|  |
| --- |
|  |
| **NOTE**  |
| Adhésion au circle of trust de BELRAI : explications concernant la check-list BelRAIVersion 6.10.2015  |

# Réglementation

L'institution souscrit à la réglementation suivante.

## La loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (LVP)

L'institution souscrit à [la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel](http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1992120832&table_name=loi). Ci-après est utilisée l'abréviation "LVP" pour désigner la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Tant les droits et obligations de la personne dont les données sont traitées que ceux de la personne qui les traite ont été fixés dans cette loi.

## La loi relative aux droits du patient (LDP)

L'institution souscrit à [la loi du 22 août 2002 relative aux droits du patient.](http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2002082245&table_name=loi) Ci-après est utilisée l'abréviation "LDP" pour désigner la loi relative aux droits du patient.

Un certain nombre de droits importants de l'utilisateur de soins (patient/client) et du dispensateur de soins ou du dispensateur d'aide (praticien professionnel) y sont énumérés.

Les droits de l'utilisateur de soins sont (voir aussi **annexe**  1 en 2):

1. le droit à une prestation de service de qualité
2. le droit au libre choix du dispensateur de soins ou du dispensateur d'aide
3. le droit à l'information sur l'état de santé
4. le droit au consentement après information
5. les droits relatifs au dossier patient
6. le droit à la protection de la vie privée
7. le droit de déposer une plainte auprès d'un service de médiation compétent.

La LDP régit les droits d'un groupe restreint de patients. Pour BelRAI, il n'y a pas de limitation, et les droits s'appliquent à tous les utilisateurs de soins (tant les soins que l’aide).

## Délibérations de la Commission de la protection de la vie privée

Vous pouvez consulter les délibérations ci-dessous sur le [site web](https://www.ehealth.fgov.be/fr/a-propos-de-ehealth/organisation/comite-sectoriel/presentation) de la plate-forme eHealth.

[Délibération n° 09/18 du 19 mai 2009, modifié la dernière fois le 19 mai 2015, en ce qui concerne l'échange de données personnelles qui concernent la santé entre les dispensateurs de soins concernés et la base de données BelRAI avec intervention de la plate-forme eHealth](http://www.privacycommission.be/sites/privacycommission/files/documents/d%C3%A9lib%C3%A9ration_SS_018_2009_3.pdf)

Délibération n° 11/088 du 18 octobre 2011, modifiée le 9 juin 2015, relative à la note relative aux preuves électroniques d'une relation thérapeutique et d'une relation de soins.

Délibération n° 14/06 du 18 février 2014, modifiée le 9 juin 2015, portant sur le règlement du partage des données entre les systèmes de santé connectés via le répertoire de références de la plate-forme eHealth.

## Autres réglementations ou dispositions réglementaires

* les dispositions légales et réglementaires relatives à l'exercice de la médecine
* les dispositions légales et réglementaires relatives au secret professionnel, en ce compris l'article 458 du Code pénal

# Autorisations de la Commission de protection de la vie privée (CPVP)

## L'institution dispose des autorisations nécessaires

L'institution doit disposer des **autorisations nécessaires pour pouvoir traiter des données à caractère personnel**. Elle doit demander ces autorisations à la Commission de la protection de la vie privée (ci-après dénommée "CPVP"), également connue sous le nom de Commission vie privée. La CPVP a été créée en tant qu'organe de contrôle indépendant par la LVP. Elle veille à ce que les données à caractère personnel soient utilisées avec soin et de façon sécurisée, dans le but de garantir la vie privée des citoyens.

La CPVP se compose de différents comités sectoriels. Ces comités sectoriels veillent, dans un secteur spécifique, à ce que la vie privée soit protégée lors du traitement de données à caractère personnel. Certains traitements sont cependant si délicats qu'ils ne sont possibles qu’avec une autorisation spécifique délivrée à cet effet par le Comité sectoriel compétent.

Le Comité sectoriel de la Sécurité sociale et de la Santé en est un exemple. Ce Comité protège la vie privée des assurés au sein du réseau de la sécurité sociale belge lors du traitement de leurs données à caractère personnel, et surveille spécialement la communication de données de santé. Le Comité se compose de 2 sections, à savoir la section Sécurité sociale et la section Santé. Le rôle de ce Comité sectoriel a été fixé par la loi. Le Comité sectoriel de la Sécurité sociale et de la Santé a été créé au sein de la Commission par la Loi belge du 15 janvier 1990.

