences peuvent compléter la présente Politique ou y déroger. Dans certaines circonstances exceptionnelles, Thera n'informerait pas l'Individu concerné tant qu'elle n'aura pas déterminé avec la compagnie d'assurance si elle est soumise à des exigences spécifiques. Le Responsable de la protection des Renseignements personnels sera chargé de déterminer si de telles obligations contractuelles ou légales existent.

**Avis aux Individus et aux Autorités réglementaires.** Les exigences relatives aux avis à donner à une Autorité réglementaire ou aux Individus concernés seront déterminées par le Responsable de la protection des Renseignements personnels. Thera peut, de sa propre initiative, aviser les Individus ou les organisations concernés de tout Incident de confidentialité, en particulier lorsque la violation donne lieu à un risque réel de préjudice important pour les Individus ou les organisations concernés. Le Responsable de la protection des Renseignements personnels déterminera le contenu d'un tel avis.

**Tenu de registres.** Thera conservera un dossier de chaque Incident de confidentialité pendant au moins cinq (5) ans après toute violation.

## **11. DROITS DES INDIVIDUS**

Les Individus disposent de divers droits légaux en ce qui concerne leurs Renseignements personnels, tel que :

- Le droit d'accéder aux Renseignements personnels que Thera détient à leur sujet;
- Le droit de rectification, c'est-à-dire le droit de demander la correction, dans les meilleurs délais, de tous les Renseignements personnels que Thera détient à sujet et qui sont inexacts ou incomplets;
- Le droit de retirer son consentement au Traitement de ses Renseignements personnels; et

- En plus de ce qui précède, les Individus ont le droit de déposer une plainte auprès des Autorités réglementaires.

En vertu du RGPD, des droits supplémentaires sont accordés aux Individus dans certaines circonstances, tel que :

- Le droit d'obtenir l'effacement de leurs Renseignements personnels, sans retard injustifié, à condition que les Renseignements personnels ne soient plus nécessaires pour les Fins pour lesquelles ils ont été collectés;
- Le droit à la portabilité des données, selon lequel l'Individu a le droit de demander l'envoi de ses Renseignements personnels dans un format structuré, couramment utilisé et lisible par machine et de les recevoir;
- Le droit à la restriction, selon lequel un Individu est en droit de demander à Thera de suspendre le Traitement de certains Renseignements personnels le concernant, par exemple pour en établir l'exactitude ou la raison du Traitement; et
- Le droit d'opposition, selon lequel un Individu peut contester si Thera traite des Renseignements personnels sur la base d'un intérêt légitime (ou de ceux d'un tiers) ou à des Fins de marketing direct. Toutefois, dans certaines circonstances, Thera peut être autorisée à poursuivre le Traitement des Renseignements personnels.

En vertu de la *Loi sur le secteur privé du Québec* :

- Un Individu a le droit de demander la cessation de la diffusion de ses Renseignements personnels ou la désindexation de tout hyperlien rattaché à son nom et permettant l'accès aux Renseignements personnels de cet Individu lorsque la diffusion des Renseignements personnels contrevient à la loi ou à une ordonnance d'un tribunal. Les Individus peuvent également demander la désindexation lorsque la diffusion des Renseignements personnels leur cause un préjudice; et
- Le droit de contester toute décision fondée exclusivement sur un Traitement automatisé de leurs Renseignements personnels lorsque cette décision a un effet juridique ou un effet similaire significatif et de demander que la décision soit réexaminée.

Sur demande, les Employés doivent fournir aux Individus un moyen complet d'exercer l'un des droits susmentionnés ou de s'informer sur le Traitement de leurs Renseignements personnels par Thera.

## **PROTECTION DES MINEURS**

Il est possible que Thera recueille des Renseignements personnels auprès de mineurs. Aux fins des présentes, on entend par « **Mineurs** » les enfants âgés de moins de 16 ans pour les résidents de l'Union européenne ou de moins de 14 ans pour les résidents du Québec. Les Mineurs méritent une protection particulière, car ils peuvent être moins sensibilisés au sujet de leurs droits ou des risques liés au traitement de leurs Renseignements personnels.

