|  |
| --- |
|  |
| **CONVENTION**  |
| Convention pour l'adhésion au Circle Of Trust de BelRAI  BelRAI03.05.2017  |

**Convention relative à l'utilisation des services web BelRAI pour le partage de données avec les institutions ET ORGANISATIONS de soins**

Entre

“**L'Etat belge**”, représenté par Pedro Facon, Directeur général Soins de santé, Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement, ci-après dénommé “**L'Etat**”,

d'une part,

et

“**l'institution**” soit <nom institution> avec numéro BCE <numéro>,<numéro(s) Inami>, <adresse>, représentée par <nom & fonction>, ci-après dénommée “l'institution”,

d'autre part,

il est convenu ce qui suit :

## Article premier.

Par “**politique de sécurité ICT stratégique**”, on entend : la politique de sécurité, élaborée et entretenue par l'institution, qui se conforme à la norme ISO27002.

Par “**l'application**”, on entend BelRAI. BelRAI est une plate-forme digitale pour l'enregistrement et le partage des évaluations de soins suivant les instruments interRAI.

## Art. 2

La présente convention ne peut porter atteinte à la Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, à la loi du 22 août 2002 relative aux droits du patient, aux dispositions légales et réglementaires relatives à l'exercice de la médecine, aux dispositions légales et réglementaires relatives au secret professionnel, en ce compris l'article 458 du Code pénal.

## Art. 3.

Sans préjudice de l'application de l'article 16, § 4, de la Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, l'institution et, le cas échéant, les dispensateurs de soins ou les prestataires d'aide, déterminent dans quelle mesure et de quelle manière les données dans les dossiers individuels sont accessibles aux personnes qui sont concernées dans leurs activités exercées dans le cadre des soins, compte tenu de la fonction de ces personnes, de la nature des données et des risques potentiels qui y sont liés, ainsi que les dispositions de la présente convention. L'institution intègre cette disposition dans une politique de sécurité ICT stratégique, conformément à la norme ISO27002.

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 [[1]](#footnote-1)Commission Vie privée BelRAI, matrices d'accès aux pages 36-40.

L'institution déclare avoir connaissance du contenu de la norme ISO27002 et accepte celle-ci comme norme stratégique pour sa politique de sécurité ICT stratégique. L'institution conformera dès lors sa propre politique de sécurité et son implémentation à cette norme.

Outre ce choix de la norme de sécurité ICT précitée, l'institution prendra les mesures opérationnelles nécessaires afin de prévoir une implémentation efficace pour les divers domaines de cette norme.

L'institution élabore une politique de sécurité, complétée de la manière dont l'utilisateur de soins est informé sur ses droits dans le cadre de la présente convention et le rôle qu'assume le consultant en sécurité de l’information.

Pour ce faire, l'institution constitue et entretient au moins la documentation ci-après, et ce conformément à la norme ISO27002 :

* politique de sécurité ICT opérationnelle, situation actuelle : l'institution y documentera la situation actuelle de l'implémentation de sécurité ICT;
* politique de sécurité ICT opérationnelle, objectif : l'institution y documentera la situation vers laquelle on tend à l'avenir;
* plan de sécurité ICT opérationnel : l'institution y indiquera les actions qu'elle réalisera prioritairement dans le cadre de la sécurité ICT dans un délai de 3 ans ainsi que le planning prévu.

## Art. 4.

Chaque institution désigne, parmi ses collaborateurs ou non, un consultant en sécurité de l’information, conformément aux articles 8, § 2 et 10, de la loi du 8 août 1983 organisant un Registre national des personnes physiques et conformément à l’article 9 de la Loi 21 août 2008 relative à l'institution et à l'organisation de la place-forme eHealth et portant des dispositions diverses.

L’identité (nom, prénom, numéro de registre national) et la fonction (convention) du consultant en sécurité de l’information ainsi que toute modification sont communiqués à l’Etat.

## Art. 5.

L'institution s'engage spécifiquement dans le cadre de BelRAI à tenir en permanence à disposition, sur simple demande de l'Etat, les données suivantes :

* l'identité des utilisateurs de l'application;
* les équipements de réseau de l'environnement pour autant que ce soit pertinent dans le cadre de BelRAI et de (des) l'application(s) qui échangent des données avec le BelRAI;
* tout échange de données par les utilisateurs finaux concernant des données à caractère personnel dans le cadre de BelRAI doit être traçable et est susceptible d'être réclamé.

## Art. 6.

L'institution déclare toujours être accessible pour un audit par le consultant en sécurité de l’information désigné par ses soins. Cet audit est annoncé au préalable ou non.

## Art. 7.

La politique de sécurité opérationnelle doit être entretenue par l'institution. L'institution s'engage à transmettre au consultant en sécurité de l’information désigné par elle :

* le plus rapidement possible toute modification importante de la politique de sécurité opérationnelle;
* au moins chaque année (en janvier) une mise à jour de la politique de sécurité opérationnelle, assortie d'un nouveau plan de sécurité ICT opérationnel.
* le rapport annuel d'activité qu’elle aura fait réaliser et qui indique les mesures prises pour consolider de manière optimale la sécurité de l’information et la maintenir ainsi que le nombre et la portée des contrôles avec les réponses et suites qui y ont été apportées.