Vous pouvez retrouver [ici](http://www.privacycommission.be/fr/) de plus amples informations concernant la CPVP.

# Accès à e-Health

## L'institution dispose d'un certificat eHealth

L'institution doit **demander un accès** aux services en ligne sécurisés de eHealth. De plus amples informations à ce sujet peuvent être trouvées [ici](https://www.ehealth.fgov.be/fr/support/services-de-base/certificats/generalites).

## L'institution a désigné un gestionnaire d'accès

L'institution doit désigner un gestionnaire d'accès. Dans le cadre de eHealth, on parle d' **un Responsable Accès Entité (RAE)**. Le RAE est responsable des accès de l'institution aux services en ligne sécurisés de eHealth. De plus amples informations à ce sujet peuvent être trouvées [ici](https://www.ehealth.fgov.be/fr/services-de-base/gestion-integree-des-utilisateurs-et-des-acces/presentation).

# Politique en matière de sécurité de l'information

## Plan de sécurité

On entend par plan de sécurité, un plan d'approche/plan par étapes en vue d'arriver à une politique de sécurité de l'information et /ou en vue de surveiller la politique de sécurité de l'information en vigueur.

Le plan de sécurité se composera des éléments suivants :

* politique de sécurité stratégique;
* politique de sécurité opérationnelle, situation actuelle;
* politique de sécurité opérationnelle, objectif;
* plan de sécurité opérationnel;
* rapports d'audit éventuels.

#### politique de sécurité stratégique

La politique de sécurité stratégique reflète les directives concernant la sécurisation de l'institution. Il s'agit d'un cadre approuvé dans lequel chaque travailleur salarié de l'institution ainsi que les tiers en relation avec eux exécutent leurs tâches.

#### Politique de sécurité opérationnelle, situation actuelle

Une politique de sécurité opérationnelle implémente la politique de sécurité stratégique de l'institution. Elle comporte toutes les mesures, conventions ... en vigueur au sein de l'institution qui sont en application lors des travaux journaliers dans le contexte de la sécurisation de l'information. Le plan de sécurité opérationnel est adapté au cadre offert par la politique de sécurité stratégique et doit donner un contenu à tous les domaines d'attention de cette dernière. (Cf. AS-IS)

#### Politique de sécurité opérationnelle, objectif

Le contenu actuel qui est donné à la politique de sécurité stratégique est rarement la situation finale souhaitable et pas davantage une donnée stable (surtout l'ICT et les aspects organisationnels fluctuent). Outre la situation actuelle, l'objectif assigné à l'institution est également documenté. (cf. TO-BE)

#### Plan de sécurité opérationnel

Le plan de sécurité opérationnel a pour but de faire évoluer l'institution vers l'objectif de façon méthodique. Le plan de sécurité opérationnel documente quelles adaptations en matière d'implémentation, quels nouveaux accords, ... seront introduits dans l'institution aux fins d'améliorer la situation sur le plan de la sécurité. Ceci comporte une incidence documentée de :

* l'inventaire des actions d'amélioration
* leur priorisation
* leur programmation

## Politique en matière de sécurité de l'information

La politique en matière de sécurité de l'information énumère les principes fondamentaux sur le plan de la sécurité de l'information. [La norme ISO 27002](http://en.wikipedia.org/wiki/ISO/IEC_27002) sert de base à la politique en matière de sécurité.

Vous pouvez vous baser lors de l'élaboration de la politique en matière de sécurité sur l'“Information Security Management System (ISMS)” tel qu'il est défini par la Banque Carrefour de la sécurité sociale (BCSC).

Ce sont les 12 normes minimales que nous pouvons distinguer au sein du ISMS.

