

## Politique de protection des données

**CENTRE DE READAPTATION AMBULATOIRE  
« Comité Entraide Lesdain » (C.R.A. « C.E.L. »)**

Sites « Le Cep » et « Le Saule »

## Table des matières

<b>1</b>	<b>L'importance de la protection des données .....</b>	<b>3</b>
<b>2</b>	<b>Champ d'application .....</b>	<b>4</b>
<b>3</b>	<b>L'organisation de la protection des données .....</b>	<b>4</b>
<b>4</b>	<b>Champ d'application des politiques de protection des données .....</b>	<b>6</b>
<b>5</b>	<b>Les responsables du traitement des dossiers des patients et leurs autorisations .....</b>	<b>6</b>
<b>6</b>	<b>Consultation interne et externe des dossiers des patients, droits et obligations des personnes chargées du traitement des données.....</b>	<b>7</b>
<b>7</b>	<b>La nature des données traitées et la manière dont elles sont recueillies .....</b>	<b>8</b>
<b>8</b>	<b>La gestion des risques .....</b>	<b>8</b>
<b>9</b>	<b>Durée de conservation des données .....</b>	<b>9</b>
<b>10</b>	<b>Droits et moyens de défense des patients en ce qui concerne la protection de leur vie privée.....</b>	<b>10</b>
<b>11</b>	<b>Objectifs de la politique de protection des données .....</b>	<b>11</b>
<b>12</b>	<b>Entrée en vigueur et modifications .....</b>	<b>11</b>

## 1 L'importance de la protection des données

Le C.R.A. « C.E.L. » attache une grande importance à la protection des données qu'elle traite, en particulier les données à caractère personnel. Cette politique, mise en place par le C.R.A. « C.E.L. », vise à établir à un niveau stratégique comment protéger les données, assigner les responsabilités à ce sujet et quelles sont les priorités fixées dans le cadre de la protection des données.

Le C.R.A. « C.E.L. » souhaite tout particulièrement protéger des risques suivants les données des patients et les données à caractère personnel qui lui sont confiées :

- la perte : les données devenues indisponibles
- les fuites : les données tombées entre de mauvaises mains.
- les erreurs : les données incorrectes, par exemple obsolètes ou incomplètes
- non accessibles : les données inaccessibles au moment des soins
- l'accès injustifié : l'accès aux données par des personnes non autorisées
- l'incapacité d'identifier la ou les personnes ayant accédé aux données, les ayant modifiées ou supprimées
- les opérations de traitement non conformes à la réglementation, aux lignes directrices ou aux normes applicables

Par le biais de cette politique, la direction souhaite inviter tous les acteurs du traitement électronique et papier à collaborer pour que les données à caractère personnel fournies soient traitées correctement, sur la base d'une vision et d'une volonté commune d'offrir des services de qualité.

La présente politique traite plus en profondeur de la protection de la vie privée et, plus particulièrement, de la protection des données à caractère personnel. Cette politique, sous forme de manuel de procédures, sert de norme pour le traitement des données à caractère personnel des patients et des employés .... Il s'agit d'un fil conducteur pour tous les processus de traitement et d'une référence pour l'audit et le contrôle. Le présent manuel donne à toute partie intéressée, employé ou partie externe impliquée, l'accès à la politique de protection des données et aux modalités de traitement des données à caractère personnel sensibles.

Le manuel s'adresse également à toute personne ayant une fonction au sein du C.R.A. « C.E.L. » exigeant le traitement de données à caractère personnel. Elles utilisent (certaines parties de) ce manuel pour concevoir des procédures et des lignes directrices à l'intention des employés et des parties externes, tels que les fournisseurs TIC (Technologies de l'Information et de la Communication). Les parties pertinentes de ce manuel relatives à notre politique de confidentialité sont intégrées dans les accords avec le personnel et les fournisseurs.

