

Règles de protection de la vie privée dans BelRAI

1. Politique de protection de la vie privée et consentement éclairé

La politique de protection de la vie privée du projet BelRAI est décrite dans le document "Privacy policy", disponible sur les sites <http://wiki.belrai.org/nl> et <http://wiki.belrai.org/fr>.

Le principe de base de l'accès à l'information sur le site Web BelRAI repose sur le principe "*need to know*" : les soignants peuvent uniquement consulter les informations qui leurs sont strictement nécessaires à propos de leurs clients afin de procéder à leur prise en charge. De plus, l'accès ne peut être accordé aux soignants qu'après avoir obtenu l'autorisation écrite explicite du client, *via* un formulaire de consentement éclairé. Le système ne permet la création d'un nouveau client que si le formulaire de consentement éclairé est signé. Le formulaire de consentement éclairé est normalement gardé par le gestionnaire de client ou son administration.

2. Authentification sur e-Health et vérification

L'inscription d'un utilisateur (soignant) sur BelRAI se déroule via e-health au moyen d'une carte d'identité électronique (eID) ou d'un token.

Il est possible d'y accéder de deux manières : via le site web e-health, qui possède une page sur BelRAI précisant les catégories de soignants pouvant l'utiliser, et via le site web BelRAI. Dans les deux cas, le site web BelRAI renvoie toujours à e-health pour le login propre et la vérification. Ensuite, BelRAI prend le relais.

Un soignant qui utilise BelRAI avec des rôles différents (par exemple un médecin qui possède sa propre clientèle et qui travaille dans un hôpital) doit faire un choix quant au titre sous lequel il veut travailler. Ses droits d'accès à BelRAI seront adaptés en fonction de ce choix.

Lors de l'inscription, e-health contrôle la qualification de l'utilisateur à partir de sources authentiques connues. Il est donc vérifié que l'utilisateur est bien un médecin, un infirmier, ... reconnu. Une fois ces sources consultées et le login vérifié, e-health renvoie les informations disponibles concernant l'utilisateur vers BelRAI. BelRAI recoupe ces informations avec ses propres rôles afin de déterminer quel accès au système sera accordé à l'utilisateur.

Toute personne reconnue comme soignant par e-health aura donc accès à BelRAI. Pour l'instant, ce n'est le cas que pour les médecins et les infirmiers. Par la suite, d'autres rôles seront ajoutés, dès que e-health pourra vérifier ceux-ci dans ses sources authentiques.

3. Accès aux clients

Un accès est donné aux soignants sur base de leur rôle (vérifié par e-health) dans le processus de soins.

La politique d'accès de BelRAI permet qu'une flexibilité soit possible entre les différentes situations de soins ("intra muros" et "inter muros"), tout en garantissant la confidentialité des données des clients.

3.1 Gestionnaire de client

Le rôle de « gestionnaire de client » est une fonction spécifique qu'un soignant remplit pour un client. Il s'agit d'une sorte de relation de confiance entre un client et un soignant, dans laquelle le premier donne sa confiance au second pour gérer ses données dans BelRAI et veiller à la protection de sa vie privée.

Le gestionnaire de client est la seule personne qui peut modifier le profil du client dans le système (ses données personnelles comme sa date de naissance, son état civil, son niveau d'éducation, etc.).

Il est aussi le seul à déterminer quels soignants auront accès au client. Il peut le faire en rendant le client membre de groupes et/ou en donnant à certains soignants un accès individuel à ce client.

En d'autres termes : un soignant aura accès aux données d'un client seulement s'il est membre du même groupe que le client ou s'il a obtenu un accès individuel au client.

Le gestionnaire de client peut à tout moment accorder ou retirer l'accès aux données d'un client.

Chaque client possède, en principe, un gestionnaire de client, mais il peut aussi en avoir plusieurs. Il appartient aussi au gestionnaire de client de déterminer si d'autres soignants peuvent également être ou non gestionnaires de client pour « son client ».

