JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 909 du 28 décembre 2019

Règlement grand-ducal du 6 décembre 2019 précisant les modalités et conditions de mise en place du dossier de soins partagé.

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,

Vu l'article 60*quater* du Code de la sécurité sociale ;

Vus les avis de la Chambre des salariés, de la Chambre des fonctionnaires et employés publics, ainsi que l'avis commun de la Chambre des métiers et de la Chambre de commerce ;

L'avis de la Chambre d'agriculture ayant été demandé ;

Vu l'avis du Collège médical ;

Vu l'avis du Conseil supérieur de certaines professions de santé ;

Vu l'avis de la Commission nationale pour la protection des données ;

Notre Conseil d'État entendu ;

Sur le rapport de Notre Ministre de la Sécurité sociale et de Notre Ministre de la Santé et après délibération du Gouvernement en conseil ;

Arrêtons :

Art. 1er. Définitions

Pour l'application du présent règlement grand-ducal, on entend par :

1° « Agence » : le groupement d'intérêt économique dénommé « Agence eSanté - Agence nationale des informations partagées dans le domaine de la santé » ;
2° « Application dossier de soins partagé » : l'application de la plateforme électronique nationale d'échange et de partage de données de santé visée à l'article 60*ter* du Code de la sécurité sociale, ci-après « plateforme », permettant d'accéder, moyennant un compte personnel et dans les conditions du présent règlement grand-ducal, à un dossier de soins partagé ;
3° « Introducteur d'une donnée » : la personne qui introduit une donnée au sein du dossier de soins partagé ;
4° « Patient » : toute personne physique qui cherche à bénéficier ou bénéficie de soins de santé, tel que prévu par l'article 2 de la loi modifiée du 24 juillet 2014 relative aux droits et obligations du patient ;
5° « Professionnel de santé » : toute personne physique exerçant légalement une profession réglementée du domaine de la santé et tout professionnel de santé, tout établissement hospitalier, ainsi que tout prestataire de soins, exerçant légalement sa profession en dehors du secteur hospitalier visé par l'alinéa second de l'article 61 du Code de la sécurité sociale, tels que prévus à l'article 2 de la loi précitée du 24 juillet 2014 ;
6° « Titulaire » : le patient auquel le dossier de soins partagé est lié.

Art. 2. Création du dossier de soins partagé

(1) Un dossier de soins partagé est créé par l'Agence pour le patient dès son affiliation à l'assurance maladie.

(2) Le patient non affilié bénéficiant de soins de santé par un professionnel de santé sur le territoire national peut demander la création d'un dossier de soins partagé moyennant une demande adressée à l'Agence.

(3) Dès la création du dossier de soins partagé, l'Agence informe par écrit le titulaire :

1° de la création ;
2° des modalités d'activation et de fermeture du dossier de soins partagé ;
3° de ses identifiants de connexion personnels ;

4° du fonctionnement du dossier de soins partagé, en ce inclus les droits d'accès et leur gestion, les mesures de sécurité, les principes d'alimentation, de traçabilité et de traitement des données du dossier de soins partagé ;
5° de son droit d'opposition au partage de données au sein d'un dossier de soins partagé ;
6° de ses droits d'accès et d'écriture visés à l'article 6 ;
7° du contenu du dossier de soins partagé au moment de son activation.

(4) Dans le cadre de ses missions d'organe central de la plateforme et de responsable du traitement au sens de l'article 60*ter*, paragraphe 4, du Code de la sécurité sociale, l'Agence fournit les informations visées à l'article 14, paragraphes 1er et 2, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ci-après « règlement (UE) 2016/679 ».

(5) Le dossier de soins partagé ne se substitue pas au dossier que tient chaque professionnel de santé ou chaque établissement de santé, quel que soit son mode d'exercice, dans le cadre de la prise en charge d'un patient.

Art. 3. Activation du dossier de soins partagé et accès par le titulaire

(1) Le titulaire dispose d'un droit d'opposition au partage dont il est informé en vertu de l'article 2, paragraphe 3, point 5°. S'il exerce ce droit d'opposition, le dossier de soins partagé ne devient pas actif et est supprimé.

Le dossier de soins partagé est accessible par voie électronique depuis la plateforme.

Pour accéder à son dossier de soins partagé, le titulaire doit préalablement activer un compte sur la plateforme et se connecter à l'application dossier de soins partagé moyennant ses identifiants de connexion qui lui ont été adressés par l'Agence. Ces identifiants de connexion sont strictement personnels.

(2) À compter de l'activation du compte par le titulaire sur la plateforme, le dossier de soins partagé peut être consulté et alimenté par le titulaire.

(3) À défaut d'activation de son compte par le titulaire endéans un délai de trente jours à compter de l'envoi des informations visées à l'article 2, paragraphe 3, le dossier de soins partagé peut être consulté et alimenté par les professionnels de santé intervenant dans la prise en charge du titulaire, conformément à leurs droits d'accès et d'écriture, au moyen de l'activation de leur compte telle que prévue à l'article 5.

Une notification est envoyée au titulaire par tout moyen pour l'informer du premier accès d'un professionnel de santé à son dossier de soins partagé.

Art. 4. Fermeture et suppression du dossier de soins partagé

(1) Le titulaire d'un dossier de soins partagé peut, à tout moment, fermer son dossier de soins partagé moyennant l'application dossier de soins partagé ou par demande adressée à l'Agence.

(2) Endéans un délai de dix ans après la fermeture du dossier de soins partagé, le titulaire peut procéder à sa réouverture moyennant l'application dossier de soins partagé ou par demande adressée à l'Agence. En cas de réouverture, le dossier de soins partagé contient les données y incluses au moment de la fermeture.

(3) À défaut de réouverture endéans le délai mentionné au paragraphe 2, les données du dossier de soins partagé sont supprimées dix ans après la fermeture du dossier de soins partagé.

(4) À défaut d'activité dans le dossier de soins partagé constaté par l'Agence, il est fermé dix ans après le dernier accès.