## 2 Champ d'application

Au début du contrat de travail, la direction est chargée de déterminer, en suivant la procédure existante, selon quels droits l'employé peut accéder aux données. De plus, il existe une matrice d'autorisation pour gérer les accès spécifiques.

Informations patients :

- Soins : Les soins de médecine préventive ou de diagnostic médical, les soins (médicaux, paramédicaux, infirmiers et psycho-sociaux) et/ou de traitements prodigués à la personne concernée ou à un parent, ou la gestion des services de santé, dans l'intérêt de la personne concernée ;
- Enregistrement : L'enregistrement des données médicales des patients à des fins internes, imposé par le gouvernement, ainsi qu'à des fins de recherche et de politique et de facturation ;
- Gestion des médicaments : Opérations de traitement relatives à la prescription, le suivi et/ou à la délivrance de médicaments ;
- Administration des patients et qualité des soins : Collecte et traitement de toutes les données relatives aux pratiques médicales et paramédicales, diagnostiques et thérapeutiques administrées aux patients afin d'améliorer la qualité des soins ;
- Traitement des plaintes : L'enregistrement des données à caractère personnel des patients et/ou des personnes de confiance désignées par ces derniers afin d'agir en tant que médiateurs dans le cadre des plaintes déposées. Enregistrement des plaintes.

Informations sur le personnel :

- Tous les employés ayant accès à des données à caractère personnel dans l'exercice de leurs fonctions, et en particulier les employés des RH bénéficiant de l'accès à des données à caractère personnel, signeront une clause de confidentialité sous forme d'avenant à leur contrat.
- Tous les candidats, volontaires, stagiaires qui entrent en contact avec des données personnelles, signeront une clause de confidentialité sous forme d'avenant à leur contrat

## 3 L'organisation de la protection des données

### Compétence

En tant que responsable du traitement de données, la compétence pour cette politique repose auprès du C.R.A. « C.E.L. », représentée par la direction. Le directeur est responsable de la formulation, de l'établissement et du contrôle du respect des principes de la politique au sein du C.R.A. « C.E.L. », avec l'appui du conseil d'administration et l'assemblée générale

### Responsable de la mise en œuvre

La direction agit en tant que plate-forme décisionnelle formelle pour la protection des données. La direction est autorisée à prendre des décisions au sujet des aspects suivants :

- L'analyse des risques et la méthodologie associée à celle-ci ;
- L'élaboration de la politique de protection des données et les lignes directrices connexes ;
- L'implémentation des mesures de sécurité (c'est-à-dire le contenu du plan de sécurité)

- La réponse structurelle aux problèmes de protection des données et aux conseils associés (dans un délai de 3 mois) ;

## **Le DPD**

Le suivi du contenu de la politique de protection des données relève de la responsabilité du délégué à la protection des données (DPD). La mission du DPD est assurée par Mademoiselle Brigitte Lievrouw. Il s'acquitte de cette tâche conformément aux dispositions du RGPD. Le C.R.A. « C.E.L. » transmettra l'identité (et toute modification) du DPD à l'autorité chargée de la protection des données. Le DPD émet des avis au Directeur du C.R.A. « C.E.L. » et est chargé en particulier de :

- Soumettre des conseils et des recommandations à la direction
- Promouvoir la sensibilisation de tous les acteurs au sein du C.R.A. « C.E.L. ».
- Surveille le respect de la politique de protection des données au sein du C.R.A. « C.E.L. »,
- Documente les questions de protection des données, telles qu'un plan de sécurité et le registre de traitement
- Exécute les tâches spécifiques assignées au DPD dans le cadre du RGPD.
- Enregistre les infractions et les soumet, accompagnées d'un conseil, au comité exécutif.

