LOI 25

Entrée en vigueur : 1 septembre 2024
Révision : 9 mai 2025

Politique de protection des renseignements personnels de SECURIMED
Conformément à la Loi 25 sur la protection des renseignements personnels dans le secteur privé

Introduction

Chez SECURIMED, la protection de vos renseignements personnels est une priorité. Nous nous engageons à respecter votre vie privée et à veiller à la sécurité de vos données personnelles conformément à la Loi 25 du Québec, relative à la protection des renseignements personnels dans le secteur privé. Cette politique a pour but de vous informer sur les types de renseignements que nous recueillons, la façon dont nous les utilisons, les mesures de sécurité mises en place et vos droits en matière de confidentialité.

---

1. Définitions

- **Renseignements personnels** : Toute information qui permet d'identifier une personne physique, qu'elle soit directement ou indirectement liée à cette personne. Par exemple : nom, adresse, numéro de téléphone, adresse électronique, données de santé, etc.
- **Traitement des renseignements personnels** : L'ensemble des opérations effectuées sur les renseignements personnels, telles que la collecte, l'utilisation, la conservation, la communication, ou encore la destruction.

---

2. Collecte des renseignements personnels

SECURIMED collecte des renseignements personnels dans le cadre de ses activités commerciales, notamment lors de la fourniture de services médicaux.

Les types de renseignements personnels que nous pouvons recueillir incluent, sans s'y limiter :

- Identifiants personnels (nom, prénom, adresse, numéro de téléphone, adresse courriel, RAMQ, numéro de CNESST date de naissance).
- Informations financières (mode de paiement, historique des transactions).

- Données de santé et de sécurité (données médicales, antécédents de sécurité, etc.).
- Autres informations relatives à la gestion de vos services.

La collecte de vos données est faite uniquement lorsque cela est nécessaire pour accomplir les fins précisées dans le cadre de notre relation avec vous.

---

3. Utilisation des renseignements personnels

Les renseignements personnels que nous recueillons sont utilisés dans les objectifs suivants :

- Fournir les services médicaux qui nous ont été demandés.
- Assurer le bon fonctionnement de nos services et répondre à vos demandes.
- Maintenir un contact avec vous pour la gestion de votre dossier médical, la facturation, et la mise à jour de nos services.
- Respecter nos obligations légales et contractuelles.

Nous ne vendons, ni ne louons, vos renseignements personnels à des tiers. Toutefois, nous pouvons partager des renseignements à la suite de votre consentement afin de pouvoir vous offrir des services de santé.

- Avec des professionnels de la santé
- Lorsque cela est exigé par la loi ou pour protéger nos droits et intérêts légaux.

---

4. Conservation des renseignements personnels

Les renseignements personnels sont conservés pendant la durée nécessaire pour que les médecins et/ou infirmier soient conformes à la règlementation de leur ordre professionnel. Nous prendrons les mesures nécessaires pour les protéger contre la perte, l'accès non autorisé, la divulgation ou l'altération.

Nous appliquons des périodes de conservation des données en fonction des exigences légales conformément à la règlementation des professionnels de la santé. Dès que les renseignements personnels ne sont plus nécessaires, ils seront détruits de manière sécurisée.

5. Sécurisation des renseignements personnels

SECURIMED met en place des mesures physiques, techniques et organisationnelles afin de protéger vos renseignements personnels contre la perte, le vol, l'accès non autorisé, la divulgation, la copie, l'altération et la destruction. Cela inclut :

- L'utilisation d'un DME autorisé par le MSSS du Québec pour les patients utilisant des traitements.
- L'utilisation de systèmes de sécurité informatique de pointe pour les services aux entreprises et pour les services de rapport médical.
- La formation continue de nos employés concernant la gestion et la protection des données personnelles.
- L'accès aux données limité aux seules personnes autorisées à les consulter en raison de leurs fonctions.

---

6. Vos droits concernant vos renseignements personnels

Conformément à la Loi 25, vous avez plusieurs droits relatifs à vos renseignements personnels :

- **Droit d'accès** :
    - Patient : Vous pouvez demander l'accès à vos renseignements personnels que nous détenons.
    - Client : Vous devez demander votre dossier médical à l'entreprise qui nous a mandaté pour faire votre évaluation médicale.
    - Immigrant : Vous pouvez demander votre sommaire de dossier standardisé produit via l'application eMedical de IRCC.
- **Droit de rectification** :
    - Patient et Client : Vous pouvez demander la correction de toute information incorrecte ou incomplète que nous détenons à votre sujet.
    - Immigrant : Vous devez faire la demande de modification d'information non médical directement à l'IRCC. Pour l'évaluation

médicale seulement, vous pouvez demander la correction de l'information incorrecte ou incomplète que nous détenons à votre sujet.

- **Droit à l'effacement** : Dans certains cas administratifs, vous pouvez demander la suppression de vos renseignements personnels provenant de votre déclaration.
- **Droit de limitation du traitement** : Vous pouvez demander que nous limitions l'utilisation de vos données dans certaines circonstances.
- **Droit de portabilité** : Vous pouvez demander la transmission de vos renseignements personnels dans un format structuré, couramment utilisé et lisible par machine.