1. Détermination du risque

2. Politique de sécurité de l'information

3. Organisation de la sécurité de l'information

4. Gestion des moyens d'exploitation

5. Sécurité en rapport avec les collaborateurs

6. Sécurisation physique et sécurisation des environs

7. Gestion opérationnelle

8. Protection logique de l'accès

9. Développement et maintenance des systèmes

10. Gestion des incidents (en matière de sécurité de l'information)

11. Gestion de la continuité

12. Respect

Au bas de cette [page web](https://www.ksz-bcss.fgov.be/fr/bcss/page/content/websites/belgium/security/security_04/security_04_02.html), vous pouvez retrouver les documents pertinents suivants :

* Le document "Normes minimales" décrit brièvement et de façon claire les normes minimales de la politique en matière de sécurité de l'information.
* Le document "Questionnaire pour l’exécution des normes minimales de sécurité" est un moyen d'évaluation intéressant pour contrôler si votre institution satisfait aux normes de sécurité minimales.
* Le document " Politique de sécurité de l'information" est un bel exemple de politique en matière de sécurité de l'information.

## Service de sécurité et conseiller en sécurité

Quelques points d'attention importants de la politique en matière de sécurité de l'information sont :

* *Un service de sécurité de l'information* doit être créé.
* *Un conseiller en sécurité de l'information* doit être désigné. Cette personne remplira les tâches suivantes :
	+ fournir des avis autorisés à la personne chargée de la gestion journalière;
	+ exécuter les missions qui lui sont confiées par la personne chargée de la gestion journalière.
* Ce conseiller en sécurité de l'information dirigera le service de sécurité de l'information.
* L'identité du conseiller en sécurité de l'information doit être communiquée aux institutions de surveillance.

# Protection logique de l'accès

## Procédure en matière d'accès sécurisé aux données

La protection logique de l'accès est un élément de la politique en matière de sécurité de l'information. L'accès aux données doit être protégé au moyen d'un système d'identification, d'authentification et d'autorisation. Ceci signifie aussi que l'institution veille à ce que les règles en vigueur en ce qui concerne le consentement éclairé et la relation thérapeutique/de soins soient respectées à tout moment et par tous les dispensateurs de soins ou les dispensateurs d'aide.

Lors de l'échange électronique d'informations sur la santé et l’aide, une protection adéquate de la vie privée de l'utilisateur de soins (patient/client) ainsi qu'une parfaite sécurité de l'information sont bien entendu très importantes. Les mesures en matière de protection de la vie privée et de la sécurité de l'information doivent être implémentées de telle sorte que les risques d'utilisation illégitime des données à caractère personnel concernant la santé soient évités au maximum alors que les avantages recherchés sur le plan de la qualité et de la continuité des soins, de la sécurité du patient et de la diminution des charges sont atteints. Aussi convient-il donc de trouver un bon équilibre entre la sécurité de l'information et un échange de données efficace.

L'institution est responsable de l'organisation interne de l'identification, de l'authentification et de l'autorisation des utilisateurs. Pour ce faire, l'institution doit disposer d'une politique en matière de sécurité de l'information.

L'institution veille en particulier à ce que l'accès qu'elle donne aux données des questionnaires BelRAI à ses dispensateurs de soins respecte les droits d'accès tels qu'ils sont définis dans l'autorisation Commission Vie privée BelRAI[[1]](#footnote-1), matrices d'accès aux pages 36-40.

BelRAI est responsable de l'organisation de l'identification, de l'authentification et de l'autorisation des utilisateurs de soins, des dispensateurs de soins ou des dispensateurs d'aide individuels ainsi que des institutions sur la plate-forme BelRAI.

## Liste actualisée de dispensateurs de soins et d’aide

Dans ce cadre, l'institution doit pouvoir prévoir à tout moment une liste actualisée de dispensateurs de soins ou de dispensateurs d'aide avec un accès éventuel à BelRAI.

## Logging d'accès

L'institution doit également prévoir une procédure de logging d'accès, ainsi que la gestion de ces données de logging. Les données qu’un tel logging doit certainement enregistrer sont qui a fait quoi, quand et dans quel contexte (pourquoi). L'institution prévoit donc aussi un système de logging de sécurité par étapes, de sorte qu'il soit toujours possible d'établir qui a consulté quelles données.

La tenue à jour des loggings de sécurité est une des mesures qui garantissent la sécurité et la confidentialité des informations de santé et d’aide. Par cette mesure, un contrôle peut être exercé sur le fonctionnement correct de la gestion de l'accès et des (tentatives d')infractions peuvent être contrôlées tant par les gestionnaires dans le cadre du fonctionnement correct du système qu'à la demande de l'utilisateur de soins (patient/client) dans l'exercice de ses droits du patient. Un tel système doit toujours être en mesure de déterminer qui a consulté quelles données.

