Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

GDK Schweizerische Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
CDS Conférence suisse des directrices et directeurs cantonaux de la santé
CDS Conferenza svizzera delle direttrici e dei direttori cantonali della sanità

eHealth Suisse

Normes et architecture
Recommandations V

Règles concernant la gestion des droits d'accès

Adopté par le comité de pilotage

Berne, le 28 août 2014

ehealthsuisse
Koordinationsorgan Bund-Kantone
Organe de coordination Confédération-cantons
Organi di coordinamento Confederazione-Cantoni

Impressum

Organisation du projet
Comité de pilotage : Alain Berset (conseiller fédéral, chef du DFI), Pascal Strupler (directeur de l'OFSP), Stefan Spycher (vice-directeur de l'OFSP), Susanne Hochuli (conseillère d'Etat, directrice de la santé, canton AG, dès 1er juillet 2014), Carlo Conti (conseiller d'Etat, directeur de la santé, canton BS, jusqu'au 30 juin 2014), Guido Graf (conseiller d'Etat, directeur de la santé, canton LU), Heidi Hanselmann (conseillère d'Etat, directrice de la santé, canton SG), Pierre-François Unger (conseiller d'Etat, directeur de la santé, canton GE, jusqu'à fin 2013), Mauro Poggia (conseiller d'Etat, directeur de la santé, canton GE, depuis début 2014).
Organe directeur du projet : Adrian Schmid (« eHealth Suisse », président), Christian Affolter (santésuisse jusqu'en juillet 2013), Lotte Arnold (SPO), Hansjörg Looser (GD SG), Daniel Notter (pharmaSuisse), Caroline Piana (H+), Georg Schielke (CDS), Adrian Jaggi (OFSP jusqu'en décembre 2012, santésuisse dès juillet 2013), Walter Stüdeli (IG eHealth), Salome von Greyerz (OFSP), Judith Wagner (FMH).

Secrétariat de l'Organe de coordination « eHealth Suisse » : Adrian Schmid (responsable), Catherine Bugmann, Isabelle Hofmänner, Sang-Il Kim, Stefan Wyss, Corina von Känel.

Conseil spécialisé : Christian Lovis (Hôpitaux Universitaires de Genève HUG, président SSIM)

Autres informations et sources :
www.e-health-suisse.ch

Objectif et positionnement de ce document

Le présent document contient des propositions relatives à la gestion des droits d'accès au dossier électronique du patient. Les recommandations concernent des projets de mise en œuvre dont l'objectif est d'élaborer des droits d'accès de patientes et de patients conformément à la stratégie. Elles comportent par ailleurs des données utilisables dans le cadre des travaux d'exécution de la loi fédérale sur le dossier électronique du patient réalisés par la Confédération. Les recommandations se basent sur un travail réalisé sur mandat par la « Communauté de travail Cas d'application ». Les documents de recommandation et les travaux de préparation sont disponibles sur www.e-health-suisse.ch.

Cadre légal modifié

Les recommandations d'« eHealth Suisse » valables jusqu'à présent étaient orientées sur le droit en vigueur. Le cadre légal prévu dans le le projet actuel de « loi fédérale sur le dossier électronique du patient » (Projet LDEIP) approuvé par la décision du Conseil des Etats du 12 juin 2014 a en outre été pris en considération pour ces recommandations V. Celui-ci peut être consulté à l'adresse http://www.parlament.ch/ab/frameset/d/s/4914/439277/d_s_4914_439277_439278.htm.

Afin de faciliter la lecture de ce document et sauf mention contraire, le masculin générique est utilisé pour désigner les deux sexes.

Table des matières

1 Situation initiale

1.1 Introduction

Position du présent document sur le plan technique

Le présent document décrit, du point de vue technique, les règles qui doivent être appliquées dans le cadre de la gestion des droits d'accès au dossier électronique du patient (DEP). La condition relative au caractère contraignant de l'application relève de décisions politiques qui doivent être clarifiées dans le cadre de projets législatifs. Des bases légales à l'échelle fédérale ou cantonale (ou des conventions contractuelles entre les différents acteurs) sont envisageables.

Recommandations précédentes comme base

Sont ici utilisés comme base les documents et rapports d'« eHealth Suisse » élaborés jusqu'à présent et en particulier les recommandations I à IV du projet partiel « Normes et architecture ». Les recommandations particulières sur les thèmes « gestion des accès » et « droits d'accès » sont les suivantes :

- *Architecture « eHealth Suisse » :* la composante de base « gestion des accès » qui doit assurer les principes de la protection des données grâce à une mise en œuvre basée sur des rôles a été introduite dans les recommandations I (19 mars 2009).
- *Composantes coordonnées sur le plan national :* les recommandations II (21 octobre 2010) définissent la « gestion des accès » comme une composante de base coordonnée sur le plan national. En même temps est introduit le concept des rôles qui définit à un niveau générique quelles sont les informations accessibles pour quels rôles. Le concept des rôles est, avec les cinq niveaux de confidentialité des documents, un instrument important de l'administration des droits d'accès.
- *Consentement et droits d'accès :* les recommandations III (27 octobre 2011) font la distinction entre trois niveaux de consentement : le « consentement de principe », les « principes personnels » par recours aux rôles ainsi que la « détermination individuelle de droits d'accès ». La matrice des droits combine les rôles possibles des professionnels de la santé et les niveaux de confidentialité possibles des documents. Sur cette base, il est possible de définir quels professionnels de la santé ont accès à quels documents avec quel niveau de confidentialité.
- *La communauté de référence administre les droits d'accès :* selon les recommandations IV (17 janvier 2013), l'administration des droits d'accès doit être réalisée de manière décentralisée dans la communauté de référence correspondante du patient. Le portail d'accès interne de la communauté de référence doit permettre au patient d'administrer ses droits d'accès.