Pour exercer vos droits, vous pouvez nous contacter à l'adresse suivante : LD@secrimed.ca

---

7. Responsabilité et contact

SECURIMED est responsable de la gestion des renseignements personnels qu'elle collecte et traite. En cas de questions ou préoccupations concernant cette politique ou le traitement de vos données, veuillez nous contacter par courriel à l'adresse LD@securimed.ca ou par téléphone au 514 521-1223, Louise-Danièle Duquette

---

8. Modifications de la politique

Cette politique peut être modifiée à tout moment pour refléter les évolutions légales, réglementaires ou de nos pratiques commerciales. Les modifications seront communiquées à nos clients de manière appropriée, et la version mise à jour sera disponible sur notre site web.

Conclusion

Chez SECURIMED, nous considérons la confidentialité et la sécurité de vos renseignements personnels comme une priorité essentielle. Nous nous engageons à respecter la Loi 25 et à prendre toutes les mesures nécessaires pour protéger vos données dans le cadre de nos activités.

Procédure de gestion des demandes d'accès et de rectification

Conformément à la Loi 25 sur la protection des renseignements personnels dans le secteur privé

Objectif

La présente procédure a pour but de définir les étapes à suivre pour la gestion des demandes d'accès et de rectification des renseignements personnels conformément à la Loi 25. SECURIMED s'engage à répondre à ces demandes de manière efficace et conforme à la législation en vigueur, tout en garantissant la confidentialité et la sécurité des données personnelles de ses clients, employés et partenaires.

---

1. Demande d'accès

Une personne a le droit de demander à SECURIMED l'accès aux renseignements personnels que nous détenons à son sujet. Selon le type de service SECURIMED indiquera qui est le bon intervenant pour faire la demande d'accès car SECURIMED n'est pas propriétaire de l'information. Cette demande doit être formulée par écrit et peut être adressée au responsable de la protection des renseignements personnels (RPR) de l'entreprise.

1.1 Étapes de la procédure

1. **Réception de la demande** :
   Toute demande d'accès doit être soumise par écrit (courriel) au responsable de la protection des renseignements personnels. La demande doit indiquer clairement les renseignements pour lesquels l'accès est demandé, ainsi que l'identité du demandeur.

2. **Identification et vérification de l'identité** :
   Afin de protéger la confidentialité des informations personnelles, SECURIMED vérifiera l'identité du demandeur avant de fournir la procédure à suivre pour l'obtention des informations. Selon le cas, il pourra être demandé des documents supplémentaires pour confirmer l'identité du demandeur.

3. **Évaluation de la demande** :
   Le responsable de la protection des renseignements personnels (RPR) évaluera la demande en fonction des critères suivants :
   - Vérification si les renseignements demandés sont en notre possession.
   - Vérification qui est le propriétaire de l'information (Entreprise, médecin, expert, etc)
   - Si des exemptions légales s'appliquent (par exemple, données protégées par le secret professionnel, informations exclusses par la loi).
   - Identification dans quel processus se trouve le demandeur :
     1. Patient : L'information inscrit au DME sera transmise dans les 30 jours directement au patient en conformité avec les règles du collège des médecins.
     2. Client : Aucune information ne sera transmise, car celle-ci appartient au demandeur. Le client devra effectuer sa demande auprès de se demandeur afin d'obtenir l'information. SECURIMED acheminera l'information au demandeur auprès duquel il pourra récupérer l'information.
     3. Immigrant : En conformité avec la règlementation de IRCC, l'immigrant doit payer les frais d'administration pour la transmission du sommaire provenant du eMedical qui lui sera transmise dans les 30 jours.
4. **Réponse à la demande** :
   Si l'accès est accordé, SECURIMED fournira une copie des renseignements demandés, sous un format structuré et lisible. Si l'accès est refusé, une explication sera donnée sur les raisons de ce refus (conformément à la Loi 25).
5. **Notification** :
   En cas de refus ou de limitation d'accès, SECURIMED notifie la personne des raisons spécifiques du refus. Si la demande est acceptée, la copie des renseignements personnels est transmise selon le processus.

2. Demande de rectification

Une personne peut également demander la rectification de renseignements personnels inexacts, incomplets ou obsolètes en notre possession qui nous a été déclaré par la personne elle même.

2.1 Étapes de la procédure

1. **Réception de la demande** :
   Toute demande de rectification doit être soumise par écrit au responsable de la protection des renseignements personnels, en précisant les renseignements concernés et la nature de la rectification demandée.
2. **Identification et vérification de l'identité** :
   Comme pour une demande d'accès, l'identification du demandeur est essentielle pour garantir la sécurité des informations personnelles. Nous demanderons des informations suffisantes pour confirmer l'identité du demandeur.
3. **Évaluation de la demande** :
   Le responsable de la protection des renseignements personnels procédera à une vérification des renseignements en question. Si les informations sont erronées ou incomplètes, SECURIMED procédera à leur mise à jour dans les plus brefs délais.
4. **Mise à jour des renseignements** :
   Si la demande de rectification est justifiée, nous apporterons les modifications nécessaires et nous veillerons à ce que les informations corrigées soient mises à jour dans tous les systèmes pertinents.
5. **Notification à la personne concernée** :
   Le demandeur sera informé des actions entreprises concernant sa demande de rectification. Si la demande est refusée, une explication détaillée des motifs du refus sera fournie.
6. **Communication aux tiers** :
   Si les renseignements rectifiés ont été communiqués à des tiers, SECURIMED prendra des mesures raisonnables pour les informer de la rectification, à moins que cela ne soit impossible ou ne présente une charge disproportionnée.