**Contact DPD : Brigitte Lievrouw**

**E-mail : [comptabilité@cracel.be](mailto:comptabilité@cracel.be)**

**Tel : 069/84.59.08**

## **L'employé**

Toute personne (interne ou externe) qui traite des données (par ex., y a accès, les enregistre, les modifie, etc.) le fait conformément aux principes de politique énoncés dans le présent manuel. L'utilisateur traite les données dans le respect du devoir de confidentialité, et conformément aux principes suivants :

- Elle est responsable des données des patients qu'il ou elle traite
- Exécute les consignes de sécurité au cours de sa mission de traitement
- Ne traite que les données pertinentes à la tâche
- Traite les données avec le plus grand soin
- Signale les infractions
- Respecte l'article 458 du Code pénal : L'utilisateur observe le secret professionnel.

- Employé TIC ou utilisateur clé** Outre les responsabilités de l'utilisateur, l'employé TIC ou l'utilisateur clé est responsable de ce qui suit :
- L'implémentation des mesures techniques
  - L'implémentation des paramètres de sécurité, conformément au présent manuel dédié à la politique.
  - Le signalement au DPD de tout problème de sécurité survenant avant, pendant ou après l'implémentation des ressources TIC.
  - Assume la fonction d'expert. Dans ce rôle, il ou elle participera à l'identification ainsi qu'à l'élimination des risques liés à la protection des données.
  - Respecte le code de bonne conduite.
- Fournisseur TIC** Le fournisseur TIC a les mêmes responsabilités que les employés TIC. À titre accessoire :
- Indique les risques de sécurité liés aux applications livrées.
  - Indique les tâches de sécurité à assumer par le fournisseur.
- Le fournisseur s'efforce de mener une politique de protection des données transparente en communiquant sur son propre niveau de sécurité actuel et sur le traitement des incidents de sécurité.

#### 4 Champ d'application des politiques de protection des données

Cette politique s'applique à l'ensemble du cycle de vie de l'information au sein du C.R.A. « C.E.L. », de l'obtention de l'information jusqu'à la suppression définitive de l'information par l'organisation.

- Tous les membres du personnel, internes et externes pour une durée déterminée ou indéterminée.
- Toutes les ressources d'entreprise et tous les systèmes de traitement de l'information gérés par le C.R.A. « C.E.L. » ainsi que les systèmes gérés par des parties externes aux fins du traitement de l'information pour le C.R.A. « C.E.L. » et les centres respectifs de réadaptation ambulatoire, tels que les bases de données, l'information quel que soit son support, les réseaux, les centres de données, etc.
- Toutes les activités de traitement, tant pour le responsable du traitement des données que pour celui ou celle qui exécute le traitement des données.

Compte tenu du rôle important des fournisseurs TIC dans la mise en place de l'environnement TIC pour le traitement des données, le manuel dédié à la politique énonce également les principes de politique à cet égard.

#### 5 Les responsables du traitement des dossiers des patients et leurs autorisations

Tous les employés et collaborateurs du C.R.A. « C.E.L. », qui, dans l'exercice de leurs fonctions, doivent accéder aux données à caractère personnel relatives à la santé, sont tenus de respecter la stricte confidentialité des données concernées.

Les personnes suivantes sont responsables du traitement des données à caractère personnel des patients, dans les limites de leur mission et des objectifs spécifiques à cette mission :

- Les membres du personnel et les professionnels indépendants associés aux différents services infirmiers et paramédicaux établissent les modules de traitement des dossiers des patients dont ils sont respectivement responsables.
- Le personnel du secrétariat médical et de l'administration médicale est responsable du traitement des données à caractère personnel contenues dans les dossiers des patients. Une attention particulière est portée à l'envoi des certificats, rapports, etc. Ceux-ci ne peuvent être envoyés qu'au patient lui-même ou aux prestataires de soins désignés par écrit par le patient.
- Le personnel d'accueil, de facturation et de comptabilité est responsable du traitement des données à caractère personnel contenues dans les dossiers des patients, à des fins de facturation, d'enregistrement médical, de suivi des débiteurs et d'information sur la politique.
- Les collaborateurs du service TIC sont responsables du traitement technique des données à caractère personnel converties en données anonymisées à des fins imposées par le gouvernement. En outre, ils travaillent avec des données à caractère personnel dans le cadre d'activités de résolution de problèmes, de gains d'efficacité interne ou d'applications similaires.
- Les membres du personnel d'un service d'accompagnement des patients sont responsables du traitement des données à caractère personnel contenues dans les dossiers des patients en vue d'effectuer les suivis respectifs des services social, psychologique, ...
- Les membres du personnel du service de médiation sont responsables du traitement des données à caractère personnel contenues dans les dossiers des patients, dans le cadre de la fonction de médiateur.