3.2 Gestionnaire de groupe

Clients et soignants peuvent appartenir à des groupes qui peuvent être structurés hiérarchiquement. Les soignants d'un groupe ont accès aux clients de leur groupe et de ses groupes sous-jacents. C'est le gestionnaire de groupe qui peut rendre un soignant membre d'un groupe.

L'accès basé sur les groupes est donc une combinaison des fonctions de confiance « gestionnaire de client » (à quels groupes peut appartenir mon client) et « gestionnaire de groupe » (quels soignants peuvent appartenir à mon groupe), dans laquelle le gestionnaire de client compte sur le fait que le gestionnaire de groupe prend la responsabilité de n'accepter dans son groupe que les soignants qui sont strictement nécessaires au processus de soins.

3.3 Responsable de questionnaire

C'est, avec le gestionnaire de client et le gestionnaire de groupe, la troisième fonction spécifique qu'un soignant peut remplir dans le système. Le responsable de questionnaire est le soignant responsable de la validation et de la clôture du questionnaire. Le responsable de questionnaire peut encore, après expiration de la date de fin d'évaluation, répondre aux questions, décider d'une réponse entre d'éventuelles réponses contradictoires, laisser calculer les résultats et finalement fermer le questionnaire.

3.4 Résumé

La figure ci-dessous présente de manière schématique la hiérarchie de groupe et la politique d'accès dans BelRAI.

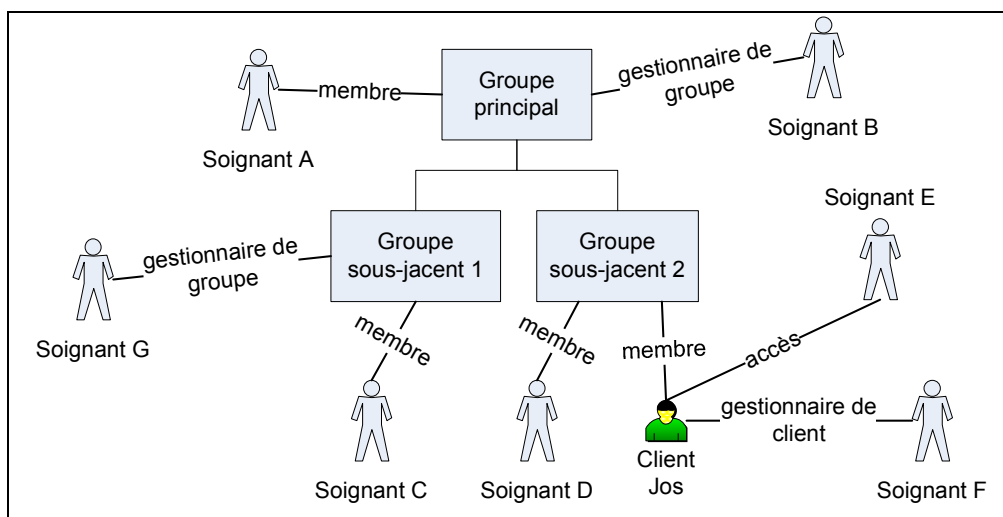


Figure 1: politique d'accès dans BelRAI

Cette figure montre un groupe principal et deux groupes sous-jacents. Le soignant B est gestionnaire de groupe du groupe principal et a donc décidé que le soignant A en était membre et que les groupes 1 et 2 en étaient les groupes sous-jacents.

Le soignant F est gestionnaire de client de notre client Jos. Après lui avoir fait signer le « formulaire de consentement éclairé », F a décidé que Jos était membre du sous-groupe 2.