3. Délais de traitement des demandes

- **Accès** :
  En vertu de la Loi 25, SECURIMED doit répondre à toute demande d'accès dans un délai maximal de **30 jours** suivant la réception de la demande. Si la demande est complexe ou nécessite plus de temps, nous informerons le demandeur des raisons du retard et indiquerons un nouveau délai raisonnable.
- **Rectification** :
  Les demandes de rectification seront traitées dans un délai raisonnable, idéalement dans les **30 jours** suivant la réception de la demande. Si des informations supplémentaires sont nécessaires, nous en informerons le demandeur.

---

4. Refus de la demande

SECURIMED se réserve le droit de refuser une demande d'accès ou de rectification si elle ne respecte pas les critères légaux ou si des exemptions légales s'appliquent. Les raisons du refus seront communiquées au demandeur, et celui-ci pourra avoir recours à d'autres recours prévus par la loi.

Les motifs de refus peuvent inclure, sans s'y limiter :

- Les informations demandées sont exemptées de divulgation selon la Loi 25 (par exemple, données qui ne peuvent être partagées en raison du secret professionnel, de la sécurité nationale, etc.).
- La demande est jugée excessive, abusive ou mal formulée.
- La demande ne doit pas être adressé à SECURIMED.
- La demande est déjà régit par une règlementation avec un processus déterminé, tel que l'immigration.

---

5. Recours en cas de refus

Si une personne estime que sa demande d'accès ou de rectification a été indûment refusée, elle peut :

- Demander une révision de la décision par le responsable de la protection des renseignements personnels.
- Faire une plainte auprès de la Commission d'accès à l'information du Québec, qui pourra évaluer la légalité du refus.

---

6. Responsable de la protection des renseignements personnels (RPR)

Le responsable de la protection des renseignements personnels chez SECURIMED est la personne désignée pour recevoir, évaluer et traiter les demandes d'accès et de rectification. Le RPR est également chargé de veiller à ce que les demandes soient traitées conformément à la législation en vigueur et de coordonner avec les autorités compétentes en cas de plainte ou de litige.

Vous pouvez contacter le responsable de la protection des renseignements personnels à l'adresse suivante :

- **Courriel** : LD@SECURIMED.CA
- **Numéro de téléphone** : 514 521-1223

---

7. Formation et sensibilisation

SECURIMED met en place des programmes de formation réguliers pour ses employés afin de garantir que la procédure de gestion des demandes d'accès et de rectification est bien comprise et correctement appliquée. Les employés responsables du traitement des demandes doivent être formés aux exigences légales liées à la protection des renseignements personnels.

Conclusion

SECURIMED s'engage à respecter vos droits relatifs à l'accès et à la rectification de vos renseignements personnels. Nous mettons en œuvre des mesures rigoureuses pour traiter toutes les demandes dans les délais légaux et avec transparence, conformément à la Loi 25.

Registre des incidents de confidentialité (violations de la confidentialité)

Conformément à la Loi 25 sur la protection des renseignements personnels dans le secteur privé

Introduction

Le présent registre a pour objectif de consigner et de suivre toutes les violations de la confidentialité des renseignements personnels (également appelées incidents de confidentialité) qui surviennent au sein de SECURIMED, conformément aux exigences de la Loi 25 sur la protection des renseignements personnels dans le secteur privé. Ce registre vise à assurer une gestion rigoureuse des incidents, à faciliter la notification auprès des autorités compétentes et des personnes concernées, et à améliorer continuellement nos pratiques de sécurité des données.

---

1. Définition d'un incident de confidentialité

Un incident de confidentialité est toute situation où il y a un accès non autorisé, une divulgation, une perte ou un vol de renseignements personnels, ou toute autre forme de violation de la sécurité des données personnelles. Cela inclut, sans s'y limiter :

- L'accès non autorisé à des fichiers contenant des renseignements personnels.
- La perte ou le vol d'un appareil ou d'un document contenant des renseignements personnels.
- La divulgation accidentelle ou malveillante de renseignements personnels.
- Des erreurs dans la gestion ou le stockage des données ayant entraîné des risques pour la confidentialité.

---

2. Gestion des incidents de confidentialité

2.1 Signalement d'un incident de confidentialité

Tout membre du personnel de SECURIMED ayant connaissance d'un incident de confidentialité est tenu de le signaler immédiatement au responsable de la protection des renseignements personnels (RPR) ou à l'équipe responsable de la sécurité des données.

- Le signalement doit être effectué dès que possible après la découverte de l'incident, en précisant les éléments suivants :
    - Nature de l'incident (vol, perte, accès non autorisé, etc.).
    - Date, heure et lieu de l'incident.
    - Type de renseignements personnels impliqués (par exemple, nom, adresse, numéro de sécurité sociale, données de santé).
    - Description des circonstances et des causes de l'incident, dans la mesure du possible.

2.2 Évaluation de l'incident

Une fois l'incident signalé, le responsable de la protection des renseignements personnels (RPR) procède à une évaluation préliminaire de l'incident pour déterminer :

- Si les renseignements personnels ont été effectivement compromis.
- La nature et la gravité de l'incident (s'il s'agit d'un incident isolé ou si plusieurs personnes sont touchées).
- Les risques pour les personnes concernées (ex : risque d'usurpation d'identité, préjudice financier, atteinte à la réputation).
- Si une notification à la Commission d'accès à l'information du Québec et/ou aux personnes concernées est nécessaire.