Le consentement d'un Mineur doit être fourni par ses parents ou autres représentants légaux avant tout Traitement de Renseignements personnels. Dans la mesure du possible, un Mineur doit pouvoir participer à la décision d'autoriser le Traitement de ses Renseignements personnels. Si Thera apprend que des Renseignements personnels ont été recueillis directement auprès d'un Mineur sans le consentement vérifiable de ses parents, des mesures appropriées pour supprimer ces Renseignements personnels devront être prises.

Étant donné que les Mineurs méritent une protection particulière, toute communication relative au Traitement des Renseignements personnels d'un Mineur doit être rédigée dans un langage clair et simple, de sorte que le Mineur puisse facilement en comprendre les conséquences. La validité du consentement est inextricablement liée à la qualité des informations fournies sur les Fins du Traitement.

Sur demande, Thera doit permettre à un Mineur d'accéder à ses Renseignements personnels dans un format facilement lisible et autoriser la rectification et l'effacement.

Les Mineurs ont également le droit de demander l'accès, la rectification et l'effacement de leurs Renseignements personnels. Les Mineurs doivent être en mesure de retirer leur consentement de manière simple, sans conséquences négatives pour l'utilisation des services ou des produits de Thera.

## **12. FORMATION**

Lors de son arrivée chez Thera, chaque nouvel Employé doit suivre une formation de sensibilisation à la cybersécurité et une formation obligatoire est dispensée à chaque Employé sur l'importance de préserver la confidentialité des Renseignements personnels.

## **13. NOUS CONTACTER**

### **13.1 Coordonnées**

Tous les commentaires, questions, préoccupations concernant les Renseignements personnels ou nos pratiques en matière de protection de la vie privée doivent être envoyés au Responsable de la protection des Renseignements personnels de Thera comme suit :

Adresse : À l'attention du : Responsable de la protection des Renseignements personnels & Délégué à la protection des données  
Jocelyn Lafond  
Conseiller juridique principal et secrétaire corporatif, agissant à titre de Responsable de la protection des Renseignements personnels & Délégué à la protection des données  
Theratechnologies Inc.  
2015 rue Peel, 11<sup>e</sup> étage  
Montréal, Québec  
Canada H3A 1T8

Par courriel : [privacy@theratech.com](mailto:privacy@theratech.com)

### **13.2 Plaintes**

Le Responsable de la protection des Renseignements personnels mènera une enquête indépendante sur toutes les plaintes et allégations de violation de la présente Politique.

Le Responsable de la protection des Renseignements personnels devra :

- Clarifier les plaintes afin d'identifier la source des problèmes;
- Si nécessaire, communiquer avec le plaignant pour recueillir des preuves suffisantes;
- Procéder à une analyse des informations obtenues au cours de l'enquête; et
- Déterminer la meilleure approche pour traiter la question et si des mesures correctives sont nécessaires.

Toute personne qui enfreint la présente Politique fera l'objet d'une action disciplinaire.

## **14. APPLICATION ET RÉVISION DE LA PRÉSENTE POLITIQUE**

Thera peut, de temps à autre, apporter des modifications à la présente Politique pour tenir compte des changements apportés à ses obligations légales ou réglementaires ou à la manière dont elle traite les Renseignements personnels.

La présente Politique entre en vigueur le 20 septembre 2023. Aucune partie de la présente Politique n'a d'effet rétroactif et ne s'applique donc qu'aux faits survenus à cette date ou ultérieurement.

La présente Politique a été approuvée et autorisée par :

**Nom :** Jocelyn Lafond  
**Fonction :** Conseiller juridique principal et secrétaire corporatif, agissant à titre de Responsable de la protection des Renseignements personnels & Délégué à la protection des données  
**À réviser d'ici le :** 20 septembre 2025

Historique de révision

<b>Version</b>	<b>Date d'entrée en vigueur</b>	<b>Auteur</b>	<b>Résumé des modifications</b>
01	20-Sept 2023	Responsable de la protection des Renseignements personnels / Délégué à la protection des données	