L'être humain en tant qu'individu et ses besoins se trouvent au centre de la « Stratégie Cybersanté (eHealth) Suisse » de 2007. Par ailleurs, le comité de pilotage d'« eHealth Suisse » a approuvé en 2009 la ligne directrice générale selon laquelle « ce sont les patients qui décident de l'usage qui sera fait de leurs données de santé ». Le « groupe d'experts Cybersanté » du DFI ainsi que le projet de loi fédérale sur le dossier électronique du patient (Projet LDEIP) confirment cette ligne directrice. Il est donc nécessaire, dans le cadre de la définition des droits d'accès, de faire attention que le patient garde toujours le contrôle sur l'accès à ses données. Un principe important en matière de gestion des accès est défini par ce que l'on appelle le « consentement informé » du patient (cf. art. 3, al. 1 projet LDEIP), soit le consentement donné librement par le patient après avoir reçu des informations appropriées sur les possibilités, les droits et les obligations. Ce consentement se trouve toujours à l'origine de l'inscription d'un patient dans le système DEP (cf. également chapitre 2.1 Principes fondamentaux).

L'être humain est au centre de la stratégie et détermine lui-même ses droits

Les variantes selon lesquelles les professionnels de la santé distribuent eux-mêmes des droits d'accès ou transmettent leurs droits d'accès sans autorisation explicite du patient ne remplissent pas ce critère. La transparence et la confiance sont des conditions importantes pour l'acceptation du dossier électronique du patient (DEP). Pour simplifier la gestion des droits d'accès, il est possible de proposer au patient une sélection de profils prédéfinis. Il pourra ainsi modifier facilement ses droits d'accès. Il faut, pour cela, que le patient soit convenablement informé.

1.2 Définitions

Dans le contexte du DEP, les données médicales ne peuvent être consultées que lorsque le contexte de traitement est « explicitement » confirmé par le patient. Ceci n'est donc possible que si le patient a attribué un droit d'accès à un professionnel de la santé.

Contexte de traitement

La notion de « professionnel de la santé » est définie comme suit à l'article 2, lettre b du projet LDEIP : *« professionnel de la santé : professionnel du domaine de la santé reconnu par le droit fédéral ou cantonal qui applique ou prescrit des traitements médicaux ou qui remet des produits dans le cadre d'un traitement médical ».*

Professionnel de la santé

Pour pouvoir accéder au système du DEP, un professionnel de la santé doit être membre d'une communauté certifiée. Cela signifie que :

- le professionnel de la santé doit être enregistré dans le service d'informations national Health Professional Index,
- le professionnel de la santé peut s'inscrire dans le système du DEP avec une authentification forte.

Dans les pages qui suivent, la notion de « professionnel de la santé » est utilisée pour désigner les personnes qui remplissent les conditions ci-dessus et sont membres d'une communauté certifiée.

Groupe de professionnels de la santé

La notion de « groupe de professionnels de la santé » englobe tous les professionnels de la santé membres d'une communauté certifiée et actifs dans une organisation de santé et ses sous-organisations. Les organisations de santé peuvent être des établissements stationnaires tels que des hôpitaux de soins somatiques aigus et de réadaptation, des cabinets médicaux de groupes ou des cabinets médicaux individuels, des pharmacies ou des organisations d'aide et de soins à domicile, etc. Peuvent par ailleurs revêtir une signification importante les groupes dits « virtuels » de professionnels de la santé, comme par exemple un réseau oncologique de professionnels de la santé de différentes organisations (par exemple Tumor Board). Tous les groupes doivent être représentés dans le Health Organisation Index (HOI).

Administrateur de patients

Pour pouvoir se consacrer aux processus administratifs liés au DEP, les administrateurs de patients d'une communauté doivent bénéficier d'un accès aux données démographiques d'un patient. Ceci est particulièrement important pour pouvoir identifier correctement le patient lors de l'ouverture du dossier électronique du patient ainsi que lors du premier contact du patient avec une organisation de santé afin de trouver le patient ou éviter les confusions. Les administrateurs de patients assument ici un rôle d'« auxiliaires » mandatés par un professionnel de la santé.

Niveaux de confidentialité des contenus du DEP

Les recommandations III ont défini cinq niveaux de confidentialité (Recommandation 4). La nomenclature y relative a été adaptée afin d'éviter toute confusion :

- Données démographiques (anciennement « données administratives ») :

  Par exemple nom, prénom, sexe, adresse, date de naissance, autres caractéristiques liées à l'identification telles que le numéro d'identification du patient selon le projet LDEIP et éventuellement d'autres données de contact du patient ;

- Données utilitaires :

  Par exemple, des informations relatives à des allergies et d'autres réactions indésirables, des thérapies spécifiques (par exemple anticoagulants), maladies particulières (par exemple diabète), mais aussi directives du patient, carte de donneur d'organe, personnes à contacter en cas d'urgence ;

- Données médicales :

  Documents et données concernant le patient et importants pour un traitement sûr, en particulier les rapports et résultats (par exemple l'anamnèse, les résultats d'examens cliniques, les résultats d'analyses, les évaluations de la situation, les traitements proposés et effectivement appliqués) ;

- Données sensibles (anciennement « données stigmatisantes ») :

  Données médicales dont la trop grande divulgation pourrait porter atteinte à la vie sociale ou privée du patient, selon sa propre appréciation.

- Données secrètes :

  Données médicales que seul le patient lui-même peut consulter.

L'illustration 1 montre que différents contenus DEP peuvent être déplacés à tout moment par le patient à d'autres niveaux de confidentialité.