---

3. Contenu du registre des incidents de confidentialité

Le registre des incidents de confidentialité doit consigner tous les incidents de confidentialité survenus, et ce, même ceux qui ont été résolus sans nécessiter de notification externe. Le registre contient, pour chaque incident :

- **Identifiant de l'incident** : Un numéro unique permettant de référencer l'incident.
- **Date et heure de l'incident** : Moment où l'incident a été constaté ou signalé.
- **Nature de l'incident** : Description détaillée de l'incident (ex. : vol de matériel, divulgation accidentelle de données, accès non autorisé).

- **Type de renseignements affectés** : Les catégories de données personnelles concernées (ex. : informations personnelles, données médicales, données financières).
- **Gravité de l'incident** : Une évaluation du risque pour les personnes concernées (ex. : faible, moyen, élevé).
- **Mesures prises** : Les actions entreprises pour limiter les effets de l'incident, telles que la réinitialisation des mots de passe, la notification interne, la sécurisation des données compromises, etc.
- **Notification** : Indication si la Commission d'accès à l'information a été notifiée, et le cas échéant, la date et les détails de la notification. De même, mention de toute notification faite aux personnes concernées.
- **Personnes responsables** : Noms des personnes responsables de la gestion et du suivi de l'incident, y compris le RPR et toute autre personne impliquée dans la gestion de la situation.
- **Mesures correctives** : Description des mesures de prévention mises en place pour éviter qu'un incident similaire ne se reproduise (amélioration des processus, formation du personnel, révision des pratiques de sécurité, etc.).
- **Statut de l'incident** : Indication de l'état de l'incident (en cours, résolu, suivi nécessaire, etc.).

---

4. Notification des incidents de confidentialité

Conformément à la Loi 25, SECURIMED doit notifier à la **Commission d'accès à l'information du Québec** tout incident de confidentialité susceptible de constituer un risque sérieux pour la confidentialité des renseignements personnels.

- **Délai de notification** : La notification à la Commission doit être effectuée **dans les 72 heures** suivant la découverte de l'incident.
- **Contenu de la notification** :
    - Une description détaillée de l'incident.
    - Le nombre estimé de personnes touchées.
    - Une description des mesures prises pour remédier à la situation.

- Une évaluation des risques pour les personnes concernées.

Si l'incident présente un risque élevé pour la personne concernée, SECURIMED doit également notifier directement les individus affectés par l'incident, en expliquant la nature de l'incident et les mesures prises pour les protéger.

---

5. Mesures correctives et prévention

Après chaque incident, SECURIMED met en place des **mesures correctives** pour éviter que des incidents similaires ne se reproduisent. Cela peut inclure :

- Des actions immédiates pour sécuriser les informations compromises (ex. : verrouillage des accès, retrait des appareils volés, etc.).
- La mise en œuvre de **mesures de prévention** à long terme, telles que :
  - La révision et la mise à jour des politiques de sécurité des données.
  - Des formations et sensibilisations régulières pour le personnel sur la gestion des données personnelles.
  - L'amélioration des contrôles d'accès et des protocoles de sécurité informatique.

Chaque incident est l'occasion d'améliorer les pratiques internes en matière de sécurité des renseignements personnels, afin de réduire les risques de violation à l'avenir.

---

6. Accès et consultation du registre des incidents

Le **registre des incidents de confidentialité** est un document interne tenu à jour et consultable uniquement par les personnes habilitées, telles que le responsable de la protection des renseignements personnels et les membres de la direction de SECURIMED. Ce registre est un outil précieux pour l'analyse des tendances et la gestion proactive des risques en matière de sécurité des données.

---

7. Confidentialité et sécurité du registre

Le registre des incidents de confidentialité est conservé dans un environnement sécurisé et ne doit être accessible qu'aux personnes ayant un besoin légitime d'y

accéder. Les informations concernant les incidents doivent être manipulées avec le plus grand soin afin de garantir la confidentialité et la sécurité des données.

Conclusion

SECURIMED prend très au sérieux la protection des renseignements personnels. Grâce à ce registre et à la gestion rigoureuse des incidents de confidentialité, nous nous engageons à respecter les obligations de la Loi 25 et à protéger les droits de nos clients, employés et partenaires. Nous mettons en œuvre des pratiques et des mesures de sécurité afin de minimiser les risques et d'améliorer en continu nos processus de gestion des incidents.

Formulaire de consentement à la collecte, à l'utilisation et à la divulgation des renseignements personnels

Conformément à la Loi 25 sur la protection des renseignements personnels dans le secteur privé

1. Introduction

Chez **SECURIMED**, la protection de vos renseignements personnels est une priorité. Conformément à la Loi 25, nous vous demandons votre consentement éclairé avant de collecter, d'utiliser ou de divulguer vos renseignements personnels. Ce formulaire vous fournit les informations nécessaires pour comprendre pourquoi et comment vos données seront utilisées, ainsi que vos droits en matière de confidentialité.

---

2. Identification de l'entreprise

Nom de l'entreprise : SECURIMED
Adresse : 110-35, Rue Port-Royal Est, Montréal (Québec) H3L 3T1
Téléphone : 514 521-1223
Courriel : LD@SECURIMED.CA
Responsable de la protection des renseignements personnels : LOUISE-DANIÈLE DUQUETTE, PRÉSIDENTE

---

3. Objectifs de la collecte et de l'utilisation des renseignements personnels

Les renseignements personnels que vous nous fournissez peuvent être utilisés aux fins suivantes :

- Fournir les services médicaux.
- Gérer votre relation avec SECURIMED, y compris la facturation, les communications, la gestion des contrats, etc.
- Respecter les obligations légales et réglementaires auxquelles SECURIMED est soumise.
- Vous offrir un service personnalisé et adapté à vos besoins.