(5) En cas de décès du titulaire, le dossier de soins partagé est fermé dès transmission à l'Agence de la date du décès par le Centre commun de la sécurité sociale ou, dès réception par l'Agence d'un certificat de décès.

(6) À compter de la fermeture, les données du dossier de soins partagé sont rendues inaccessibles et sont archivées par le biais de l'application dossier de soins partagé.

Art. 5. Accès au dossier de soins partagé par les professionnels de santé

(1) Sans préjudice du droit d'opposition du titulaire et de la procédure d'activation, visés à l'article 3, le professionnel de santé intervenant dans la prise en charge du titulaire peut accéder au dossier de soins partagé pour le consulter et l'alimenter.

En vue d'accéder au dossier de soins partagé, le professionnel de santé doit préalablement activer son compte sur la plateforme moyennant ses identifiants personnels de connexion et il se connecte à l'application dossier de soins partagé :

1° s'il exerce dans un cabinet individuel, à partir de la plateforme ou à partir d'un programme informatique conforme aux dispositions de l'article 11, paragraphe 2 ;
2° s'il exerce au sein d'une collectivité de santé, à partir du programme informatique utilisé par la collectivité et conforme aux dispositions de l'article 11, paragraphe 2.

(2) Le compte sur la plateforme, visé au paragraphe 1er, est créé par l'Agence sur demande du professionnel de santé ou de la collectivité de santé pour les professionnels de santé qui y exercent et qui sont inscrits dans l'annuaire référentiel d'identification des professionnels de santé.

Dès la création de son compte sur la plateforme, l'Agence informe le professionnel de santé :

1° de cette création ;
2° des modalités d'activation et de fermeture du compte ;
3° de ses identifiants de connexion personnels ;
4° du fonctionnement du compte et de l'application dossier de soins partagé, en ce inclus les droits d'accès, les mesures de sécurité, les principes d'alimentation, de traçabilité et de traitement des données du dossier de soins partagé.

Art. 6. Droits d'accès, d'écriture et d'effacement du titulaire

(1) Le titulaire a un droit de consultation de toutes les données figurant dans son dossier**.**

(2) En outre, à partir de son dossier de soins partagé, le titulaire peut :

1° inscrire des informations et verser des données relatives à sa santé ou pertinentes pour sa prise en charge dans l'espace d'expression qui lui est réservé pour les porter a`la connaissance des professionnels de santé ;
2° sans préjudice des dispositions légales applicables, indiquer ses volontés en matière de don d'organes, de directives anticipées ou une information relative à des dispositions de fin de vie.

(3) Il peut également, à partir de son dossier de soins partagé, modifier les droits d'accès applicables par défaut tels qu'ils sont fixés à l'article 7, paragraphe 1er :

1° en interdisant l'accès à son dossier intégral à un ou plusieurs professionnels de santé qu'il désigne, en apportant la précision « niveau privé » ;
2° en rendant inaccessibles certaines données spécifiques à un ou plusieurs professionnels de santé qu'il désigne, en leur accordant un niveau « restreint ».

Lors de sa prise en charge médicale, le titulaire peut s'opposer au versement d'une donnée à son dossier de soins partagé.

Le titulaire est informé par l'application dossier de soins partagé et, le cas échéant, par son médecin référent ou un autre professionnel de santé, des risques éventuels encourus pour sa santé du fait de l'exercice de ses droits de restriction d'accès.

Le titulaire dispose également d'un droit à l'effacement de ses données personnelles conformément à l'article 17 du règlement (UE) 2016/679, qu'il exerce auprès du responsable du traitement.

(4) Le titulaire peut modifier à tout moment les choix et indications visés aux paragraphes 2 et 3.

(5) Le titulaire a le droit d'obtenir dans les meilleurs délais la rectification des données inexactes ou incomplètes dans son dossier de soins partagé soit par le professionnel de santé auteur de la donnée, soit par l'Agence.

Art. 7. Droits d'accès et d'écriture des professionnels de santé

(1) Sans préjudice des dispositions de l'article 6, paragraphe 3, les droits d'accès et d'écriture maximaux par catégorie de données des professionnels de santé intervenant dans la prise en charge du titulaire, ainsi que la durée des accès sont déterminés par défaut par la matrice d'accès figurant à l'annexe 1. Cette matrice est établie en fonction de la profession du professionnel de santé, du contexte de prise en charge et de la catégorie de données.

Le classement d'un type de donnée au sein d'une catégorie de données et d'éventuelles restrictions d'accès et d'écriture à certains types de données à l'intérieur d'une même catégorie de données se font conformément aux procédures déterminées par l'Agence.

(2) Seuls les professionnels de santé intervenant dans la prise en charge médicale du titulaire peuvent accéder à son dossier de soins partagé et y verser une donnée, pendant la durée de cette prise en charge et dans les limites fixées par la matrice d'accès visée au paragraphe 1er.

(3) Au moment de la collecte des données du titulaire, le professionnel de santé fournit les informations visées à l'article 13, paragraphes 1er et 2, du règlement (UE) 2016/679 ».

(4) Dès transmission de l'arrêt temporaire ou définitif de l'autorisation d'exercer la profession par le ministre ayant la Santé dans ses attributions, les droits d'accès et d'écriture du professionnel de santé sont retirés. L'Agence en informe le titulaire du dossier de soins partagé.

Art. 8. Traçabilité des accès et des actions

(1) Tout accès et toute action réalisés sur le dossier de soins partagé sont tracés et conservés. Les accès et actions réalisés sont datés et comportent l'identification de la personne qui a consulté, alimenté ou rendu inaccessible une ou plusieurs données ainsi que le contexte de son intervention, indépendamment du fait que cette personne est un professionnel de santé individuel ou fait partie d'une collectivité de santé.

Les données de journalisation qui comprennent les traces et logs fonctionnels permettant la traçabilité des accès et actions au sein d'un dossier de soins partagé par l'application dossier de soins partagé, suivent le même cycle de vie que les données auxquelles elles se rapportent.