Tous les contenus du DEP doivent être classés dans l'un des cinq niveaux de confidentialité. Chaque nouveau contenu du DEP affiche un niveau de confidentialité fixé par le paramétrage défini par défaut dans la législation d'exécution de la LDEIP. Ce paramétrage peut être adapté par le patient.

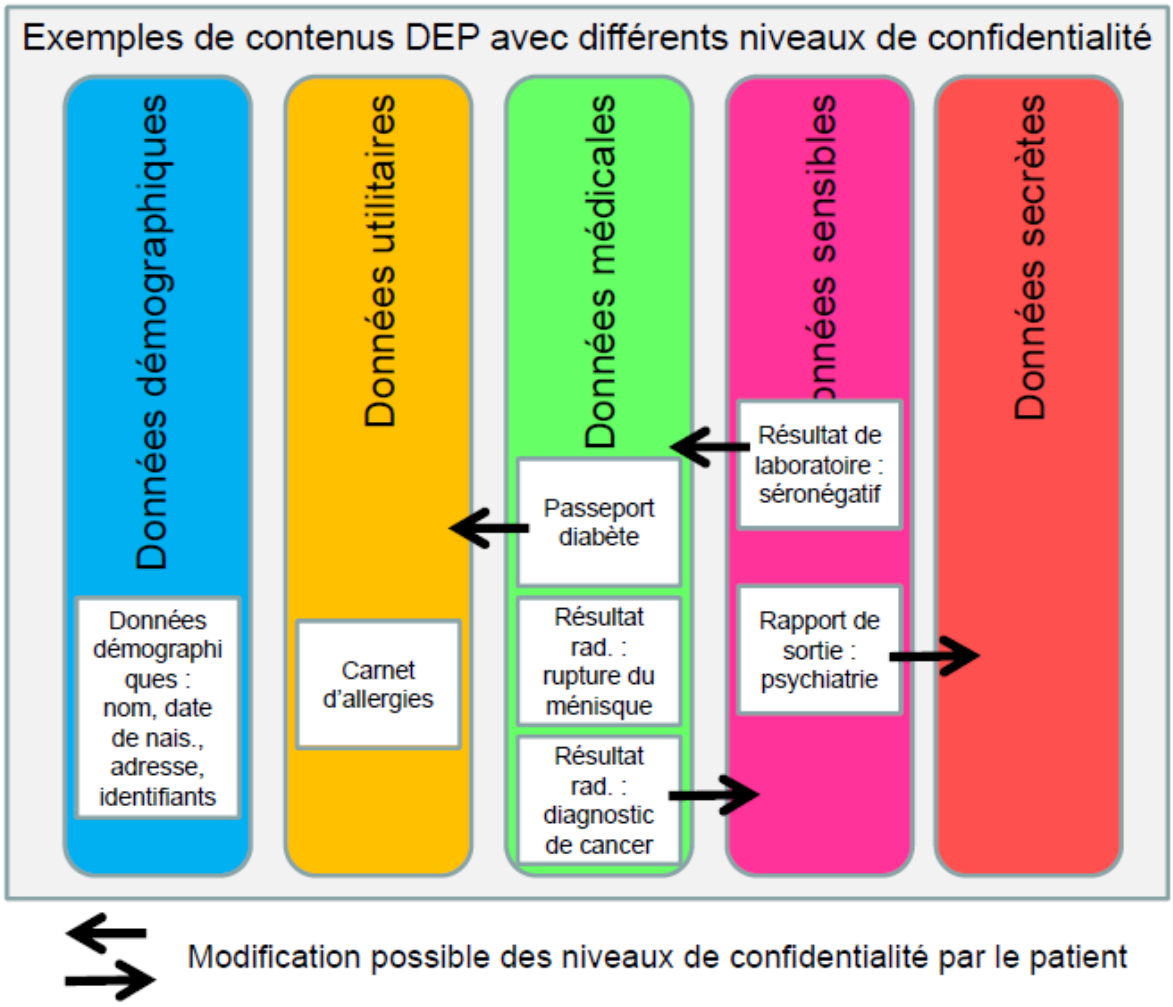

Illustration 1 : Les niveaux de confidentialité et leurs possibilités de modification (exemple fictif)

Matrice de droits

Les règles d'accès choisies par le patient sont fixées sous la forme d'une matrice de droits constituée d'une combinaison entre les personnes autorisées à qui ont été attribués des niveaux d'accès et les niveaux de confidentialité des contenus du DEP. Il est nécessaire d'évaluer ces règles pour décider si un accès à un document doit être accordé ou refusé. Les personnes autorisées (professionnels de la santé et patients) ont accès au DEP si les conditions requises sont remplies. La matrice de droits peut être adaptée à tout moment par le patient.

Paramétrage par défaut

Le paramétrage par défaut des droits d'accès est valable pour tous les DEP nouvellement créés. Le paramétrage par défaut fixe une matrice de droits et d'autres règles, telles que la durée de validité des droits d'accès ou les règles de définition des niveaux de confidentialité. Le patient peut modifier en tout temps tous les paramètres du paramétrage par défaut.

Profils prédéfinis

Les profils prédéfinis de la gestion des accès correspondent à des résumés des différents paramètres. Ces profils prédéfinis doivent représenter pour le patient une simplification de l'administration des droits d'accès à son DEP afin qu'il ne doive pas adapter manuellement chaque paramètre. Le paramétrage par défaut peut être considéré comme un profil prédéfini particulier. Le patient peut également modifier en tout temps les profils prédéfinis.

Services d'interrogation centralisés

Pour que la communication électronique entre les communautés puisse fonctionner, les services d'interrogation mentionnés ci-après doivent être exploités de manière coordonnée à l'échelle nationale et leurs données doivent être mise à disposition avec une qualité fiable et actuelle. Parmi ces services se trouvent en particulier les registres suivants :

- Registre des professionnels de la santé (service HPI) ;
- Registre des organisations de santé et des groupes de professionnels de la santé (service HOI).