L'institution est responsable de l'organisation interne d'un mécanisme de logging tant pour le logging fonctionnel que technique du réseau pour les informations de santé et d’aide via la plate-forme BelRAI et les solutions ICT concernées.

BelRAI est responsable de l'organisation d'un mécanisme de logging dans la plate-forme BelRAI.

## Procédure d'examen et procédure disciplinaire

L'institution doit prévoir une procédure d'examen et une procédure disciplinaire, en cas d'abus signalé ou supposé de l'accès aux données.

## Donner accès au logging d'accès à l'utilisateur de soins et d’aide

L'institution doit donner aussi au patient / client l'accès au logging d'accès à ses données.

# Consentement éclairé au sein de l'institution

## L'institution dispose de documentation concernant le consentement éclairé et le principe opt-in

Sans le consentement éclairé, aucune donnée relative au patient en question ne peut être partagée entre dispensateurs de soins ou les dispensateurs d'aide.

L'institution est responsable de l'organisation interne de l'information du patient. L'information se fait de préférence à l'aide d'***une brochure d'information*.**

Les éléments d'information sont :

* mention d'un responsable
* mention d'un interlocuteur pour les questions et les compléments d'information
* explications sur l'organisation du traitement des informations de santé et d’aide
* explications sur les "Droits du patient"

Chaque utilisateur de soins doit avoir une idée claire et compréhensible de qui peut échanger quelles informations de santé et d’aide, quand, avec qui et à quelles fins. Lors de l'information de l'utilisateur de soins, l'institution doit tenir compte de l'âge, de la formation, des possibilités psychiques, ... de l'utilisateur de soins. Dans la communication, les termes techniques doivent être évités autant que possible et expliqués de manière simple. L'utilisateur de soins a en outre toujours le droit de décider librement s'il autorise ou non l'échange de données via la plate-forme BelRAI. De plus, l'utilisateur de soins a la possibilité à tout moment de ne plus partager de données via la plate-forme BelRAI.

## L'institution dispose d'une procédure pour l'enregistrement du consentement éclairé

La procédure pour l'enregistrement du consentement éclairé doit permettre aux institutions d'enregistrer un consentement éclairé d'un patient. Avant tout, le patient doit être inscrit dans l'institution. L'institution doit informer le patient d'une manière claire et non technique des conséquences de ce consentement. Dans ce cadre, le principe opt-in doit aussi être éclairé.

## L'institution dispose d'une procédure pour la révocation du consentement éclairé

Il y lieu aussi de communiquer la procédure pour la révocation du consentement éclairé.

# Relation thérapeutique / de soins

## L'institution dispose d'une procédure pour l'enregistrement, l'exclusion, la gestion et la vérification de la relation thérapeutique/de soins.

Le partage de données de santé via la plate-forme BelRAI requiert la vérification préalable de l'existence d'une relation thérapeutique ou de soins entre le dispensateur de soins/dispensateur d’aide qui partage les données et le patient. Dans les institutions qui recourent au service web BelRAI, le contrôle est assuré par l'institution, et non plus par la plate-forme BelRAI.

L'institution est responsable de sa propre organisation interne de l'enregistrement, de l'exclusion, de la gestion et de la vérification de la relation thérapeutique/de soins. L'institution fait usage de ses propres banques de données spécifiques relatives aux relations thérapeutiques/de soins, ou de banques de données qui sont accessibles via un service de base de la plate-forme eHealth. Chaque acte relatif à l'enregistrement, l'exclusion, la gestion et la vérification de la relation thérapeutique/de soins doit être enregistré.

L'institution doit disposer d'une procédure pour enregistrer et implémenter des exclusions. Par *exclusion*, nous entendons la possibilité du patient de refuser l'accès à ses données de santé à un dispensateur de soins ou dispensateur d'aide individuel.

L'institution respecte les dispositions du Comité sectoriel de la Sécurité sociale et de la Santé de la CPVP sur ce qu’est une relation thérapeutique/de soins, et quels sont les moyens de preuve électroniques.