(2) Le titulaire peut consulter une vue « historique des accès » dans laquelle il voit l'ensemble des traces des accès et des actions relatives aux données de son dossier de soins partagé.

(3) La consultation des traces des accès et des actions susvisées se fait par l'intermédiaire de l'application dossier de soins partagé.

Art. 9. Délai de versement des données au dossier de soins partagé par le professionnel de santé

(1) Un professionnel de santé, intervenant dans la prise en charge médicale du titulaire, détenteur d'une donnée qu'il estime utile et pertinente au sens de l'article 60*quater*, paragraphe 2 du Code de la sécurité sociale, verse celle-ci au dossier de soins partagé dans un délai raisonnable après la prise de connaissance de cette donnée ou après son premier accès au dossier de soins partagé si cette donnée est antérieure à son activation.

(2) En cas de demande du titulaire de verser une donnée au dossier de soins partagé, le professionnel de santé l'introduit, conformément à ses droits d'accès et d'écriture, endéans un délai de quinze jours à compter de cette demande.

(3) Sans préjudice du paragraphe 1er, les données utiles et pertinentes suivantes sont versées au dossier de soins partagé au plus tard quinze jours après la fin de la prise en charge par le professionnel de santé qui en est l'auteur :

1° les résultats d'analyses de biologie médicale ;
2° les résumés cliniques et les rapports médicaux de sortie ;
3° les rapports d'images radiologiques ou de toute autre imagerie médicale ;
4° le résumé patient.

(4) La Caisse nationale de santé communique à l'Agence dans un délai raisonnable après leur réception les informations administratives relatives à la désignation, à la reconduction, au changement et au remplacement du médecin référent par le titulaire afin que celles-ci soient retranscrites au dossier de soins partagé.

(5) Les données sont conservées au dossier de soins partagé pendant dix ans à compter de leur versement au dossier. À l'échéance, l'Agence procède à la destruction des données par le biais de l'application dossier de soins partagé.

Par dérogation à l'alinéa 1er, le professionnel de santé peut, avec l'accord du titulaire, déterminer une durée de conservation plus courte en fonction de l'utilité et de la pertinence de la donnée pour l'état de santé du titulaire. Cette durée peut être modifiée par la suite selon l'évolution de l'état de santé du titulaire.

Par dérogation à l'alinéa 1er, le professionnel de santé peut, avec l'accord du titulaire, déterminer que certaines données médicales jugées utiles et pertinentes à vie pour l'état de santé du titulaire, sont conservées jusqu'à la fermeture du dossier de soins partagé.

L'accord du titulaire est daté et consigné dans son espace d'expression personnelle dans l'application dossier de soins partagé.

Par dérogation à l'alinéa 1er, les informations relatives à l'expression personnelle du titulaire du dossier de soins partagé sont conservées jusqu'à ce que ce dernier les modifie ou les supprime.

Art. 10. Sécurité de la plateforme

(1) L'Agence met en œuvre un système de management de la sécurité de l'information certifié conforme à la norme internationale ISO/IEC 27001 incluant un processus de gestion des risques.

Les mesures de sécurité à mettre en œuvre par l'Agence comprennent au minimum :

1° un système d'authentification forte ;
2° un système d'identification des utilisateurs incluant l'identification unique des patients et des professionnels de santé ;
3° un contrôle des accès ;
4° une sécurisation de toutes les transactions sur la plateforme et avec les programmes informatiques connectés à celles-ci ;
5° la mise en place d'audits de sécurité annuels ;
6° une gestion des incidents liés à la sécurité de l'information ;
7° un hébergement des données dans un centre de données assurant un très haut niveau de disponibilité selon les standards ;
8° un système de lutte contre les intrusions et les logiciels malveillants ;
9° un chiffrement des données pour l'application dossier de soins partagé.

(2) Le professionnel de santé, responsable du traitement, et, le cas échéant, le sous-traitant, connectés à la plateforme, mettent en œuvre les mesures techniques et organisationnelles de sécurité appropriées afin de garantir un niveau de sécurité adapté aux risques.

Les mesures visées à l'alinéa qui précède comprennent au minimum :

1° un système d'authentification fort ;
2° une gestion de l'identification unique des patients et des professionnels de santé ;
3° un contrôle des accès ;
4° une procédure de gestion des incidents pour tout évènement, anomalie ou incident ayant ou pouvant avoir, directement ou indirectement, un impact sur la sécurité de la plateforme, incluant une coopération avec l'Agence selon les bonnes pratiques applicables en la matière ;
5° une sensibilisation du personnel utilisant une application de la plateforme conformément aux règles et bonnes pratiques de sécurité.

Pour l'application du présent paragraphe, les professionnels de santé et sous-traitants s'appuient sur les bonnes pratiques de sécurité et de confidentialité des données figurant à l'annexe 2.

Art. 11. Modalités techniques de versement des données au dossier de soins partagé et interopérabilité

(1) Les référentiels d'interopérabilité applicables y inclus les spécifications techniques, les formats et garanties d'intégrité, de versement des données au dossier de soins partagés sont déterminés par l'Agence sur base des profils d'intégration « Integrating the Healthcare Enterprise » utilisés pour la plateforme.

Les données non structurées et les données structurées sont versées au dossier de soins partagé sur base des profils d'intégration « Integrating the Healthcare Enterprise » appliqués et selon les nomenclatures arrêtées par domaine de santé.

Une liste des profils visés aux alinéas qui précèdent est publiée sur le site internet de l'Agence et leurs modalités d'implémentation pour l'application dossier de soins partagé sont communiquées à tout professionnel de santé et sous-traitant ayant introduit une demande de connexion conformément au paragraphe 2.

(2) Pour établir une connexion à l'application dossier de soins partagé, le programme informatique utilisé par le professionnel de santé doit être conforme aux critères de connexion inclus dans les référentiels d'interopérabilité définis pour la plateforme et obtenir l'attestation de conformité y relative.