Les types de renseignements que nous collectons peuvent inclure, sans s'y limiter :

- Identifiants personnels (nom, adresse, courriel, numéro de téléphone, RAMQ, numéro CNESST, etc.).
- Données financières (informations bancaires, historiques de paiement).
- Données médicales (si nécessaire pour la prestation de services).
- Autres informations relatives à nos services ou à votre sécurité.

---

4. Consentement à la collecte, à l'utilisation et à la divulgation

En signant ce formulaire, vous consentez expressément à ce que SECURIMED recueille, utilise et divulgue vos renseignements personnels aux fins mentionnées ci-dessus. Vous comprenez également que ce consentement est requis pour la prestation de certains services et que vous pouvez retirer votre consentement à tout moment, sous réserve des restrictions légales et contractuelles.

Voir un exemple du consentement Annex 1

---

5. Durée de conservation des renseignements personnels

SECURIMED conservera vos renseignements personnels uniquement pendant la période nécessaire pour atteindre les objectifs pour lesquels ils ont été collectés, et conformément aux exigences légales applicables. Une fois cette période écoulée, vos renseignements personnels seront supprimés ou anonymisés de manière sécurisée.

---

6. Droit de retrait du consentement et droits des personnes concernées

Vous avez le droit de retirer votre consentement à tout moment. Toutefois, ce retrait pourrait affecter la capacité de SECURIMED à fournir certains services. Si vous souhaitez retirer votre consentement ou si vous avez des questions concernant l'utilisation de vos renseignements personnels, veuillez contacter notre responsable de la protection des renseignements personnels à l'adresse suivante : LD@securimed.ca

Vous avez également les droits suivants concernant vos renseignements personnels :

- **Droit d'accès** :
    - Patient : Vous pouvez demander l'accès à vos renseignements personnels que nous détenons.
    - Client : Vous devez demander votre dossier médical à l'entreprise qui nous a mandaté pour faire votre évaluation médicale.
    - Immigrant : Vous pouvez demander votre sommaire de dossier standardisé produit via l'application eMedical de IRCC.
- **Droit de rectification** :
    - Patient et Client : Vous pouvez demander la correction de toute information incorrecte ou incomplète que nous détenons à votre sujet.
    - Immigrant : Vous devez faire la demande de modification d'information non médical directement à l'IRCC. Pour l'évaluation médicale seulement, vous pouvez demander la correction de l'information incorrecte ou incomplète que nous détenons à votre sujet.
- **Droit à l'effacement** : Dans certains cas administratifs, vous pouvez demander la suppression de vos renseignements personnels provenant de votre déclaration.
- **Droit de limitation du traitement** : Vous pouvez demander que nous limitions l'utilisation de vos données dans certaines circonstances.
- **Droit de portabilité** : Vous pouvez demander la transmission de vos renseignements personnels dans un format structuré, couramment utilisé et lisible par machine.

Pour exercer vos droits, veuillez contacter le responsable de la protection des renseignements personnels à l'adresse courriel suivante : LD@securimed.ca

---

7. Mesures de sécurité

SECURIMED met en œuvre des mesures de sécurité physiques, administratives et techniques appropriées pour protéger vos renseignements personnels contre la perte, l'accès non autorisé, la divulgation, la modification et la destruction. Nous nous engageons à maintenir un environnement sécurisé pour garantir la confidentialité de vos données.

---

8. Consentement éclairé

En signant ce formulaire, vous reconnaissez avoir lu et compris les informations ci-dessus concernant la collecte, l'utilisation, la conservation et la divulgation de vos renseignements personnels. Vous consentez également à ce que SECURIMED collecte, utilise et divulgue vos renseignements personnels selon les modalités décrites dans ce formulaire.

---

9. Signature du consentement

- Voir Annexe 1

---

10. Pour toute question ou préoccupation

Si vous avez des questions concernant ce formulaire ou la gestion de vos renseignements personnels, n'hésitez pas à nous contacter :

- **Responsable de la protection des renseignements personnels**
  LOUISE-DANIELE DUQUETTE, PRÉSIDENTE
  Courriel : LD@SECURIMED.CA
  Téléphone : 514 521-1223

Plan de formation du personnel

Conformément à la Loi 25 sur la protection des renseignements personnels dans le secteur privé

Introduction

Le respect de la **Loi 25** sur la protection des renseignements personnels dans le secteur privé est une priorité pour **SECURIMED**. Afin de garantir la conformité aux exigences légales et de protéger les renseignements personnels de nos clients, employés et partenaires, nous avons mis en place un **Plan de formation du personnel**. Ce plan vise à sensibiliser et à former nos employés à la gestion sécurisée des renseignements personnels, ainsi qu'à leur fournir les outils et connaissances nécessaires pour protéger ces informations.

---

1. Objectifs du plan de formation

Les objectifs de ce plan sont les suivants :

- **Assurer la conformité** avec la **Loi 25** et toutes les législations pertinentes relatives à la protection des renseignements personnels.
- **Sensibiliser les employés** à l'importance de la confidentialité et de la sécurité des renseignements personnels.
- **Former les employés** aux meilleures pratiques pour la collecte, l'utilisation, la conservation et la divulgation des renseignements personnels.
- **Éviter les violations de la confidentialité** en renforçant la vigilance et la rigueur dans la gestion des données.
- **Encourager une culture de la sécurité** des données au sein de l'entreprise, en impliquant tous les niveaux hiérarchiques.