Les personnes suivantes, figurant dans le schéma, ont accès au client Jos :

- Le soignant F, parce qu’il est gestionnaire de client
- Le soignant D parce qu’il est membre du même groupe (sous-groupe 2)
- Le soignant E parce que le gestionnaire de client lui a donné un accès individuel au dossier de Jos
- Les soignants A et B (gestionnaire de groupe) parce qu’ils sont membres du groupe principal

Les personnes suivantes n’ont pas accès au client Jos :

- Le soignant C parce qu’il n’est pas membre du sous-groupe 2
- Le soignant G (gestionnaire de groupe) parce qu’il n’est pas membre du sous-groupe 2

3.5 Exemple de scénario

Jos a atteint l’âge de 80 ans. Il habite encore dans sa maison mais a été provisoirement admis à l’hôpital pour un problème cardiaque. Pour pouvoir réaliser une première évaluation RAI, l’infirmier en chef du service de Cardiologie a téléchargé et imprimé un formulaire de « consentement éclairé » sur l’application web BelRAI. Il a expliqué à Jos ce qu’il voulait faire avec BelRAI et ils ont parcouru ensemble le formulaire que Jos a signé. Jos a choisi son médecin généraliste comme gestionnaire de client.

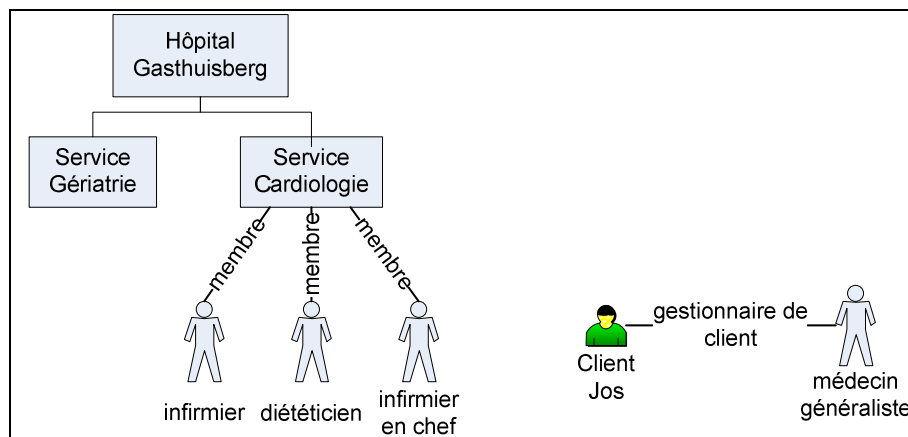


Figure 2: scénario étape 1

L’infirmier en chef crée Jos en tant que nouveau client dans BelRAI et sélectionne son médecin généraliste comme gestionnaire de client. Il transmet (par la poste) à celui-ci le formulaire de « consentement éclairé » et lui demande d’inscrire Jos dans le groupe du service de Cardiologie de son hôpital.

Le médecin généraliste se connecte au système BelRAI et clique sur « mes clients ». Il voit que Jos en fait partie. Il va à la page de détails de Jos et, ensuite, à la page de gestion de groupe. Il ajoute Jos comme membre du groupe « Service de Cardiologie », dans l’hôpital Gasthuisberg.

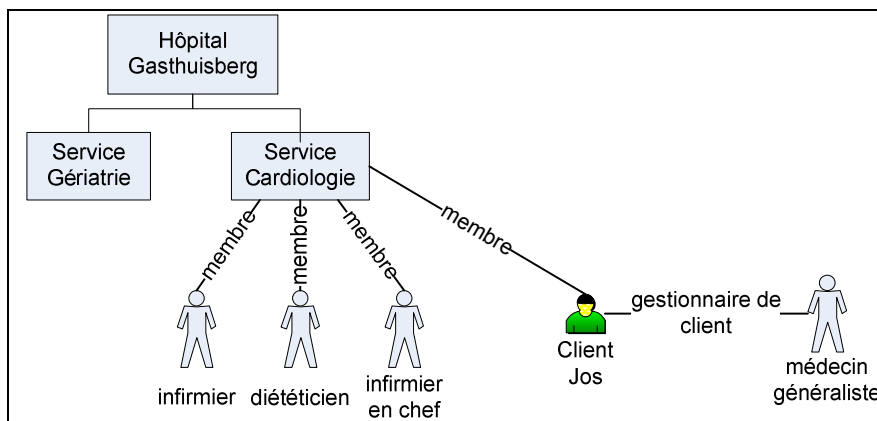


Figure 3: scénario étape 2

L'infirmier, le diététicien et l'infirmier en chef du service de Cardiologie ont dorénavant accès au client Jos dans BelRAI. L'infirmier en chef peut donc commencer un nouveau questionnaire RAI pour Jos et le faire compléter par les personnes chargées de lui prodiguer des soins (voir ci-dessus).