À cet effet, le professionnel de santé ou sous-traitant introduit une demande de connexion auprès de l'Agence en fournissant à l'appui de sa demande une description de son programme informatique ainsi que du contexte d'utilisation.

La procédure de connexion à la plateforme s'effectue obligatoirement en deux étapes :

1° une phase d'analyse et de tests destinée à valider la conformité aux exigences techniques, fonctionnelles, organisationnelles et de sécurité requises pour l'accès à l'application dossier de soins partagé ;
2° une phase de tests et de contrôle pour valider la connexion effective du programme informatique à la plateforme.

L'attestation de conformité n'est délivrée que si le professionnel de santé ou son sous-traitant remplit les conditions suivantes ;

1° avoir passé avec succès les tests mentionnés au paragraphe 2, alinéa 3, point 1° effectués par un organisme ou une société expert en interopérabilité des systèmes de santé ;
2° avoir mis en œuvre des mesures pour assurer le respect des dispositions du présent règlement grand-ducal, en particulier en ce qui concerne l'attribution des droits d'accès et d'écriture ainsi que le classement des données selon la matrice des accès, la traçabilité des accès et des actions, l'information des professionnels sur l'utilisation de l'application dossier de soins partagé.

L'attestation mentionnée à l'alinéa 1er est délivrée par l'Agence sur base du résultat des tests réalisés par un organisme ou une société expert en interopérabilité des systèmes de santé.

Elle reste valable tant qu'aucune modification n'affecte la validité des tests réalisés au cours de la procédure de connexion ou l'une des conditions liées à sa délivrance. L'Agence tient à jour sur son site internet la liste des professionnels de santé et sous-traitants bénéficiant d'une attestation de conformité.

(3) Toute modification du programme informatique ainsi que toute mise à jour des référentiels d'interopérabilité susceptible d'avoir un impact sur les critères de connexion visés au paragraphe 2 est communiquée par écrit et sans délai dès sa connaissance aux personnes désignées.

Après communication d'un des changements visés à l'alinéa 1er du présent paragraphe et en fonction de l'ampleur des adaptations techniques à réaliser, l'Agence et le professionnel de santé ou le sous-traitant mettent en œuvre un plan d'évolution et déterminent, en cas de besoin, les tests de conformité à repasser en vue du maintien de l'attestation.

À défaut d'accord sur la mise en œuvre d'un plan ou à défaut de remise en conformité selon le plan convenu et lorsqu'elle constate ou est informée que la non-conformité entraîne un dysfonctionnement de l'application du dossier de soins partagé, l'Agence prend les mesures conservatoires nécessaires jusqu'à ce que les conditions liées à l'attestation de conformité sont à nouveau remplies.

Art. 12. Disposition modificative

À l'article 2 du règlement grand-ducal modifié du 15 novembre 2011 déterminant les modalités de désignation, de reconduction, de changement et de remplacement en cas d'absence du médecin référent, l'alinéa 5 est supprimé.

Art. 13. Formule exécutoire et de publication

Notre ministre ayant la Sécurité sociale dans ses attributions et notre ministre ayant la Santé dans ses attributions sont chargés, chacun en ce qui le concerne, de l'exécution du présent règlement qui sera publié au Journal officiel du Grand-Duché de Luxembourg.

Le Ministre de la Santé,
Étienne Schneider

Le Ministre de la Sécurité sociale,
Romain Schneider

Château de Berg, le 6 décembre 2019.
Henri

ANNEXE 1 - MATRICE DES DROITS D'ACCÈS PAR DEFAUT ET D'ÉCRITURE DES PROFESSIONNELS DE SANTÉ

	CATEGORIES DE PROFESSIONNELS DE SANTE (1)										
CATEGORIES DE DONNEES (2)	Médecin	Médecin Référent	Pharmacien	Infirmier	Professionnel de Santé expert	Sage-femme	Laborantin	Assistant Technique Médical	Aide-soignant	Intervenant Social	Biologiste médical
Expression personnelle du titulaire	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ
Synthèses	✔	✔	⊘	ⓘ	ⓘ	ⓘ	⊘	ⓘ	ⓘ	ⓘ	⊘
Antécédents de santé	✔	✔	ⓘ	ⓘ	ⓘ	✔	⊘	ⓘ	ⓘ	⊘	ⓘ
Allergies – intolérances	✔	✔	✔	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ	⊘	ⓘ
Prothèses et appareillages	✔	✔	⊘	ⓘ	ⓘ	ⓘ	⊘	ⓘ	ⓘ	⊘	ⓘ
Comptes rendus de prise en charge	✔	✔	ⓘ	✔	✔	✔	ⓘ	ⓘ	ⓘ	✔	ⓘ
Certificats et déclarations	✔	✔	⊘	ⓘ	ⓘ	ⓘ	⊘	⊘	ⓘ	⊘	⊘
Imageries médicales	✔	✔	⊘	ⓘ	ⓘ	ⓘ	⊘	ⓘ	⊘	⊘	⊘
Analyses médicales	✔	✔	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ	ⓘ	⊘	✔
Dispensation médicamenteuse	ⓘ	ⓘ	✔	ⓘ	⊘	⊘	⊘	⊘	⊘	⊘	⊘
Bilans soignants de prise en charge	✔	✔	⊘	✔	✔	✔	⊘	ⓘ	✔	ⓘ	ⓘ
Prescriptions et traitements	✔	✔	✔	ⓘ	ⓘ	✔	ⓘ	ⓘ	ⓘ	⊘	ⓘ
Prévention	✔	✔	ⓘ	✔	✔	✔	⊘	⊘	✔	ⓘ	ⓘ
Données socio-éducatives	ⓘ	ⓘ	⊘	✔	✔	ⓘ	⊘	⊘	ⓘ	ⓘ	⊘
Environnement social	ⓘ	ⓘ	⊘	✔	✔	✔	⊘	⊘	ⓘ	✔	⊘
Régime protection juridique titulaire	ⓘ	ⓘ	⊘	ⓘ	ⓘ	✔	⊘	⊘	ⓘ	✔	⊘
Couverture et assurance sociale	ⓘ	ⓘ	ⓘ	ⓘ	✔	ⓘ	ⓘ	⊘	ⓘ	✔	ⓘ
Éducation	✔	✔	ⓘ	✔	✔	✔	⊘	⊘	✔	⊘	⊘
Tableau de bord des traces	⊘	ⓘ	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘

Légende

Sigle	Niveau d'accès	Description
✔	Lecture et écriture	Le professionnel de santé est autorisé à introduire et à consulter les documents appartenant à la catégorie de données concernée au sein du dossier de soins partagé du titulaire.
ⓘ	Lecture seule	Le professionnel de santé est autorisé à consulter les documents appartenant à la catégorie de données concernée au sein du dossier de soins partagé du titulaire.
⃠	Aucun accès	Le professionnel de santé n'est autorisé ni à introduire ni à consulter les documents appartenant à la catégorie de données concernée au sein du dossier de soins partagé du titulaire.

(1) Catégories de professionnels de santé

Les catégories de professionnels de santé sont définies par rapport aux attributions respectives que leur confèrent les lois et règlements encadrant l'exercice de leur profession ainsi que les règles déontologiques qui leur sont applicables.

Catégories de Professionnels de santé	Professions réglementées / Fonction réglementée
Médecin	Médecin généraliste / Médecin spécialiste Médecin-dentiste / Médecin-dentiste spécialiste Psychothérapeute (si diplôme de base de médecin) *non inclus : médecins vétérinaires
Pharmacien	Pharmacien
Infirmier	Infirmier Infirmier en anesthésie et réanimation Infirmier en pédiatrie Infirmier psychiatrique Infirmier gradué Assistant technique médical (spécialité chirurgie)
Professionnel de Santé expert	Masseur-Kinésithérapeute Masseur Ergothérapeute Diététicien Orthophoniste Orthoptiste Ostéopathe Pédagogue curatif Podologue Psychothérapeute (si diplôme de base autre que médecin) Rééducateur en Psychomotricité
Sage-femme	Sage-femme

Laborantin	Laborantin Assistant technique médical (spécialité laboratoire)
Assistant Technique Médical	Assistant technique médical (spécialité radiologie)
Aide-soignant	Aide-soignant
Intervenant Social	Assistant social Assistant d'hygiène sociale
Biologiste médical	Médecin spécialiste biologie clinique (formation spécialisée biologie médicale) Pharmacien (formation spécialisée biologie médicale) Chimiste – biochimiste (formation spécialisée biologie médicale)

(2) <u>Catégories de données</u>

Les catégories de données sont définies en fonction des dispositions légales et réglementaires, des règles déontologiques et des usages au regard des données acquises de la science.

Catégories de données	**Description**
Expression personnelle du titulaire	Comprend les informations qui apportent la perception clinique du titulaire sur sa situation et son état de santé et jugées pertinentes pour sa prise en charge coordonnée et la continuité des soins, ainsi que celles contenant les volontés du titulaire (don d'organe, directives anticipées ou informations relatives aux dispositions de fin de vie).
Synthèses	Comprend les documents synthétiques cliniques comportant un ensemble de données de santé du titulaire à un moment "t", ainsi que les documents émis par la Caisse nationale de santé relatifs à la prise en charge du titulaire.
Antécédents de santé	Comprend les informations relatives à des allergies ou maladies chroniques aux conséquences sévères, antécédents chirurgicaux graves pouvant avoir un impact sévère sur la santé du titulaire.
Allergies – intolérances	Comprend les informations relatives aux allergies, aux intolérances, et aux réactions causées par un traitement identifiées et/ou observées par un professionnel de santé.
Prothèses et appareillages	Comprend les informations relatives aux appareils et dispositifs médicaux, utilisés auprès du titulaire, soit en utilisation implantable, soit en dispositif externe. Ces dispositifs et appareils peuvent être permanents ou temporaires, actuels ou passés.
Comptes rendus de prise en charge médicale	Comprend les comptes rendus émis à la suite d'une prise en charge médicale, soignante ou multi-disciplinaire du titulaire permettant de comprendre ce qui a été fait ou qui est mis en place auprès du titulaire. Ils sont produits respectivement : - à la suite d'un acte médical ou chirurgical ou obstétrique, - à la suite d'une demande diagnostique formulée médicalement ou dans le cadre d'une prise en charge thérapeutique médicale ou chirurgicale ou obstétrique, - à la suite d'un acte prophylaxique (acte de vaccination), - à la suite d'un épisode de prise en charge, - à la suite d'un suivi réalisé à domicile par un réseau d'aide et de soins ou un réseau de santé spécialisé ou par une équipe hospitalière soignante souhaitant faire une transmission spécifique de soins participant à la continuité des soins à prodiguer auprès du titulaire par les prochains intervenants,