---

2. Public cible

Le plan de formation s'applique à tous les employés, sous-traitants, consultants et toute personne ayant accès à des renseignements personnels au sein de

SECURIMED. La formation est adaptée en fonction des responsabilités et des accès aux données de chaque groupe.

- **Nouveaux employés** : Signature du contrat de respect de la confidentialité est obligatoire à leur entrée en fonction.
- **Employés en contact direct avec des données personnelles** : Formation approfondie sur la gestion des renseignements personnels.
- **Cadres supérieurs et responsables de la sécurité des données** : Formation sur les obligations légales et la supervision de la conformité.
- **Sous-traitants et partenaires** : Sensibilisation aux principes de base de la confidentialité et de la sécurité des données.

---

3. Contenu de la formation

La formation sur la protection des renseignements personnels sera divisée en plusieurs modules adaptés aux différents groupes cibles.

Module 1 : Introduction à la protection des renseignements personnels

- **Objectifs** : Présenter les bases de la confidentialité et des droits des individus en vertu de la Loi 25.
- **Contenu** :
    - Les principes de la protection des renseignements personnels.
    - Les droits des personnes concernées (droit d'accès, de rectification, d'effacement, etc.).
    - Les responsabilités de l'entreprise et des employés en matière de protection des données.
    - Notions de collecte, d'utilisation, de conservation et de divulgation des données.
    - La réglementation canadienne (Loi 25, Loi sur la protection des renseignements personnels et les documents électroniques, etc.).

Module 2 : Pratiques sécuritaires pour la gestion des renseignements personnels

- **Objectifs** : Former les employés à appliquer des pratiques sécuritaires dans la gestion quotidienne des données personnelles.
- **Contenu** :
    - Comment sécuriser les données (mots de passe, cryptage, sécurisation des documents).
    - Les risques de sécurité liés aux accès non autorisés, au vol ou à la divulgation accidentelle.
    - Sensibilisation aux incidents de confidentialité et à la manière de les signaler.
    - Utilisation sécuritaire des technologies de communication (emails, smartphones, ordinateurs portables).
    - Gestion des documents papier et électroniques.

Module 3 : Gestion des demandes d'accès, de rectification et de suppression

- **Objectifs** : Sensibiliser les employés aux droits des individus concernant leurs données et aux processus à suivre.
- **Contenu** :
    - Le processus de gestion des demandes d'accès et de rectification des renseignements personnels.
    - Les délais légaux et les obligations de l'entreprise.
    - Comment répondre à une demande de suppression de données personnelles.
    - Les procédures de suivi et de documentation des demandes.

Module 4 : La notification des violations de la confidentialité

- **Objectifs** : Former les employés à reconnaître une violation de la confidentialité et à agir rapidement.
- **Contenu** :
    - Identification des violations de la confidentialité (vol, perte, accès non autorisé).

- Processus de notification interne et externe (Commission d'accès à l'information, personnes concernées).
- Mesures de remédiation immédiates et à long terme.
- Rôle de chaque employé dans la gestion des incidents de confidentialité.

Module 5 : Sensibilisation continue et mise à jour des pratiques

- **Objectifs** : Mettre en place une culture de la sécurité des renseignements personnels et assurer une veille continue.
- **Contenu** :
  - L'importance de la formation continue en matière de protection des données.
  - Actualisation des connaissances sur les évolutions législatives et les risques liés à la cybersécurité.
  - Encourager la vigilance et l'implication active de chaque employé.

---

4. Méthodes de formation

Les formations seront dispensées à l'aide de plusieurs méthodes pédagogiques pour garantir leur efficacité et leur accessibilité :

- **Formation en ligne** : Modules interactifs accessibles via une plateforme de gestion de l'apprentissage (LMS), permettant aux employés de suivre la formation à leur rythme.
- **Sessions en présentiel** : Séances de formation animées par des experts en protection des données, adaptées aux groupes cibles (notamment pour les cadres et les responsables de la sécurité).
- **Ateliers pratiques** : Séances interactives pour simuler des situations réelles de gestion des renseignements personnels et d'incidents de confidentialité.
- **Documentation et guides** : Fourniture de ressources écrites (manuel de l'employé, guides pratiques) pour renforcer les connaissances acquises et offrir un soutien continu.

---

5. Fréquence et suivi des formations

- **Formation initiale** : Chaque nouvel employé doit suivre la formation dans les 30 jours suivant son embauche.
- **Formation continue** : Des sessions de recyclage seront organisées annuellement pour tous les employés afin de maintenir la conformité aux nouvelles exigences légales et aux évolutions de la protection des données.
- **Formations spécifiques** : Pour les employés en contact direct avec des renseignements sensibles ou les responsables de la sécurité des données, des formations supplémentaires peuvent être nécessaires.

Suivi et évaluation :

- Chaque participant devra passer un test à la fin de chaque module pour évaluer sa compréhension des concepts clés.
- Un rapport annuel sera produit pour suivre l'évolution de la formation et identifier les besoins en formation supplémentaire.

---

6. Responsabilités et rôle des managers

Les managers et responsables de département ont un rôle clé dans la mise en œuvre du plan de formation :

- **Encourager la participation active** de leur équipe à la formation.
- **Suivre l'assiduité** et l'engagement de leurs employés dans le programme de formation.
- **Soutenir** les employés dans l'application des bonnes pratiques en matière de protection des renseignements personnels.
- **Évaluer** régulièrement les connaissances et compétences de leurs équipes pour assurer une culture de sécurité constante.