## Art. 8.

Le consultant en sécurité de l’information désigné par l'institution assure le suivi de ces accords ainsi que le bon fonctionnement de la politique de sécurité ICT, y compris son implémentation.

Pour ces tâches, le consultant en sécurité de l’information fait rapport et conseille au besoin directement la direction de l'institution.

L'institution prend également connaissance du fait que le consultant en sécurité de l’information ne peut pas assumer de responsabilité finale (ICT) au sein de l'institution. La responsabilité du consultant en sécurité de l’information consiste en sa mission de suivre correctement l'institution et de délivrer si nécessaire des conseils de qualité. L'institution s'engage à réagir à un tel conseil dans un délai de quatre semaines.

## Art. 9.

L'institution est d'accord pour que les données de patient, qu'elle transmet à BelRAI, soient éventuellement envoyées sous forme codée à interRAI (toujours dans le cadre des règles en vigueur sur la vie privée) et s'assure de ce que les patients aient marqué au préalable et de façon explicite leur accord pour que leurs données puissent être utilisées à des fins de recherche scientifique.

L'institution s'assure que chaque client pour lequel des données sont transmises à BelRAI ait signé un formulaire de consentement éclairé. Ce formulaire est en ligne avec le formulaire "consentement éclairé" de BelRAI, et mentionne que des données seront échangées avec la banque de données publique BelRAI.

## Art. 10.

L'institution souscrit à ce que la la banque de données publique BelRAI soit la source centrale authentique pour les évaluations BelRAI. Elle veille à ce que les données soient échangées à une fréquence suffisante. La dernière version complète de l'évaluation doit toujours se trouver dans la banque de données BelRAI, et ce dans les 24 heures qui suivent l’enregistrement des données.

## Art. 11.

En cas de rapport d'un incident qui peut avoir été signalé par les patients, membres de la famille, dispensateurs de soins, organisations coordinatrices, associations de patients et consultants en sécurité de l'information,… les règles en vigueur sont les suivantes :

1. Le gestionnaire du circle of trust de BelRAI rapporte l'incident au consultant en matière de sécurité BelRAI.
2. Le gestionnaire du circle of trust de BelRAI examine l'incident avec le consultant en matière de sécurité dans un rôle de conseiller.
3. Si l'incident révèle un grave manquement au niveau de l'application ICT liée au service web BelRAI ou un non respect des conditions fixées dans le cookbook :
	1. le gestionnaire du circle of trust de BelRAI demande au helpdesk BelRAI de supprimer l'application ICT avec effet immédiat de la liste des applications agréées dans le circle of trust de BelRAI.
	2. Le gestionnaire du circle of trust de BelRAI en informe le développeur ICT.
	3. Pour pouvoir adhérer à nouveau au circle of trust de BelRAI, le développeur ICT doit remédier au problème et ensuite parcourir à nouveau toute la procédure pour pouvoir adhérer au circle of trust.
4. Si l'incident révèle un grave manquement au niveau de la politique de sécurité de l'établissement de soins ou un non respect des conditions fixées dans la checklist pour les établissements :
	1. le gestionnaire du circle of trust de BelRAI demande au helpdesk BelRAI de supprimer l'établissement de soins avec effet immédiat de la whitelist circle of trust BelRAI.
	2. Le gestionnaire du circle of trust de BelRAI en informe l'établissement de soins.
	3. Pour pouvoir adhérer à nouveau au circle of trust de BelRAI, l'établissement de soins doit remédier au problème et ensuite parcourir à nouveau toute la procédure pour pouvoir adhérer au circle of trust.

## Art. 12.

La présente convention peut être dénoncée par les deux parties, en respectant un délai de préavis de 3 mois. La résiliation se fait par écrit en mentionnant le motif.

La présente convention a été établie en trois exemplaires, dont chaque partie signataire déclare en avoir reçu un, ainsi qu'un exemplaire destiné à la Commission de protection de la vie privée (CPVP).

En cas d’avenant à la présente convention proposé par l’Etat belge, l’institution dispose d’un délai d'un mois pour s'y opposer. Dans ce cas, la convention prend fin dans un délai de 3 mois qui suivent la date à laquelle l’avenant a été transmis à l’institution.

Fait à Bruxelles,

Pour <nom institution> Pour l'Etat belge

<nom> Pedro Facon

<fonction> Directeur général Soins de santé

1. [Délibération n° 09/018 du 19 mai 2009, dernièrement modifiée le 19 mai 2015, portant sur l’échange de données à caractère personnel relatives à la santé entre les prestataires de soins concernés et la banque de données BelRAI à l’intervention de la plate-forme eHealth](https://www.ehealth.fgov.be/sites/default/files/assets/nl/pdf/sector_committee/2015/09-018-n085-belrai_gewijzigd_op_19_mei_2015.pdf)  [↑](#footnote-ref-1)