	- à la suite ou pendant une prise en charge spécialisée (exemple : carnet de soins palliatifs). Comprend également les documents reprenant les différentes administrations médicamenteuses effectuées, en relation avec une prescription, pouvant être un résumé des actions et contrôles soignants effectués dans le cadre de l'administration des médicaments auprès du titulaire.
Certificats et déclarations	Comprend les documents produits à la demande du titulaire comportant des éléments d'évaluation sur un état ou sur un risque, en vue de lui permettre de bénéficier des prestations auxquelles il a légitimement droit.
Imageries médicales	Comprend les comptes rendus d'imagerie médicale comportant l'interprétation d'un spécialiste en radiologie ou en technique d'imagerie avec un lien vers les images.
Analyses médicales	Comprend les informations relatives aux résultats des analyses médicales, après validation médicale biologique.
Dispensation médicamenteuse	Comprend les informations permettant de suivre la consommation médicamenteuse du titulaire (liste des médicaments délivrés, contexte de délivrance, etc.).
Bilans soignants de prise en charge	Comprend les informations issues de l'entretien du titulaire avec un professionnel de santé spécialisé pour optimiser sa prise en charge. Il s'agit respectivement de : - l'évaluation initiale pour déterminer le degré d'autonomie et les zones de dépendance ou de limitation, afin d'établir un programme d'accompagnement pour le maintien, l'amélioration ou le recouvrement d'un degré d'autonomie ; - l'évaluation de l'état fonctionnel décrivant l'handicap acquis du titulaire afin d'établir un programme thérapeutique adapté.
Prescriptions et traitements	Comprend les informations sur des prescriptions médicales faites pour le titulaire (médicaments, actes de soins, appareils et dispositifs médicaux, demandes d'avis ou consultation, analyses de biologie médicale, examens d'imagerie, cures thermales, etc.).
Prévention	Comprend les informations relatives aux mesures visant à éviter ou réduire le nombre et la gravité des maladies, des accidents et des handicaps.
Données socio-éducatives	Comprend les informations éducatives et sociales relatives au niveau d'éducation et au degré d'indépendance physique, mentale et morale du titulaire, du degré de perte d'autonomie du titulaire.
Environnement social	Comprend les informations relatives à l'environnement social du titulaire qui peuvent interférer dans sa prise en charge, dont le suivi des actions en cours ou effectuées en termes de prise en charge sociale, et qui permettent de définir les mesures à mettre en place autour du titulaire.
Régime protection juridique	Comprend les informations pertinentes concernant le régime de protection juridique du titulaire.
Couverture et assurance sociale	Comprend les informations relatives à la couverture en matière d'assurance sociale (obligatoire ou complémentaire).
Éducation	Comprend les informations relatives aux actions d'éducation en matière de la santé prévues, planifiées ou réalisées auprès du titulaire.
Tableau de bord des traces	Comprend les informations créées automatiquement par l'application dossier de soins partagé relatives aux traces des accès et actions portant sur le dossier de soins partagé d'un titulaire (historique des accès, chronologie des accès, historique de l'activité, historique de l'état du dossier).

(3) <u>Durée des accès par défaut</u>

La durée d'accès par défaut au dossier de soins partagé d'un titulaire et aux données qui y sont contenues est déterminée par le contexte dans lequel le professionnel de santé prend en charge le titulaire. Les contextes de prises en charge sont définis conformément aux lieux d'exercice des professionnels de santé.

	Durée d'accès par défaut
Consultation de professionnel de santé exerçant à titre individuel	À compter de la communication par le titulaire lors de la consultation d'un identifiant de connexion et pendant une durée maximale de 15 jours prévue par l'article 9, paragraphe 3 du présent règlement grand-ducal.
Consultation hors urgence dans une collectivité de santé	À compter de l'enregistrement du titulaire à l'entrée de la collectivité de santé et pendant une durée maximale de 45 jours**.** La durée maximale peut être reconduite par période maximale de 30 jours en cas de présence prolongée du titulaire ou, avec l'accord du patient, jusqu'à la réception d'un résultat d'analyse de biologie médicale.
Consultation d'urgence dans un établissement hospitalier	À compter de l'enregistrement du titulaire à l'entrée du service d'urgence et pendant une durée maximale de 24 heures, augmentée du délai de 15 jours prévu par l'article 9, paragraphe 3 du présent règlement grand-ducal.

ANNEXE 2 - BONNES PRATIQUES DE SÉCURITÉ ET DE CONFIDENTIALITÉ DES DONNÉES

IDENTIFICATION DES MENACES

La mise en œuvre de mesures de sécurité commence par le choix d'une méthode reconnue pour analyser les risques de sécurité du système d'information.

PÉRIMÈTRE DU SYSTÈME-CIBLE DE L'ANALYSE

Le périmètre fonctionnel à prendre en compte pour la gestion des risques de sécurité du système d'information est précisé de manière synthétique.

Périmètre du système d'information considéré	Description macroscopique des principales fonctions du système et inventaires des catégories d'informations manipulées
Enjeux et finalités	Description des bénéfices attendus de la mise en œuvre du système-cible, en particulier en réponse aux attentes du promoteur et des utilisateurs.

EXPRESSION DES BESOINS DE SÉCURITÉ

Sur base du périmètre fonctionnel déterminé et pour les fonctions et les informations les plus sensibles, une évaluation d'impact d'une perte totale ou partielle par rapport aux critères de classification de l'information DICA (Disponibilité, Intégrité, Confidentialité, Auditabilité) est réalisée moyennant les indicateurs de la méthode choisie comme illustré au tableau ci-dessous :

Évènement redouté DICA	Fonction / Informations	Impact
Perte de Disponibilité	Fonction de téléconsultation.	Perte de chance pour les patients.
Perte d'Intégrité	Informations médicales contenues dans les dossiers patients.	Erreur de diagnostic. Perte de chance pour les patients.
Perte de Confidentialité	Fonction d'accès aux dossiers des patients.	Atteinte à la vie privée, non-respect des obligations légales et réglementaires
Perte Auditabilité	Fonction d'archivage de l'historique des accès aux dossiers des patients.	Impossibilité de fournir des éléments de preuve lors d'un contentieux.

Pour les besoins de la réalisation de l'évaluation d'impact, les critères de classification de l'information « Disponibilité, Intégrité, Confidentialité et Auditabilité » s'entendent comme suit :