## 6 Consultation interne et externe des dossiers des patients, droits et obligations des personnes chargées du traitement des données.

### 6.1 En interne

- La consultation en interne et le traitement des dossiers des patients sont effectués par les personnes définies au point 5. Toutefois, ce droit est limité aux impératifs de leur mission et les personnes chargées du traitement des données n'ont pas accès aux données à caractère personnel non pertinentes à l'exécution de leur mission.
- Lors du traitement de données à caractère personnel, les personnes chargées du traitement des données ont l'obligation de traiter les données à caractère personnel de manière irréprochable et licite. Elles sont tenues de traiter les données à caractère personnel uniquement aux fins mentionnées au point 5 du présent règlement.
- Dans une optique de contrôle qualité, les auditeurs internes peuvent consulter les dossiers des patients ou les applications. Une déclaration de non-divulgence y est alors associée.
- En outre, les personnes chargées du traitement des données sont tenues de respecter la confidentialité lors du traitement des données à caractère personnel relatives à la santé et sont placées sous la supervision du médecin-directeur, du directeur des soins infirmiers et du délégué à la protection des données.

## 6.2 En externe

Dans le cadre de l'art. 7, sous-section 4 de la L.V.P., les catégories d'instances suivantes sont en droit d'obtenir des données à partir des dossiers des patients :

- Les institutions d'assurance, dans la mesure où elles sont imposées par ou en vertu de la loi ou avec le consentement du patient ;
- Les patients concernés ou leur représentant - à condition que le formulaire de demande signé soit disponible pour inspection ainsi qu'une copie du dossier du patient ;
- Les instances gouvernementales habilitées à le faire par décision publique ;
- Les soignants externes du patient avec son consentement ;
- D'autres institutions, dans la mesure où elles sont imposées par ou en vertu de la loi ou avec le consentement du patient ;
- Les fournisseurs de logiciels et de matériel informatique pour fournir un soutien. À cet effet, une déclaration spécifique (politique d'accès à distance) est signée pour garantir la confidentialité de ces données.

## 7 La nature des données traitées et la manière dont elles sont recueillies

La nature des données est définie comme suit :

- Données d'identification, y compris le numéro d'enregistrement national
- Données financières et administratives relatives à l'admission et à la facturation, y compris l'affiliation à la caisse d'assurance maladie
- Données médicales, paramédicales et relatives aux soins infirmiers, ventilées selon les applications suivantes :
  - données médicales
  - données relatives aux soins infirmiers
  - données paramédicales
  - médicaments
- Données sociales
- Autres données nécessaires à l'exécution des objectifs déterminés ou imposés par la loi (données judiciaires).

## 8 La gestion des risques

Le C.R.A. « C.E.L. » cartographie les risques de protection des données au moyen d'une analyse de risque sur la base des critères suivants (cadre de référence) :

- Les documents d'orientation sur la sécurité de l'information, notamment des données à caractère personnel, publiées par la Commission pour la protection de la vie privée.
- Le Règlement général sur la protection des données
- La norme ISO 27001 sur la sécurité de l'information

L'analyse a permis d'identifier les risques opérationnels et tactiques. Ces risques ont été examinés en concertation avec la direction. Les résultats de l'analyse des risques ont été discutés et seront inclus dans un plan d'action pour traiter les risques identifiés. Dans ce rapport, le C.R.A. « C.E.L. » a déterminé quatre traitements possibles des risques :