Jos peut quitter l'hôpital après 2 semaines, mais un infirmier à domicile doit encore lui prodiguer des soins deux fois par semaine, pendant deux mois. Après un mois, son infirmier à domicile, employé des « Soins à domicile » de Louvain, doit compléter un formulaire RAI pour lui. Pour ce faire, il demande au médecin généraliste de Jos d'inclure ce dernier dans le groupe « Soins à domicile » de Louvain. L'infirmier à domicile a maintenant accès aux données de Jos dans le système BelRAI. Puisque Jos n'est plus à l'hôpital, son médecin généraliste peut l'exclure du groupe « Service de Cardiologie ».

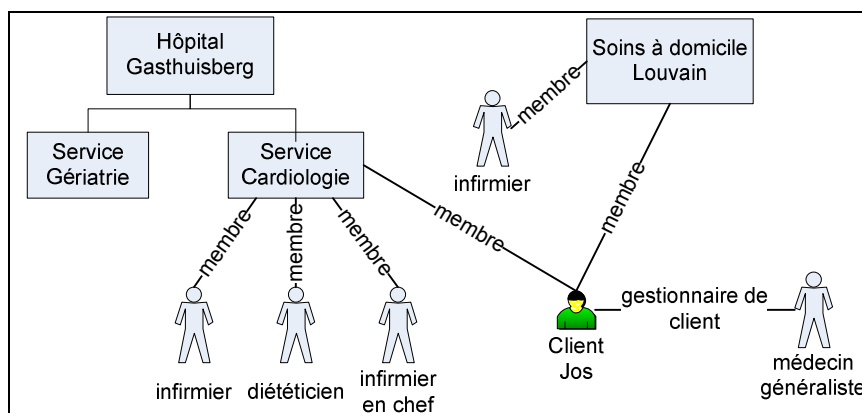


Figure 4: scénario étape 3

4. Accès en fonction des rôles

“Avoir accès” à un client, tel que décrit en 3.2, est seulement un premier filtre de sécurité dans le système BelRAI. En plus de ce filtre, c'est le rôle du soignant dans le processus de soins qui détermine ce que ce soignant peut faire avec le client dans le système.

Chaque soignant a, dans le système, un rôle déterminé qui est relié à sa fonction dans le processus de soins. Cet accès, basé sur le rôle, détermine pour chaque soignant :

- Quelles opérations il peut exécuter sur le site Web (par exemple, commencer un questionnaire, lire les résultats, créer un nouveau client, etc.).
- Quelles types d'informations il peut consulter sur le client (par exemple médicales, sociales, comportementales, etc.).

4.1 Accès aux opérations

Une première matrice d'accès détermine quels rôles ont accès à quelles opérations dans le système.

Cette matrice est déterminée pour tout le système et ces droits d'accès ne peuvent pas être modifiés.