Portail d'accès des patients

Selon les « Recommandations IV Normes et architecture » du 17 janvier 2013, l'administration des droits d'accès individuels par le patient ne peut être réalisée que sur le portail d'accès interne de sa communauté de référence.

Niveaux d'accès en lieu et place de rôles

Les anciennes désignations de rôles tirées des « Recommandations III Normes et architecture » ont été renommées en différents niveaux d'accès (Access Levels) pour une meilleure compréhension. Le patient doit explicitement attribuer un niveau d'accès aux professionnels de la santé avant que ceux-ci puissent consulter les contenus de son DEP. Le patient peut modifier ou retirer à tout moment le niveau d'accès attribué.

- Niveau d'accès « administratif », ancien rôle « participant administratif » :
  donne exclusivement accès aux données du niveau de confidentialité « données démographiques » ;
- Niveau d'accès « limité » (ancien rôle « professionnel de la santé en général ») :
  donne accès aux données des niveaux de confidentialité « données démographiques » et « données utilitaires » ;
- Niveau d'accès « normal » (ancien rôle « mon professionnel de la santé ») :
  donne accès aux données des niveaux de confidentialité « données démographiques », « données utilitaires » et « données médicales » ;
- Niveau d'accès « étendu » (ancien rôle « mon professionnel de la santé de confiance ») :
  donne accès aux données des niveaux de confidentialité « données démographiques », « données utilitaires », « données médicales » et « données sensibles » ;

- Niveau d'accès « urgence » (ancien rôle « professionnel de la santé d'urgence ») :
  donne accès aux niveaux de confidentialité « données démographiques », « données utilitaires » et « données médicales » en cas d'urgence médicale et même sans attribution préalable de droits d'accès par le patient. Le patient doit être informé ultérieurement des accès attribués. Le patient peut refuser à tout moment un accès en cas d'urgence médicale ou le limiter aux niveaux de confidentialité « données démographiques » et « données utilitaires » ;
- Niveau d'accès « global » :

  Ce niveau d'accès est réservé au patient. Il permet au patient de consulter toutes les données de tous les niveaux de confidentialité, et en particulier celles du niveau de confidentialité « données secrètes ». Il n'est pas prévu que ce niveau d'accès puisse être modifié dans la matrice de droits.

2 Principes fondamentaux et ensemble de règles

2.1 Principes fondamentaux

Le DEP est un système secondaire

Le système du DEP permet d'un côté au patient d'avoir accès en tout temps à un recueil de ses données médicales les plus importantes et de l'autre, d'améliorer l'échange d'informations entre les professionnels de la santé. Le DEP n'est donc pas un système primaire pour professionnels de la santé (par exemple système d'information d'une clinique ou d'un cabinet médical) qui documente les actes médicaux internes. Le DEP est un système secondaire qui rassemble toutes les informations importantes pour la poursuite d'un traitement par d'autres professionnels de la santé. La gestion des accès du DEP ne définit pas les modalités de l'accès aux données des patients dans les systèmes primaires. Dans ces systèmes, les règles d'accès sont fixées au sein des organisations respectives. Les réflexions suivantes ne concernent par conséquent que le DEP considéré comme un système secondaire qui peut être consulté par plusieurs personnes et donne accès à des informations datant parfois de plusieurs années et issues de tous les domaines médicaux.

Principes fondamentaux au sujet de l'accès

En consentant à ouvrir un DEP, le patient accepte les principes fondamentaux de la gestion des droits d'accès après avoir reçu des informations et des précisions convenables (« Informed Consent »). Il est en particulier parfaitement conscient des possibilités, des droits et des obligations des acteurs du DEP. Font partie des principes fondamentaux :

- Le consentement explicite de gestion d'un DEP (modèle opt-in) avec droit de révocation en tout temps ;
- Un niveau d'accès défini ne peut être attribué qu'à des professionnels de la santé (y compris leurs assistants) qui sont enregistrés dans le « Health Professional Index » (HPI) national, sont ainsi membres d'une communauté certifiée et possèdent une identité électronique ;
- L'attribution explicite d'un niveau d'accès à des professionnels de la santé. Le patient définit (via la matrice de droits) quels niveaux de confidentialité sont visibles pour quels niveaux d'accès ;
- La possibilité d'exclusions individuelles de professionnels de la santé (liste d'exclusion) ;
- Au moment de la demande, l'accès à un document du DEP est vérifié au moyen de l'évaluation de la matrice de droits ;
- La possibilité d'un accès en cas d'urgence pour les professionnels de la santé enregistrés dans le HPI, et ce sans attribution explicite préalable des droits d'accès par le patient. Le patient définit si un accès en cas d'urgence est possible et quels niveaux de confidentialité sont visibles.

Les principes fondamentaux de gestion d'accès susmentionnés s'appliquent à l'accès aux données après l'ouverture d'un DEP. Les cas d'application « Ouverture d'un DEP » et « Modification des données administratives du DEP » ainsi que les exigences qui en découlent ne sont pas abordés ici.

Structure de la gestion des accès

Selon les Recommandations III, la gestion des accès du DEP est basée sur trois éléments (cf. illustration 4) :

- Le consentement écrit pour l'ouverture du dossier électronique du patient après avoir fourni des informations convenables (Informed Consent) ;
- La définition du paramétrage personnel par défaut de la matrice de droits et du paramétrage par défaut des niveaux de confidentialité pour les nouveaux documents créés (principes personnels) ;
- L'attribution explicite des niveaux d'accès à des professionnels de la santé ou à des groupes de professionnels de la santé ainsi que modification des niveaux de confidentialité des différents documents (paramètres individuels).