Sigle	Critère	Signification selon la méthode EBIOS
D	**Disponibilité**	Propriété d'accessibilité en temps utile d'un élément essentiel, par les utilisateurs autorisés. Pour une fonction : garantie de la continuité du service offert ; respect des temps de réponse attendus. Pour une information : garantie de l'accès aux données dans les conditions prévues de délai ou d'horaire
I	**Intégrité**	Propriété d'exactitude et de complétude d'un élément essentiel. Pour une fonction : assurance de conformité de l'algorithme ou de la mise en œuvre des traitements, automatisés ou non, par rapport aux

		spécifications ; garantie de production de résultats corrects et complets par la fonction (sous réserve d'informations correctes et complètes en entrée). Pour une information : garantie d'exactitude et d'exhaustivité des données vis-à-vis d'erreurs de manipulation, de phénomènes accidentels ou d'usages non autorisés ; non-altération de l'information.
C	**Confidentialité**	Propriété d'un élément essentiel de ne pouvoir être connu que des utilisateurs autorisés. Pour une fonction : protection des algorithmes décrivant les règles de gestion et les résultats dont la divulgation à un tiers non autorisé porterait préjudice ; absence de divulgation d'un traitement ou mécanisme à caractère confidentiel. Pour une information : protection des données dont la connaissance par des tiers non autorisés porterait préjudice; absence de divulgation de données à caractère confidentiel.
A	**Auditabilité**	Propriété d'un élément essentiel permettant de retrouver, avec une confiance suffisante, les circonstances dans lesquelles cet élément évolue. Pour une fonction : capacité à déterminer la personne ou le processus automatisé à l'origine de la demande de traitement et à déterminer les autres circonstances utiles associées à cette demande. Pour une information : capacité à déterminer la personne ou le processus automatisé à l'origine de l'accès à l'information et à déterminer les autres circonstances utiles associées à cet accès.

INVENTAIRE DES TYPES DE MENACE CONSIDÉRÉS

L'inventaire des types de menaces doit être exhaustif et chaque type de menace non retenu doit être justifié.

Au cours de l'inventaire, les types de menaces selon la méthode EBIOS sont pris en considération :

Types de menace
01 – INCENDIE Destruction ou altération de ressources techniques, de supports de stockage, de documents ou de locaux du système, liée à un incendie dans ou à proximité des locaux du système
02 - DÉGÂTS DES EAUX Destruction ou altération de ressources techniques, de supports de stockage, de documents ou de locaux du système, liée à des infiltrations ou des écoulements d'eau dans ou à proximité des locaux du système.
03 - POLLUTION Propagation, dans ou à proximité du site d'une plateforme, d'une pollution chimique, nucléaire ou biologique, de fumées ou de poussières conduisant à endommager ou à rendre inaccessible une plateforme du système
04 - SINISTRE MAJEUR Dommages physiques occasionnés à une plateforme du système ou à son environnement, par un phénomène majeur naturel, un accident industriel ou un acte volontaire survenu à proximité du site de la plateforme
05 - DESTRUCTION DE MATÉRIELS OU DE SUPPORTS Destruction ou altération d'un équipement ou d'un support de stockage d'une plateforme du système, due à un accident ou une négligence ou encore à un acte délibéré, par une personne ayant accès à cet élément
06 - PHÉNOMÈNE CLIMATIQUE Perturbation du fonctionnement d'une plateforme ou altération des éléments stockés en raison de conditions climatiques dépassant la limite des caractéristiques de fonctionnement ou de stockage des ressources techniques. Le site est placé dans une zone géographiquement sensible à des conditions climatiques extrêmes
07 - PHÉNOMÈNE SISMIQUE Dommages physiques occasionnés à une plateforme du système ou à son environnement, par un phénomène sismique
08 - PHÉNOMÈNE VOLCANIQUE Dommages physiques occasionnés à une plateforme du système ou à son environnement, par un phénomène volcanique
09 - PHÉNOMÈNE MÉTÉOROLOGIQUE Dommages physiques d'une plateforme du système ou de son environnement ou perturbations de fonctionnement, occasionnées par un phénomène météorologique d'ampleur inhabituelle (foudre, pluie, neige, vent)

10 - CRUE Inondation des locaux d'une plateforme, de ceux de stockage de supports, de documents ou d'équipements, de ceux d'exploitation, de ceux d'alimentation électrique ou de télécommunication, ou inondation à proximité empêchant l'accès physique du personnel d'exploitation
11 - DÉFAILLANCE DE LA CLIMATISATION Arrêt ou dysfonctionnement de la climatisation dans les locaux d'une plateforme, de ceux de stockage de supports, de documents ou d'équipements, suite à une panne ou un acte volontaire
12 - PERTE D'ALIMENTATION ÉNERGÉTIQUE Surtensions, perturbations ou arrêt de l'alimentation électrique d'une plateforme du système
13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION Incident rendant indisponibles les moyens de télécommunication nécessaires au fonctionnement du système ou à son utilisation
14 - RAYONNEMENTS ÉLECTROMAGNÉTIQUES Perturbation du fonctionnement d'équipements d'une plateforme du système ou des communications, en raison d'incompatibilités électromagnétiques entre équipements ou à cause d'une source de rayonnement à proximité
15 - RAYONNEMENTS THERMIQUES Effet thermique provoqué par un sinistre ou des conditions météorologiques exceptionnelles (incendie de forêt), engin provoquant un effet thermique entraînant un dysfonctionnement ou une destruction des matériels (déchets nucléaires, explosion thermonucléaire)
16 - IMPULSIONS ÉLECTROMAGNÉTIQUES Destruction ou altération des équipements d'une plateforme du système ou de ses servitudes (alimentation électrique, climatisation, télécommunications), à la suite d'une impulsion électromagnétique d'origine nucléaire ou industrielle à proximité du site
17 - INTERCEPTION DE SIGNAUX PARASITES COMPROMETTANTS Capture et exploitation de signaux conduits ou émis par les équipements, signaux pouvant être porteurs d'informations confidentielles
18 - ESPIONNAGE À DISTANCE Observation des activités d'exploitation ou d'administration du système par des personnes non autorisées (visiteurs, caméras cachées, observateurs par des fenêtres)
19 - ÉCOUTE PASSIVE Au niveau des réseaux ou des supports de communication utilisés, interception des échanges entre un utilisateur et le système, entre deux plateformes du système, entre deux équipements d'une même plateforme
20 - VOL DE SUPPORTS OU DE DOCUMENTS