BelRAI est responsable de l'organisation de l'enregistrement de la relation thérapeutique entre un utilisateur de soins et un dispensateur de soins ou dispensateur d'aide individuel sur la plate-forme BelRAI.

# Droit de plainte[[2]](#footnote-2)

## L'institution satisfait au droit de plainte tel que défini dans la loi relative aux droits du patient

Le patient a le droit de déposer une plainte relative aux droits définis dans la LDP qui peuvent être exercés par l'utilisateur de soins (patient/client). Les plaintes fondées sur des erreurs médicales supposées relèvent également de la compétence de la fonction de médiation.

La fonction de médiation couvre les missions suivantes.

* La prévention des questions et des plaintes par la communication entre l'utilisateur de soins (patient/client) et le dispensateur de soins ou le dispensateur d'aide (praticien professionnel)
* La médiation concernant les plaintes en vue de trouver une solution
* L'information du patient au sujet des possibilités en matière de règlement de sa plainte en l'absence de solution
* La communication d’informations sur l’organisation, le fonctionnement et les règles de procédure de la fonction de médiation
* La formulation de recommandations permettant d’éviter que les manquements soient susceptibles de donner lieu à une plainte

Non seulement le patient mais aussi le représentant désigné[[3]](#footnote-3), le conjoint cohabitant, le partenaire cohabitant légal ou le partenaire cohabitant de fait, un enfant majeur, un parent, un frère ou une sœur majeurs, peuvent introduire une plainte auprès de la fonction de médiation.

# Organisation interne de l'institution

## L'institution désigne un interlocuteur pour les problèmes techniques

Un interlocuteur doit être désigné pour les problèmes techniques. Cette personne fait office de point de contact unique (‘Single point of contact’ SPOC) au sein de l'institution pour ce qui est des problèmes techniques. Par problèmes techniques, nous entendons des problèmes en rapport avec la solution ICT utilisée (p.ex. connexion lente, messages d'erreur technique, ...).

## L'institution désigne un interlocuteur pour les problèmes (fonctionnels) intrinsèques

L'institution doit désigner un interlocuteur (SPOC) pour les problèmes (fonctionnels) intrinsèques. Par problèmes fonctionnels, nous entendons des problèmes en rapport avec le contenu des données dans l'application (p.ex. données erronées ou manquantes).

# Formation / partage des informations

## L'institution organise des formations pour les dispensateurs de soins et d’aide au sein de l'institution

Des formations doivent être prévues pour les dispensateurs de soins ou les dispensateurs d'aide au sein de l'institution. Ces formations doivent éclairer sur l'utilisation de la solution d'information, ainsi qu'attirer l'attention des utilisateurs sur leurs droits et obligations. La politique de sécurité peut certainement y être également exposée brièvement.

## L'institution partage les informations et s'occupe des relations publiques envers les utilisateurs de soins (patients/clients), tous les collaborateurs et autres parties intéressées

## L'institution informe l'utilisateur de soins (patient/client) de ses droits

L'institution informe le patient de ses droits. La brochure du SPF Santé publique est un bon moyen pour ce faire.

1. [Délibération n° 09/18 du 19 mai 2009, modifié la dernière fois le 19 mai 2015, en ce qui concerne l'échange de données personnelles qui concernent la santé entre les dispensateurs de soins concernés et la base de données BelRAI avec intervention de la plate-forme eHealth](http://www.privacycommission.be/sites/privacycommission/files/documents/d%C3%A9lib%C3%A9ration_SS_018_2009_3.pdf) [↑](#footnote-ref-1)
2. Le droit de plainte est défini à l'art. 11 de la LDP. [↑](#footnote-ref-2)
3. Le **représentant désigné** est défini à l'art. 14 § 1er de la LDP. Un représentant désigné est une personne désignée préalablement par le patient, qui se substituera au patient. Ceci si et aussi longtemps que le patient n'est pas en mesure d'exercer ses droits définis dans la LDP. Le représentant désigné exercera alors ces droits. La désignation de cette personne s’effectue par un mandat écrit spécifique, daté et signé par cette personne ainsi que par le patient, mandat par lequel cette personne marque son consentement. [↑](#footnote-ref-3)