Rôle \ Opération	Examiner le questionnaire	Calculer les résultats	CMS	Créer des clients	Créer des groupes	Débuter un questionnaire	Gérer les rôles	Créer des soignants
Administrateur du système	v	v	v	v	v	v	v	v
Animateur	v	v		v	v	v		
Aidant informel	v	v		v		v		
Assistant social	v	v		v		v		
Chercheur	v	v		v	v	v		v
Dentiste	v	v		v		v		
Diététicien	v	v		v		v		
Directeur	v	v		v	v	v		v
Ergothérapeute	v	v		v		v		
Infirmier	v	v		v		v		
Kinésithérapeute	v	v		v		v		
Logopède	v	v		v		v		
Médecin	v	v		v	v	v		v
Pharmacien	v	v		v		v		
Podologue	v	v		v		v		
Psychologue	v	v		v		v		
Soignant	v	v		v		v		
Visiteur	v	v		v		v		

Tableau 1: matrice rôles/opérations

NOTE: chaque "médecin" et "infirmier(-ère)", vérifié par e-health, aura en premier lieu accès au site de production. Ceci sera étendu, dans le futur, aux autres rôles.

Tous les rôles ont accès au site-test.

4.2 Accès aux types d'informations

Une deuxième matrice d'accès détermine quels rôles ont accès à quels types d'informations dans le système.

Dans la matrice, il est déterminé, pour tout le système, quels rôles standards ont accès à quels types d'informations et si cet accès peut éventuellement être modifié pour un questionnaire spécifique. Pour remplir un questionnaire RAI spécifique, on peut donc décider –si nécessaire et à l'intérieur de limites déterminées au préalable- d'étendre l'accès à certains types d'informations déterminés ou de le limiter pour des rôles déterminés.

On peut ainsi, par exemple, déterminer qu'un diététicien n'a pas accès aux questions médicales et que cet accès n'est pas modifiable. Dans ce cas, le diététicien ne peut jamais remplir de questions médicales. On pourrait instituer qu'un soignant n'a pas accès aux questions médicales mais que ceci est modifiable. Dans ce cas, celui qui commence un questionnaire pour un client déterminé peut décider que, dans cette situation, un soignant précis reçoit quand même l'accès aux questions médicales.

Type d'information Rôle	Nom		Données personnelles		Santé mentale		Cognition, communication, humeur et comportement, bien-être psychosocial et détente		Fonctions corporelles et continence	
	A	M	A	M	A	M	A	M	A	M
Administrateur du système	v	v								
Aidant informel	v	v								
Animateur	v	v		v		v	v	v	v	v
Assistant social	v	v	v	v		v	v	v		v
Chercheur	v	v								
Dentiste	v	v		v		v		v		v
Diététicien	v	v		v		v	v	v	v	v
Directeur	v	v								
Ergothérapeute	v	v		v		v	v	v	v	v
Infirmier	v	v		v		v	v	v	v	v
Kinésithérapeute	v	v		v		v	v	v	v	v
Logopède	v	v		v		v	v	v	v	v
Médecin	v	v	v	v	v	v	v	v	v	v
Pharmacien	v	v		v		v		v		v
Podologue	v	v		v		v	v	v	v	v

Psychologue	v	v		v	v	v	v	v	v	v
Soignant	v	v		v		v	v	v	v	v
Visiteur	v	v								

Tableau 2: matrice rôles/types d'informations (A=Accès, M=Modifiable) PARTIE 1

Type d'information Rôle	Syndrômes et médicaments		Problèmes de santé, buccaux et alimentaires		Peau		Traitements et procédures		Soins spécifiques, moyens et mesures	
	A	M	A	M	A	M	A	M	A	M
Administrateur du système										
Aidant informel										
Animateur		v		v		v		v		v
Assistant social		v		v		v		v		v
Chercheur										
Dentiste	v	v	v	v		v		v	v	v
Diététicien		v	v	v		v		v		v
Directeur										
Ergothérapeute		v	v	v	v	v		v		v
Infirmier	v	v	v	v	v	v	v	v	v	v
Kinésithérapeute		v	v	v	v	v		v		v
Logopède		v		v		v		v	v	v
Médecin	v	v	v	v	v	v	v	v	v	v
Pharmacien	v	v		v		v		v	v	v
Podologue		v		v	v	v		v		v
Psychologue	v	v	v	v	v	v	v	v	v	v
Soignant		v	v	v	v	v		v		v
Visiteur										