Vol de documents du système, vol ou substitution d'un support de stockage d'informations dans un site du système, dans un site de stockage (sauvegarde par exemple) lors d'un transport de support; ou lors de la restitution partielle ou totale du dossier sur support papier ou support informatique
21 - VOL DE MATÉRIELS Vol ou substitution d'équipements dans les locaux d'une plateforme, ou dans ceux de stockage, ou à la faveur de la maintenance ou du transport de ces équipements, avec capture éventuelle de données résiduelles
22 - RECUPERATION DE SUPPORTS RECYCLES OU MIS AU REBUT Exploitation de données résiduelles sur les supports de stockage ou les équipements retirés du système avant réemploi par ailleurs ou mise au rebut
23 - DIVULGATION Personne interne à l'organisme qui, par négligence, diffuse de l'information à d'autres personnes de l'organisme n'ayant pas le besoin d'en connaître, ou à l'extérieur. Personne diffusant consciemment de l'information à d'autres personnes de l'organisme n'ayant pas le besoin d'en connaître, ou à l'extérieur
24 - INFORMATIONS SANS GARANTIE DE L'ORIGINE Réception et exploitation dans le système d'information de l'organisme de données externes ou de matériels non adaptés provenant de sources extérieures. Personne transmettant des informations fausses, destinées à être intégrées au système d'information, pour désinformer le destinataire et porter atteinte à la fiabilité du système ou la validité des informations.
25 - PIÉGEAGE DU MATÉRIEL Implantation de fonctionnalités illicites dans un équipement ou une plateforme du système, en vue de provoquer des dysfonctionnements ou des détournements d'information
26 - PIÉGEAGE DU LOGICIEL Implantation et activation de fonctions illicites (cheval de Troie, bombe logique, virus, keylogger...) dans les logiciels du système ou propagation de telles fonctions à partir des dispositifs d'accès des utilisateurs ou des postes de travail des autres accédants
27 - GÉOLOCALISATION Localisation géographique d'une personne à son insu, à partir des informations contenues dans le système.
28 - PANNE MATÉRIELLE Panne d'un matériel du système, entraînant la dégradation de service ou l'indisponibilité du système.
29 - DYSFONCTIONNEMENT DU MATÉRIEL Dysfonctionnement d'un matériel du système, entraînant la dégradation de service ou l'indisponibilité du système.
30 - SATURATION DU SYSTÈME INFORMATIQUE Saturation des équipements du système liée à un défaut de capacité ou de conception ou à une sollicitation anormale du système (attaque de type déni de service par exemple)

31 - DYSFONCTIONNEMENT LOGICIEL Fonctionnement non conforme du logiciel du système, résultant d'un défaut de réalisation, d'installation, de maintenance ou d'exploitation
32 - ATTEINTE À LA MAINTENABILITÉ DU SYSTÈME D'INFORMATION Impossibilité ou difficulté à assurer le maintien en condition opérationnelle du système, du fait de défauts de conception du système, d'insuffisances du dispositif de soutien, de défaillances de fournisseurs, d'obsolescence de ressources techniques
33 - UTILISATION ILLICITE DES MATÉRIELS Accès à un équipement du système par une personne non autorisée et utilisation de cet équipement pour accéder aux fonctions ou aux données du système
34 - COPIE FRAUDULEUSE DE LOGICIELS Copie de logiciels du système en vue de leur utilisation par ailleurs
35 - UTILISATION DE LOGICIELS CONTREFAITS OU COPIÉS Mise en œuvre dans le système de logiciels dont les droits d'utilisation ou d'exploitation sont insuffisants
36 - ALTÉRATION DES DONNÉES Modification/altération des données échangées entre les équipements ou les plateformes du système ou entre le système et les dispositifs d'accès des utilisateurs (menace de type Man in the middle), ou modification/altération des données sur les supports de stockage (voire substitution de support) ou dans les équipements du système
37 - TRAITEMENT ILLICITE DES DONNÉES Utilisation des données de santé ou des données personnelles à d'autres fins que celles autorisées par la législation ou un règlement
38 - ERREUR D'UTILISATION Erreur d'exploitation ou d'intervention, erreur d'utilisation.
41 - RENIEMENT D'ACTIONS Contestation, par une personne autorisée, des actions effectuées sur le système ou ses informations
42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL Indisponibilité du personnel d'exploitation ou d'administration ou impossibilité pour celui -ci d'accéder au système et d'effectuer les actions nécessaires (exemples : pandémie, évacuation d'un site, mouvement social)

Niveaux de risques

Les niveaux de risques retenus lors de l'analyse sont précisés selon la description figurant au tableau ci-dessous :

	Confidentialité	**Disponibilité**	**Intégrité**	**Traçabilité**
0	Public	Aucun besoin de disponibilité	Normal	Normal
	Données accessibles au public (ex : données de l'annuaire).	Le bien peut être indisponible définitivement ou pas, sans que cela n'ait de conséquence	Il y a un besoin de garantir l'intégrité du bien à minima	Il y a un besoin de garantir la traçabilité de ce bien à minima
1	Interne	Long terme		
	Le bien est sensible, certaines personnes identifiées peuvent y accéder.	Le bien peut être indisponible plus d'une journée mais il ne doit pas être perdu définitivement		
2	Restreint	Moyen terme	Important	Important
	Le bien est sensible, seules certaines personnes identifiées peuvent y accéder.	Le bien peut être indisponible une demi-journée. (ex : environnement d'intégration ou espace collaboratif)	Il y a un besoin de garantir l'intégrité du bien de manière élevée	Il y a un besoin de garantir la traçabilité de ce bien de manière élevée
3	Confidentiel	Court terme		
	Le bien est très sensible, seules certaines personnes avec des responsabilités particulières peuvent y accéder.	Le bien ne peut pas être indisponible plus d'une heure (ex : environnement de préproduction ou messagerie sécurisée)		
4	Secret Médical	Très court terme	Vital	Forte
	Données médicales nominatives, seules les personnes astreintes au secret médical peuvent y accéder.	Le bien doit être disponible en temps réel (ex : environnement de production, ou aspect applicatif)	Le bien doit être parfaitement intègre (ex : données médicale)	Le bien doit être parfaitement traçable. Les actions doivent être non répudiables (ex : rapport d'analyse)