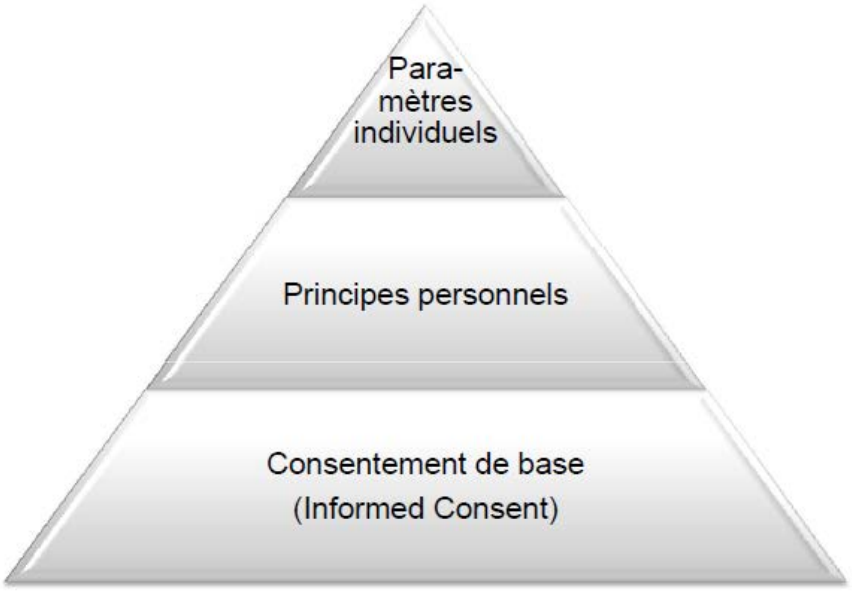

Illustration 2 : Structure de la gestion des accès

2.2 Ensemble de règles

Ensemble de règles

Les principes fondamentaux peuvent être représentés par un ensemble de règles. La définition ci-après est une définition professionnelle à un niveau abstrait et non un objectif pour l'implémentation technique. Les communautés conservent leur liberté dans le cadre de la structure interne de la mise en œuvre tant que la logique de l'ensemble de règles décrit est respectée.

L'idée fondamentale de cet ensemble de règle consiste en un procédé à trois niveaux avec vérification

- des critères d'exclusion,
- des critères d'inclusion et
- de la matrice de droits.

Les critères d'exclusion sont vérifiés au premier niveau. Si l'un des critères est valable (par exemple, le professionnel de la santé demandeur se trouve sur la liste d'exclusion du patient), l'accès est refusé sans autre forme de vérification.

Si aucun critère d'exclusion n'interdit un accès, les critères d'inclusion sont vérifiés au deuxième niveau. Si au moins un des critères d'inclusion est valable (par exemple, le patient a attribué un niveau d'accès correspondant au professionnel de la santé demandeur), il est procédé à une vérification au troisième niveau. Si aucun critère d'inclusion n'est valable, l'accès est également refusé.

Le troisième niveau implique une vérification de la matrice de droits, et donc de la combinaison du niveau d'accès du professionnel de la santé demandeur et du niveau de confidentialité des documents enregistrés dans le DEP.

L'illustration 3 représente schématiquement cet ensemble de règles à trois niveaux :

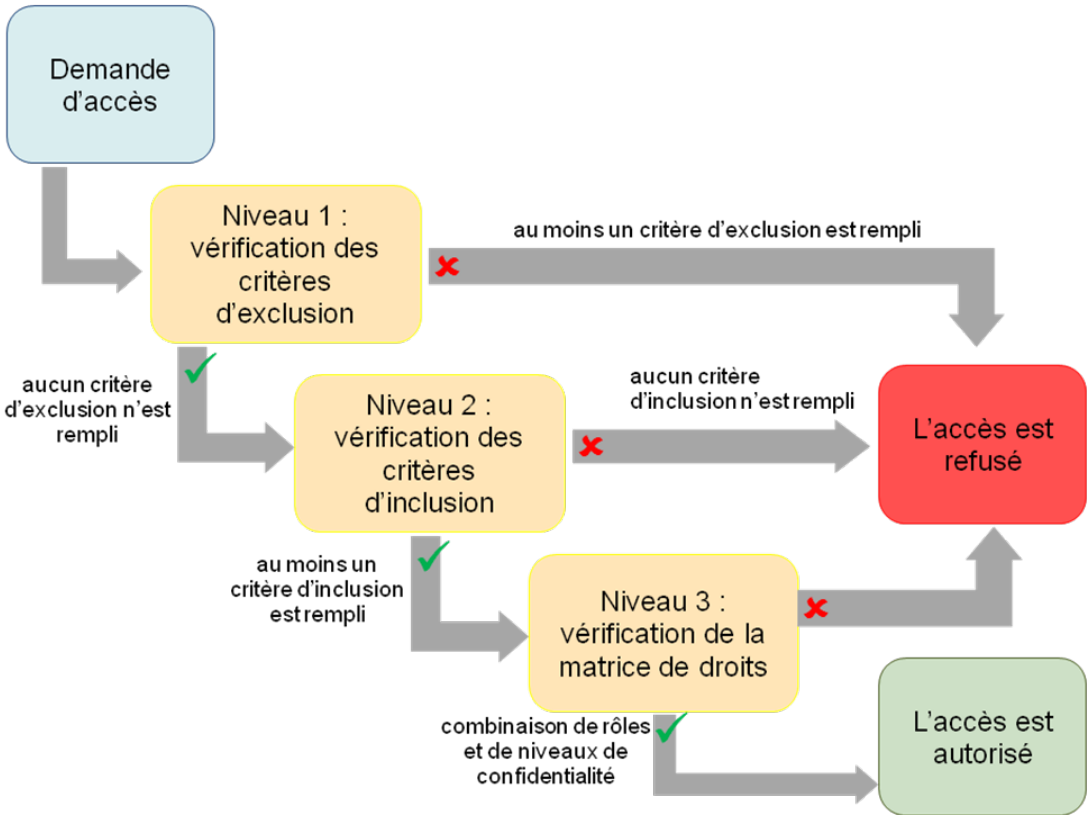

Illustration 3 : Ensemble de règles à trois niveaux

Les critères d'exclusion, les critères d'inclusion et la matrice de droits sont vérifiés avant l'accès au DEP. Pour qu'un accès soit attribué, il est nécessaire qu'aucun critère d'exclusion ne soit valable ET qu'au moins un critère d'inclusion soit rempli ET que l'accès soit autorisé selon la matrice de droits.	Recommandation 1 Ensemble de règles à trois niveaux