Tableau 3: matrice rôles/types d'informations (A=Accès, M=Modifiable) PARTIE 2

Type d'information Rôle	Responsabilité et dispositions		Aide et entourage		Sortie et informations de retour		Informations d'évaluation	
	A	M	A	M	A	M	A	M
Administrateur du système								
Aidant informel								
Animateur		v	v	v		v		v
Assistant social	v	v	v	v	v	v		v
Chercheur								
Dentiste		v		v		v		v
Diététicien		v	v	v		v		v
Directeur								
Ergothérapeute		v	v	v		v		v
Infirmier	v	v	v	v	v	v	v	v
Kinésithérapeute		v	v	v		v		v
Logopède		v	v	v		v		v
Médecin	v	v	v	v	v	v	v	v
Pharmacien		v		v		v		v
Podologue		v	v	v		v		v
Psychologue	v	v	v	v	v	v	v	v
Soignant		v	v	v		v		v
Visiteur								

Tableau 4: matrice rôles/types d'informations (A=Accès, M=Modifiable) PARTIE 3

4.3 Accès aux rôles

Une troisième et dernière matrice d'accès détermine quels rôles les utilisateurs peuvent créer en fonction des différents rôles repris dans le système BelRAI. Dans l'exemple repris ci-dessous, un médecin peut créer des utilisateurs avec tous les rôles mais un kinésithérapeute ne peut créer de nouveaux utilisateurs qu'avec d'autres kinésithérapeutes. De cette façon, on évite que des utilisateurs octroient, injustement, à eux-mêmes ou à d'autres, des droits d'accès plus importants que celui que leur rôle dans le processus de soins ne leur accorde.

Rôle nouvel utilisateur Rôle utilisateur actuel	Administrateur du système	Aidant informel	Animateur	Assistant social	Chercheur	Dentiste
Administrateur du système	v	v	v	v	v	v
Aidant informel		v				
Animateur			v			
Assistant social				v		
Chercheur		v		v	v	v
Dentiste						v
Diététicien						
Directeur		v		v	v	v
Ergothérapeute						
Infirmier						
Kinésithérapeute						
Logopède						
Médecin						
Pharmacien						
Podologue						
Psychologue						
Soignant						
Visiteur						

Tableau 5: matrice rôles/rôles PARTIE 1

Rôle nouvel utilisateur	Diététicien	Directeur	Ergothérapeute	Infirmier	Kinésithérapeute	Logopède
Rôle utilisateur actuel						
Administrateur du système	v	v	v	v	v	v
Aidant informel						
Animateur						
Assistant social						
Chercheur		v		v		
Dentiste						
Diététicien	v					
Directeur		v		v		
Ergothérapeute			v			
Infirmier				v		
Kinésithérapeute					v	
Logopède						v
Médecin						
Pharmacien						
Podologue						
Psychologue						
Soignant						
Visiteur						

Tableau 6: matrice rôles/rôles PARTIE 2

Rôle nouvel Utilisateur						
Rôle utilisateur actuel	Médecin	Pharmacien	Podologue	Psychologue	Soignant	Visiteur
Administrateur du système	v	v	v	v	v	v
Aidant informel						
Animateur						
Assistant social						
Chercheur	v					
Dentiste						
Diététicien						
Directeur	v					
Ergothérapeute						
Infirmier						
Kinésithérapeute						
Logopède						
Médecin	v					
Pharmacien		v				
Podologue			v			
Psychologue				v		
Soignant					v	
Visiteur						v

Tableau 6 : matrice rôles/rôles PARTIE 3

4.4 Exemple de scénario

L'infirmier en chef de la figure 3 commence un nouveau questionnaire et devient lui-même responsable du questionnaire. Il détermine que le soignant peut remplir les questions de tout type, à part les médicales, et que le diététicien peut compléter uniquement les questions sur le comportement alimentaire. En tant que responsable du questionnaire, l'infirmier en chef peut lui-même compléter toutes les questions.