---

7. Évaluation de la conformité et amélioration continue

SECURIMED effectuera une évaluation annuelle de l'efficacité du programme de formation pour s'assurer qu'il répond aux exigences légales et aux besoins de l'entreprise. Cette évaluation prendra en compte :

- Le taux de participation des employés aux formations.
- Les résultats des tests de formation.
- Les retours d'expérience des employés sur la clarté et la pertinence des formations.
- Le nombre d'incidents de confidentialité et de violations de la sécurité des données.

Des ajustements seront apportés au programme de formation en fonction des résultats de l'évaluation et des évolutions législatives ou organisationnelles.

---

8. Conclusion

Chez **SECURIMED**, nous sommes pleinement engagés à protéger les renseignements personnels et à respecter la **Loi 25**. Ce plan de formation est essentiel pour assurer une gestion rigoureuse et conforme des données personnelles et pour cultiver une culture de la sécurité au sein de l'entreprise.

Procédure de notification des violations de données à la Commission d'accès à l'information (CAI)

Conformément à la Loi 25 sur la protection des renseignements personnels dans le secteur privé

Introduction

En vertu de la **Loi 25** sur la protection des renseignements personnels dans le secteur privé, **SECURIMED** s'engage à respecter les obligations légales en matière de protection des renseignements personnels. Cette procédure a pour but de décrire les étapes à suivre pour notifier une violation de données personnelles à la **Commission d'accès à l'information (CAI)**, conformément aux exigences de la loi.

---

1. Objectifs de la procédure

Les objectifs de cette procédure sont les suivants :

- Garantir une réponse rapide et efficace en cas de violation des données personnelles.
- Assurer la conformité avec les exigences légales en matière de notification à la CAI.
- Protéger les droits et la sécurité des personnes concernées par la violation des données.
- Mettre en œuvre des mesures correctives afin de minimiser l'impact de l'incident.

---

2. Définition d'une violation de données

Une **violation de données personnelles** est un événement où des renseignements personnels sont accidentellement ou illégalement divulgués, modifiés, perdus, ou consultés par une personne non autorisée. Cela inclut, mais ne se limite pas à :

- L'accès non autorisé à des bases de données contenant des renseignements personnels.

- La perte, le vol ou la divulgation accidentelle d'appareils contenant des renseignements personnels (ex. : ordinateurs, smartphones, documents papier).
- La modification ou l'altération non autorisée de renseignements personnels.
- L'envoi erroné ou non sécurisé de renseignements personnels à des destinataires non autorisés.

---

3. Identification d'une violation de données

Lorsqu'un incident de violation de données survient ou est suspecté, l'employé ou la personne ayant connaissance de l'incident doit immédiatement signaler cet incident au **Responsable de la protection des renseignements personnels (RPR)** ou au responsable de la sécurité des données.

Le processus de signalement comprend :

- **Description complète de l'incident** : nature, circonstances, et personnes impliquées.
- **Type de données concernées** : quelles informations personnelles ont été affectées.
- **Impact potentiel** sur les personnes concernées (ex. : risques d'usurpation d'identité, vol de données sensibles, etc.).

---

4. Évaluation de la violation de données

Une fois l'incident signalé, le **Responsable de la protection des renseignements personnels (RPR)**, en collaboration avec l'équipe de sécurité informatique et d'autres parties concernées, procède à une évaluation complète de l'incident. Cette évaluation vise à déterminer :

- **La gravité de l'incident** : Quelle est l'étendue de la violation ? Quel est le nombre de personnes touchées ?
- **Le type de données impliquées** : Quelles catégories de données personnelles ont été compromises (ex. : informations de santé, informations financières, identifiants personnels) ?

- **Les risques pour les personnes concernées** : Existence d'un risque de préjudice important pour les individus touchés par la violation (ex. : risques financiers, psychologiques, réputationnels).
- **Les actions correctives immédiates** prises pour contenir la violation (ex. : sécurisation des données, réinitialisation des mots de passe, suppression des accès non autorisés).

---

5. Obligation de notification à la Commission d'accès à l'information (CAI)

Conformément à la **Loi 25**, SECURIMED doit notifier la **Commission d'accès à l'information (CAI)** de toute violation de données personnelles qui présente un **risque sérieux** pour la confidentialité des données. La notification doit être effectuée **dans un délai maximal de 72 heures** suivant la découverte de la violation, sauf si cette notification n'est pas possible dans ce délai, auquel cas elle doit être faite **dès que possible**, avec une justification des raisons du retard.

La notification doit inclure les éléments suivants :

- **Description de la violation** : Une explication détaillée de ce qui s'est passé, y compris la nature de l'incident et comment il a été détecté.
- **Type de données concernées** : Identification des catégories de données personnelles touchées (ex. : nom, adresse, informations de santé, etc.).
- **Mesures prises pour remédier à la violation** : Actions immédiates mises en place pour limiter les effets de la violation (ex. : désactivation des comptes compromis, retour au contrôle des données, notification interne, etc.).
- **Évaluation des risques pour les personnes concernées** : Description du risque pour les individus concernés, en fonction de la nature de la violation.
- **Mesures proposées pour éviter de futures violations** : Mesures préventives pour éviter la récurrence de violations similaires (révision des protocoles de sécurité, amélioration des contrôles d'accès, etc.).
- **Nombre estimé de personnes affectées** : Nombre approximatif de personnes dont les renseignements personnels ont été affectés par l'incident.