Deux critères d'exclusion peuvent être déduits des principes fondamentaux susmentionnés :

Vérification des critères d'exclusion

1. Le consentement du patient est nécessaire pour l'établissement et la gestion d'un DEP (modèle opt-in). Le patient peut en tout temps révoquer ce consentement et bloquer ainsi toute possibilité d'accès.
2. Le patient peut à tout moment exclure des professionnels de la santé de l'accès à son DEP. Une liste d'exclusion est établie à cet effet. Cette liste d'exclusion est prioritaire sur toutes les autres règles.

L'illustration 4 représente schématiquement les différentes étapes de vérification.

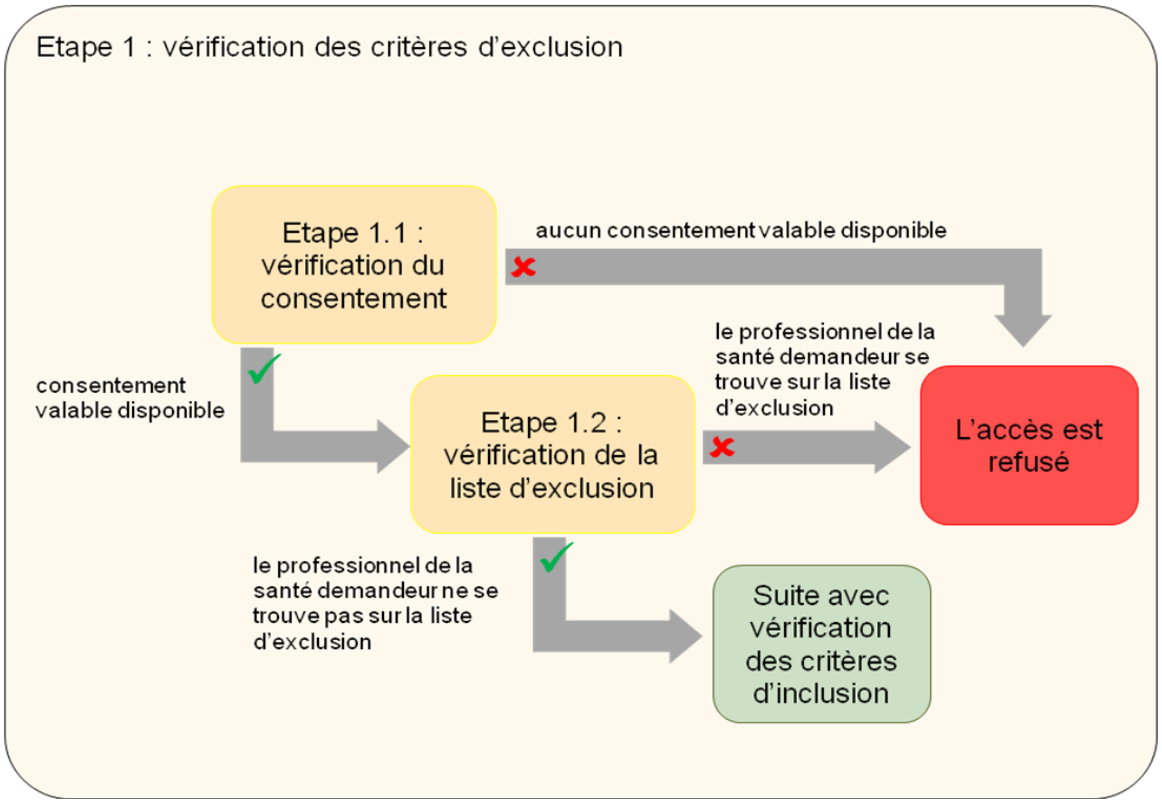

Illustration 4 : Ensemble de règles - Critères d'exclusion (zoom sur le « niveau 1 » de l'illustration 3)

Les critères d'exclusion suivants sont vérifiés et empêchent un accès : ➢ Le consentement de gestion d'un DEP n'est pas disponible car le patient a révoqué son consentement. ➢ Le professionnel de la santé demandeur se trouve sur la liste d'exclusion du patient.	Recommandation 2 Critères d'exclusion

Vérification des critères d'inclusion

La relation qui existe entre le patient et le professionnel de la santé demandeur au moment de la demande est déterminante lors de la vérification des critères d'inclusion. Il est possible de distinguer deux cas différents qui seront vérifiés comme critères d'inclusion. Si l'un d'entre eux est valable, la matrice de droits sera vérifiée au troisième niveau.

Les deux cas suivants doivent être vérifiés d'après l'illustration 5 ci-dessous :

Deux cas en présence de critères d'inclusion

Cas 1 :

Le professionnel de la santé demandeur a-t-il été nommément autorisé en se voyant attribuer un niveau d'accès ? Si ce critère est valable, le professionnel de la santé demandeur peut accéder aux niveaux de confidentialité correspondants selon la matrice de droits du patient et en fonction de son niveau d'accès.