- Acceptation : un risque est accepté, aucune mesure supplémentaire n'est prise. Le C.R.A. « C.E.L. » s'efforce d'accepter le moins de risques possible.
- Transfert : un risque est transféré de sorte à ce que la responsabilité du risque n'incombe plus au C.R.A. « C.E.L. ».
- Limitation : le C.R.A. « C.E.L. » prend les mesures nécessaires pour limiter un risque afin que le risque soit réduit à un niveau acceptable.
- Exclusion : le C.R.A. « C.E.L. » doit prendre des mesures pour éviter qu'un risque donné ne survienne.

Toutes les mesures nécessaires sont prises pour garantir l'exactitude et l'exhaustivité des données enregistrées. Les mesures techniques et organisationnelles nécessaires sont également prises pour garantir que les dossiers des patients soient protégés contre la perte ou la détérioration des données et de l'accès, la modification ou la divulgation non autorisés.

L'objectif est de revoir l'analyse des risques au moins une fois par an. Cela fait partie des tâches du DPD.

Des campagnes de sensibilisation seront également menées chaque année à l'intention du personnel du C.R.A. « C.E.L. » et des centres de réadaptation ambulatoires respectifs.

Etant donné que le C.R.A. « C.E.L. » et les centres de réadaptation ambulatoire respectifs disposent d'un grand nombre de données sensibles, le département TIC a développé une matrice d'autorisation qui indique, pour chaque département et service, quel rôle dispose de quelle compétence dans le domaine de l'accès numérique.

## 9 Durée de conservation des données

Dans le respect des éventuelles dispositions légales, un délai de conservation de :

- 1 an pour les données à caractère personnel permettant l'identification de l'individu, à partir de la dernière autorisation de sortie ou du dernier traitement du patient :
  - 10 ans pour les données de facturation provenant des dossiers des patients qui servent de pièce justificative comptable ;
  - 30 ans pour les données médicales ;
  - 1 an pour les dossiers clos du service de médiation (après établissement du rapport annuel).
- 
- Lorsque la période de conservation arrive à son terme, les données à caractère personnel en question sont supprimées des fichiers et détruites dans un délai d'un an. Pour le module médical stricto sensu, cela ne peut se faire qu'avec l'accord du médecin-directeur.
  - Toutefois, la destruction ne doit pas avoir lieu lorsque :
    - la conservation des données est requise sur la base d'une disposition légale ;

- la conservation est considérée comme ayant une importance raisonnable du point de vue médical ou du point de vue de l'espérance de vie du patient, ou encore du point de vue de la défense de ses intérêts légitimes ou de ceux de ses ayants droit ;

- un accord sur la conservation des données a été conclu entre le patient et le médecin-directeur du C.R.A.

Si les données en question ont été traitées de telle sorte qu'il est raisonnablement impossible de remonter jusqu'à des individus, elles peuvent être conservées sous forme anonyme.

## 10 Droits et moyens de défense des patients en ce qui concerne la protection de leur vie privée.

• Le patient, ayant prouvé son identité, a le droit de prendre connaissance auprès du responsable du traitement, de :

- l'existence ou non de traitements de données le concernant,

- les objectifs d'un tel traitement,

- les catégories de données concernées par ce traitement,

- les catégories de destinataires auxquels les données sont communiquées,

- les données elles-mêmes faisant l'objet du traitement et toutes les informations disponibles sur l'origine de ces données, à moins que la loi sur l'accès aux données ne l'exclue.

• Toute personne peut s'opposer, gratuitement et sans indiquer de motif, au traitement des données à des fins de marketing direct.

• Dans le cas de la collecte de données à caractère personnel concernant le patient, celui-ci en sera informé selon les dispositions de l'article 4 de la L.V.P. via :

- Le site Web du C.R.A. « C.E.L. »

• En outre, toute personne a le droit d'obtenir, soit directement, soit par l'intermédiaire d'un professionnel de santé, les données à caractère personnel relatives à sa santé qui sont traitées. Cette demande d'accès ou de copie doit être adressée à la direction générale.