---

6. Modèle de notification à la Commission d'accès à l'information (CAI)

Voici un modèle de notification à envoyer à la **Commission d'accès à l'information (CAI)** :

Objet : Notification de violation de données personnelles
Date : [Date]

Commission d'accès à l'information
[Adresse de la CAI]
[Courriel de la CAI]

Madame, Monsieur,

Conformément à l'article 14.1 de la Loi 25 sur la protection des renseignements personnels dans le secteur privé, nous vous informons par la présente d'une violation de données personnelles survenue au sein de notre organisation, **SECURIMED**.

Description de l'incident

[Décrivez la violation, y compris les circonstances de la découverte de l'incident, la nature de la violation et toute autre information pertinente.]

Type de données concernées

[Liste des catégories de données personnelles affectées : nom, adresse, numéro de téléphone, informations financières, données de santé, etc.]

Mesures correctives prises

[Décrivez les mesures prises immédiatement après la découverte de la violation pour sécuriser les données et limiter l'impact de l'incident.]

Risques pour les personnes concernées

[Évaluez les risques potentiels pour les personnes touchées par l'incident, par exemple : risques d'usurpation d'identité, pertes financières, atteinte à la réputation, etc.]

Nombre de personnes affectées

[Indiquez le nombre estimé de personnes concernées par la violation.]

Mesures préventives et correctives à long terme

[Indiquez les mesures mises en place pour éviter la récurrence de ce type d'incident à l'avenir, telles que des formations, des mises à jour des protocoles de sécurité, etc.]

Nous restons à votre disposition pour toute information complémentaire.

Cordialement,

LOUISE-DANIELE DUQUETTE
514 421-1223
SECURIMED

---

7. Notification des personnes concernées

Si l'incident de violation des données présente un risque élevé pour la confidentialité des renseignements personnels des personnes concernées, SECURIMED doit également notifier ces personnes directement, dès que possible.

La notification doit comporter :

- Une description de la violation des données.
- Le type de renseignements personnels concernés.
- Les mesures prises pour remédier à la violation et limiter les risques.
- Les actions que les personnes concernées peuvent entreprendre pour protéger leurs données.
- Les coordonnées du responsable de la protection des renseignements personnels chez SECURIMED pour toute question.

---

8. Suivi de la notification

Après la notification à la CAI et aux personnes concernées, le **Responsable de la protection des renseignements personnels (RPR)** doit suivre de près la situation pour s'assurer que toutes les actions correctives sont mises en œuvre et que des mesures de prévention sont prises pour éviter la répétition de l'incident.

Conclusion

La notification rapide et complète des violations de données à la **Commission d'accès à l'information (CAI)** est une obligation légale cruciale pour assurer la conformité avec la **Loi 25**. En suivant cette procédure, **SECURIMED** garantit non seulement la protection des renseignements personnels, mais aussi la transparence et la réactivité face à toute violation de données personnelles.

Annexe 1

Je _____ consens librement aux éléments suivants :

Je consens à ce que SECURIMED utilise mes renseignements personnels pour la gestion de mes services et de ma relation avec l'entreprise.

ACTES MÉDICAUX :
J'autorise les médecins, le personnel médical de la Clinique médicale SECURIMED et le personnel de la clinique de radiologies à effectuer les actes médicaux reliés à mon séjour/visite.

TRANSMISSION DE L'INFORMATIONS CONFIDENTIELLES MÉDICALES
J'autorise les médecins, le personnel médical, de la Clinique médicale SECURIMED et la clinique de radiologie et des laboratoires à transmettre toutes les images, les rapports, les informations sur mon état de santé et autres documents résultants de la visite par la poste, messagerie, télécopie, courriel ou dépôt de fichier aux intervenants suivants :

- personnel de la clinique SECURIMED;
- aux archives médicales de SECURIMED;
- médecin prescripteur;
- radiologistes inscrits au eMedical de la clinique MEDICA pour SECURIMED;
- à l'entreprise demandeur;
- à l'IRCC.

.

RAPPORT DE RADIOLOGISTES POUR L'IRCC
Je comprends que seul le rapport effectué (à partir des images de la clinique locale) par les radiologistes inscrits au eMedical de Medica pour SECURIMED sera officiel et transmis à IRCC.

JURIDICTION
LOI APPLICABLE : J'accepte, par la présente, que la relation entre moi-même, le docteur et/ou les employés de la Clinique médicale SECURIMED et le règlement de tout différend qu'elle pourra susciter, soient régis par les lois de la Province de Québec et interprétés en fonction de celles-ci.

JURIDICTION : Je reconnais, par la présente, que le traitement sera prodigué dans la Province de Québec et dans la localité désignée par SECURIMED et que les cours de la Province de Québec auront juridiction pour recevoir toute plainte, demande, réclamation ou cause d'action que celle-ci soit fondée sur une présumée rupture de contrat ou une présumée négligence consécutive au traitement.

Je conviens, par la présente, que si j'entame de telles procédures judiciaires, ce sera uniquement dans la Province de Québec ; je m'en remets irrévocablement, par la présente, à la juridiction exclusive des cours de la Province de Québec.J'ai pris connaissance du formulaire et je comprends que c'est dans l'optique d'une demande faite par un tier. Je comprends la nature, les avantages, les risques et les inconvénients. Je suis satisfait(e) des explications, précisions et réponses que la clinique m'a fournies.

Signature: _____ Date : _____