Cas 2 :

Cette demande concerne-t-elle un accès d'urgence ? Dans ce cas, le professionnel de la santé demandeur se verra attribuer le niveau d'accès « urgence » dès qu'il confirmera l'accès d'urgence. Il peut ensuite voir les niveaux de confidentialité autorisés, pour autant que le patient n'a pas exclu explicitement l'accès d'urgence. Il existe ici un contexte de traitement particulier puisque le professionnel de la santé recourt à l'accès d'urgence et s'attribue ainsi lui-même le niveau d'accès « urgence ».

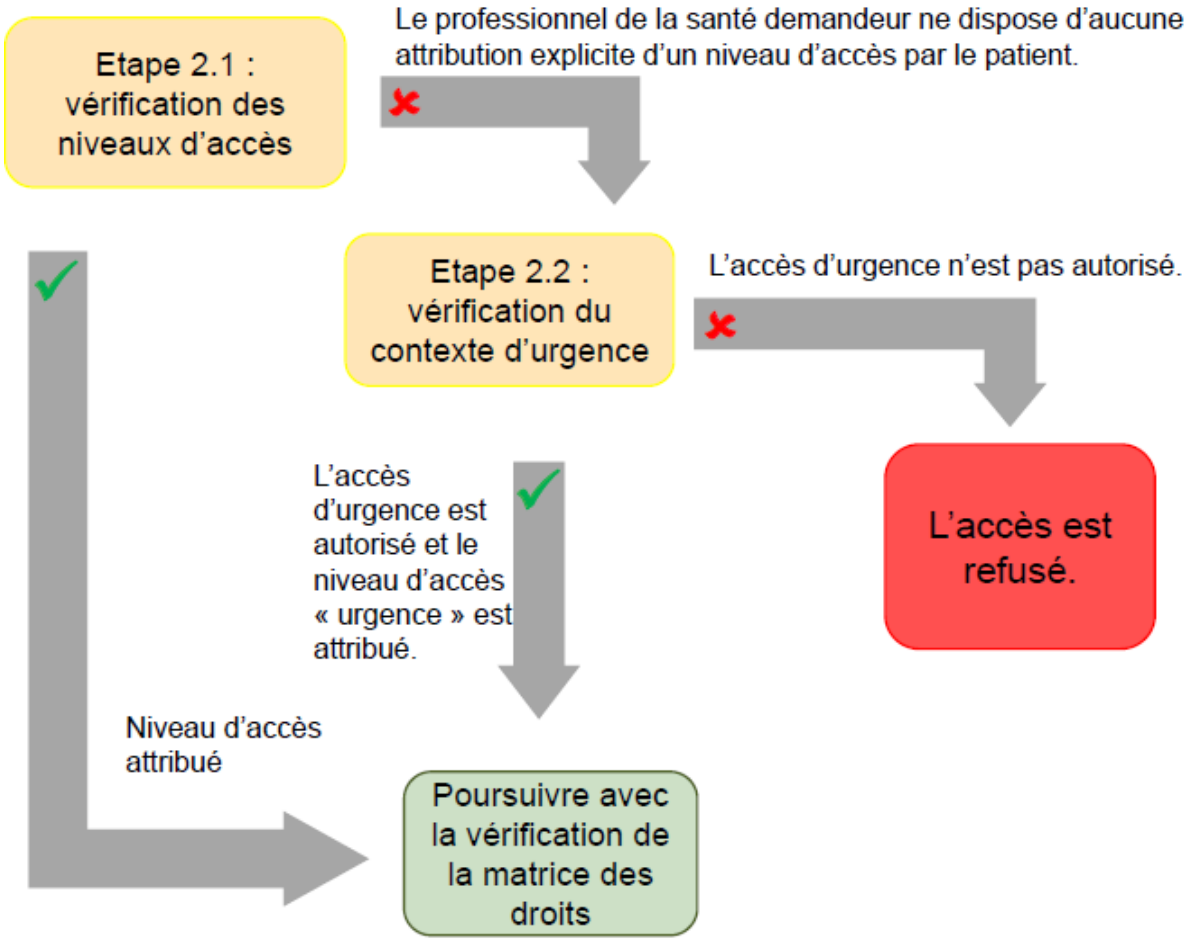

Illustration 5 : Ensemble de règles - Critère d'inclusion (zoom sur le « niveau 2 » de l'illustration 3)

Les critères d'inclusion suivants sont vérifiés : ➢ Contexte de traitement : le patient définit qui fait partie de son cercle de professionnels de la santé. Il attribue explicitement les niveaux d'accès adaptés aux professionnels de la santé souhaités. ➢ Contexte d'urgence : dans des situations d'urgence médicale, les professionnels de la santé peuvent accéder à des données du DEP sans disposer de droits d'accès attribués au préalable. Le professionnel de la santé demandeur se voit alors attribuer le niveau d'accès « urgence ». Le patient peut définir les niveaux de confidentialité visibles pour l'accès d'urgence. Un professionnel de la santé peut exiger un accès d'urgence. Cet accès ne concerne que le dossier du patient sélectionné. Le patient est informé activement de cet accès.	Recommandation 3 Critères d'inclusion
La matrice de droits personnelle du patient est évaluée au troisième et dernier niveau. Les données et les documents effectivement accessibles dépendent du niveau d'accès du professionnel de la santé demandeur, des niveaux de confidentialité des documents enregistrés dans le DEP et des règles que le patient a définies dans sa matrice de droits.	Evaluation de la matrice de droits

2.3 Paramétrage par défaut et profils prédéfinis

Le principe fondamental de gestion d'accès a été défini par les recommandations précédentes et est valable pour tous les cas d'application.