Après que chacun ait complété ses questions, l'infirmier en chef calcule les résultats et clôture le questionnaire. Le soignant peut maintenant consulter les résultats parce qu'il a accès à cette fonction mais le diététicien ne le peut pas. Le diététicien peut seulement revoir les réponses des questions auxquelles il a répondu.

5. Encryptage

Les données du client qui sont échangées entre les soignants via le site web BelRAI sont cryptées, de manière à ce qu'il soit impossible à quelqu'un d'extérieur (par exemple à quelqu'un qui écoute) de savoir quelles sont les données qui ont été envoyées. Le cryptage est appliqué sur base du protocole SSL.

Les données du client sont conservées de manière cryptée dans la base de données BelRAI, de manière à ce que les personnes qui ont directement accès à la base de données (par exemple les informaticiens qui développent et entretiennent l'application web) ne puissent consulter aucune donnée personnelle.

6. Droit d'accès et de correction

Un client a le droit de consulter ses propres données conservées dans BelRAI. Pour cela, le mieux est de prendre contact avec le gestionnaire de client. Par conséquent, si le client demande l'accès à ses données, il faut donc le renvoyer vers son gestionnaire de client. Dans le cas où le client est représenté (par exemple en cas d'incapacité de décision ou de fait), seul le représentant peut demander l'accès aux données du client (et pas le client lui-même).

On peut vérifier quels soignants ont concrètement accès à quelles données d'un client sur base de la liste des « personnes compétentes ». Typiquement, c'est le gestionnaire de client qui peut le réclamer, que le client le demande ou non.

Un soignant a également un droit d'accès à ses propres données, qui sont traitées au sein de l'application. Il a aussi le droit de les modifier. Ceci signifie que, le cas échéant, il peut faire corriger gratuitement toutes les données personnelles le concernant si elles sont incorrectes ou incomplètes.

Ces informations sont reprises dans le document "Privacy policy".

7. Consultant en sécurité

Un consultant en sécurité est désigné pour toute l'application et pour chaque groupe individuel. Cette personne veille à la stricte application de la politique de protection de la vie privée dans son groupe et peut, entre autres, vérifier les accès et signaler d'éventuels abus. Une condition essentielle est que le consultant en sécurité n'ait aucun accès aux dossiers individuels des clients.

8. Enregistrement

Toutes les actions concernant un client, réalisées en ligne par les soignants, sont enregistrées. Par exemple, le soignant A a démarré un questionnaire pour un client, le soignant B a consulté certaines informations concernant un client, etc.

L'administrateur du système et/ou le consultant en sécurité peut consulter ces actions pour détecter d'éventuelles atteintes à la vie privée. Des outils sont disponibles pour détecter de possibles abus dans les actions enregistrées.

Les actions suivantes sont enregistrées dans la banque de données :

- Toutes les actions des utilisateurs qui peuvent avoir une influence sur la protection de la vie privée des clients. Les actions concernant les clients et les questionnaires sont considérées comme étant plus sensibles par rapport à la protection de la vie privée que les actions concernant les soignants ; les actions considérées comme les moins sensibles étant celles concernant les groupes.
- Toutes les actions qui adaptent l'accès des soignants aux clients, aux données et aux questionnaires.
- Les adaptations de l'instrument.

Liste détaillée des actions enregistrées :