• Si le patient estime que les dispositions du présent règlement n'ont pas été respectées ou s'il a d'autres motifs de plainte au sujet de la protection de sa vie privée, il peut contacter la ou les personnes mentionnées au §5 et la direction générale à tout moment.

• Sans préjudice de tous les recours et moyens de défense internes énumérés ci-dessus, le patient peut, conformément aux dispositions de l'art. 13, 14 et 63 et suivants de la L.V.P., s'adresser respectivement au Président du Tribunal de première instance et à la Commission pour la protection de la vie privée, à l'adresse Hoogstraat 139 - 1000 BRUXELLES

## 11 Objectifs de la politique de protection des données

Le C.R.A. « C.E.L. », à la fois dans son rôle de responsable et d'exécutant du traitement de données :

1. Applique une entière transparence en ce qui concerne les données à caractère personnel qu'elle traite et de l'objectif dudit traitement, tant envers la personne concernée que pour les clients et les autorités de contrôle. La communication se veut honnête, facilement accessible et compréhensible. Le principe de transparence s'applique également lors de la transmission de données à caractère personnel.
2. Ne traite que les données pertinentes pour l'exécution de ses tâches. Chacune des tâches pour lesquelles des données à caractère personnel sont traitées obéissent au principe de licéité. Cela signifie, entre autres, que le traitement est conforme aux objectifs légaux et statutaires du C.R.A. « C.E.L. ». Celui-ci est évalué en fonction de chaque nouvel objectif du traitement, le cas échéant au moyen d'une analyse d'impact sur la protection des données.
3. Ne traite que les données à caractère personnel strictement nécessaires à l'exécution des activités. Aussi, les identificateurs associés aux données à caractère personnel sont réduits au minimum.
4. Surveille l'intégrité des données à caractère personnel tout au long du cycle de traitement.
5. Ne conserve pas les données plus longtemps que nécessaire. Cette nécessité a été vérifiée par rapport aux obligations légales et aux droits et libertés de la personne concernée.
6. Empêche les violations résultant du traitement des données à caractère personnel. La sécurité de l'information, la conception de la protection des données et les paramètres par défaut respectueux de la vie privée sont des outils développés à ces fins. En cas d'infraction, celle-ci fait l'objet d'un rapport, conformément à la réglementation en vigueur.
7. Est en mesure d'exercer tous les droits en vigueur de la personne concernée, tels que le droit d'accès, de copie et éventuellement de suppression. Ce faisant, le C.R.A. « C.E.L. » surveille les éventuelles limitations de ces droits.
8. Veille activement, lors du traitement des données à caractère personnel dans un but spécifique, à ce que les droits et libertés de la personne concernée (par exemple le droit à l'assurance, le droit aux soins) soient respectés.
9. Traite les données conformément aux droits et libertés en vigueur dans l'Espace économique européen et contrôle leur application lorsque les données sont transférées en dehors de l'Espace économique européen. Le C.R.A. « C.E.L. » se conforme donc à tous les cadres juridiques et normatifs (c'est-à-dire les réglementations wallonnes, fédérales et européennes) lors du traitement des données à caractère personnel et, à cette fin, a clairement défini ses responsabilités et celles des autres parties en ce qui concerne les données à caractère personnel. En outre, le C.R.A. « C.E.L. » surveille et applique les codes de conduite en vigueur dans son secteur d'activité.
10. Peut démontrer qu'elle respecte tous les objectifs de la politique, conformément aux dispositions légales. Cette responsabilité, vérifiée par les suivis et contrôle internes, est exécutoire conformément aux principes juridiques en vigueur.

## 12 Entrée en vigueur et modifications

Cette version de la politique de confidentialité est entrée en vigueur le 25 mai 2018