- Clients :
 - Créer un nouveau client
 - Regarder les détails
 - Demander la liste de tous les questionnaires (pour un client)
 - Consulter le profil complet
 - Modifier le profil
 - Modifier le(s) gestionnaire(s) de client
 - Ajouter un soignant en tant que gestionnaire de client
 - Ecarter un soignant en tant que gestionnaire de client
 - Modifier l'accès individuel d'un soignant
 - Donner à un soignant un accès individuel à un client
 - Interdire à un soignant l'accès individuel à un client
 - Modifier l'adhésion d'un membre à un groupe
 - Rendre un soignant membre d'un groupe
 - Interdire à un soignant de faire partie d'un groupe
 - Consulter les statistiques individuelles
- Questionnaires :
 - Démarrer un nouveau questionnaire
 - Adapter le questionnaire existant (par exemple, modifier la date limite de l'évaluation ou les droits d'accès) (cette fonction n'existe pas encore)
 - Consulter les détails
 - Compléter une section du questionnaire
 - Consulter les réponses aux questions d'une section d'un questionnaire (ses propres réponses ou celles des autres)
 - Clôturer un questionnaire
 - Consulter les résultats
- Soignants (utilisateurs) :
 - Login réussi
 - Mauvais login
 - Déconnexion
 - Création d'un nouveau soignant
 - Consulter les détails
 - Réclamer une liste de tous les questionnaires (pour lesquels le soignant est concerné)
 - Consulter le profil complet
 - Modifier le profil
 - Modifier l'appartenance à un groupe

- Groupes :
 - Créer un nouveau groupe
 - Consulter les détails
 - Modifier le profil (nom + type)
 - Modifier le groupe principal
 - Exclure du groupe principal
 - Modifier le(s) gestionnaire(s) de groupe :
 - Autoriser un soignant comme gestionnaire de groupe
 - Interdire un soignant comme gestionnaire de groupe
- Modification des matrices d'accès :
 - Matrice "Accès des rôles aux questions types"
 - Matrice "Accès des rôles aux opérations du système"
 - Matrice "Accès des rôles aux autres rôles"
- Modification du contenu de l'instrument via le système CMS
- Modification du contenu administratif via le système CMS (cette fonction n'existe pas encore)

Les informations suivantes sont enregistrées :

- Toujours :
 - o Précision temporelle de l'enregistrement de l'action (date, heure, minutes, secondes)
 - o Adresse IP de l'utilisateur
 - o Action qu'a réalisée ou qu'a voulu réaliser l'utilisateur
 - o Si le login est correct : Information au sujet de l'utilisateur connecté :
 - Database ID
 - Rôle
 - Numéro de Registre National
 - Nom et prénom (backup d'identification si l'enregistrement a disparu de la base de données)
- Si l'action concerne un utilisateur : Informations au sujet de l'utilisateur concerné :
 - Database ID
 - Rôle
 - Numéro de Registre National
 - Nom et prénom (backup d'identification si l'enregistrement a disparu de la base de données)
- Si l'action concerne un client : Informations au sujet du client concerné :
 - Database ID
 - Nom et prénom (backup d'identification si l'enregistrement a disparu de la base de données)
 - Date et lieu de naissance (backup d'identification)
 - Numéro de carte SIS (backup d'identification)

- Si l'action concerne un questionnaire : Informations au sujet du questionnaire concerné :
 - Database ID
 - Identification du client concerné (voir ci-dessus)
 - Section consultée ou complétée (si d'application)
 - Lors de l'encodage : les champs que les utilisateurs ont adaptés (ancienne et nouvelle valeur) (Note : ceci n'est provisoirement pas développé, étant donné qu'il n'est pas certain qu'il sera nécessaire que l'enregistrement des données soit aussi détaillé)
 - Lors de la modification des droits d'accès ou de la date limite : nouvelle date limite, anciens et nouveaux droits d'accès
- Si l'action concerne un groupe : Informations au sujet du groupe concerné :
 - Database ID
 - Nom (backup d'identification)
- Si l'action concerne les droits d'accès :
 - Identification des droits d'accès refusés (cases décochées dans la matrice)
 - Identification des droits d'accès ajoutés (cases cochées dans la matrice)

9. Backup et surveillance physique

Le serveur BelRAI se trouve dans les bâtiments de la K.U.Leuven, Faculté des Sciences sociales, Mediacentrum, Parkstraat 45, 3000 Leuven, dans un local fermé, sous la protection d'un dispositif d'alarme.

Des backups ont lieu chaque nuit vers un serveur du service Ludit, le service Informatique de la K.U.Leuven, qui se trouve dans un bâtiment séparé à Heverlee.