Principe

L'ouverture d'un DEP implique un paramétrage par défaut défini sur le plan juridique pour la gestion des droits d'accès. Ce paramétrage par défaut doit afficher un bon équilibre entre les exigences en matière de protection des données, le sentiment de sécurité de larges cercles de la population et l'utilisation et l'utilité des données du DEP pour un traitement meilleur et plus sûr des patients. Le patient peut en tout temps adapter ce paramétrage à ses besoins individuels, en particulier immédiatement après l'ouverture de son DEP.

Afin de ne pas devoir adapter séparément chaque paramètre de la gestion des accès, des profils prédéfinis de gestion d'accès différant du paramétrage par défaut peuvent être proposés au patient Il est ainsi possible d'aider tous les patients qui souhaitent définir simplement un paramétrage plus ouvert ou plus restrictif de ses droits d'accès. Le choix d'un modèle différant du paramétrage par défaut n'exclut pas des adaptations individuelles ultérieures par le patient.

Un paramétrage par défaut des droits d'accès défini sur le plan juridique s'applique après le consentement de principe et l'ouverture d'un DEP. Le patient peut faire son choix parmi plusieurs profils prédéfinis. Tous les paramètres peuvent être adaptés à tout moment par le patient.	Recommandation 4 Paramétrage par défaut défini, choix de profils prédéfinis

L'attribution de droits d'accès est toujours limitée dans le temps et orientée sur le contexte de traitement. Les professionnels de la santé souhaitant un accès doivent donc disposer du droit d'accès aussi longtemps qu'il est judicieux et raisonnable pour un traitement optimale. En principe, le patient définit la durée des droits d'accès attribués.

Les droits d'accès sont limités dans le temps au niveau du paramétrage par défaut. Le patient peut modifier ou supprimer ces délais à tout moment.	Recommandation 5 Limitation dans le temps des droits d'accès

L'attribution du niveau de confidentialité d'un document et l'évaluation de cet attribut jouent un rôle primordial dans le processus de gestion des droits d'accès. Les règles qui s'appliquent à l'attribution des niveaux de confidentialité initiaux lors de la publication des documents dans le DEP sont parties intégrantes du paramétrage par défaut.

Définition des niveaux de confidentialité

Selon les principes fondamentaux, le patient peut adapter le niveau de confidentialité de chaque document à tout moment. Pour un aspect plus pratique de la gestion des niveaux de confidentialité, le patient peut établir de manière sommaire des règles simples et compréhensibles sur la base des métadonnées des documents.

Le patient peut à tout moment définir des règles pour la définition sommaire des niveaux de confidentialité de documents. Le portail d'accès de sa communauté de référence offre ces fonctions.	Recommandation 6 Règles relatives à la définition des niveaux de confidentialité
Afin d'assurer le contrôle du patient sur les contenus de son DEP, il convient d'adapter les recommandations 5 et 6 tirées des « Recommandations III » du projet partiel « Normes et architecture » du 27 octobre 2011. La possibilité d'accéder aux données démographiques du patient permet de garantir que les administrateurs de patients (auxiliaires) et les professionnels de la santé puissent trouver et identifier de manière univoque les patients correspondants dans le système du DEP. Par ailleurs, seul le patient doit pouvoir consulter des documents présentant le niveau de confidentialité « données secrètes ». Si des documents affichant le niveau de confidentialité « données secrètes » devaient être rendus accessibles, le patient devrait alors modifier en conséquence le niveau de confidentialité du document à « données sensibles » ou « données médicales ».	Adaptation des recommandations 5 et 6 tirée des « Recommandations III »
La matrice de droits et le paramétrage par défaut représenté doit être appliqué à l'ouverture d'un DEP. Le patient peut modifier en tout temps les champs modifiables de la matrice. Dans ce cas s'applique la règle que les paramètres moins restrictifs des niveaux de confidentialité sont toujours sous-entendus.	Recommandation 7 Utilisation de la matrice de droits

		Niveaux de confidentialité						
		Données démographiques	Données utilitaires	Données médicales	Données sensibles	Données secrètes		
Acteurs DEP	Administrateur de patients	✓/✗	✗	✗	✗	✗	Niveau d'accès « administratif »	Niveaux d'accès
	Professionnel de la santé avec contexte de traitement	✓/✗	✓/✗	✗	✗	✗	Niveau d'accès « limité »	
		✓	✓	✓	✗	✗	Niveau d'accès « normal »	
		✓	✓	✓	✓	✗	Niveau d'accès « étendu »	
		✓	✓	✓	✗/✓	✗	Niveau d'accès « urgence »	
	Patient	✓	✓	✓	✓	✓	Niveau d'accès « global »	

✓/✗= Le paramétrage par défaut est oui. ✗/✓= Le paramétrage par défaut est non.

Illustration 6 : Parametrage par défaut

Remarque : A chaque paramétrage par défaut ou profil prédéfini s'applique toujours le principe d'« attribution explicite d'un niveau d'accès à un professionnel de la santé pour accéder à des contenus du DEP » (cf. également Recommandation 3). Des « droits d'accès automatiques » ne sont pas possibles.

2.4 Habilitation et représentation

Utilisation des possibilités d'habilitation

Dans certaines situations, il peut être judicieux pour le patient d'attribuer également à son professionnel de la santé le droit d'attribuer un niveau d'accès à un professionnel de la santé en tant que représentant. Le processus d'habilitation doit être réalisé par voie électronique. Cela signifie que le processus d'habilitation doit être vérifié, consigné et journalisé électroniquement.

Puisque la matrice de droits ne peut être modifiée qu'au sein d'une communauté de référence, le patient peut uniquement habiliter des professionnels de la santé dans sa communauté de référence afin qu'ils attribuent à leur tour un niveau d'accès à d'autres professionnels de la santé en tant que représentant. Ces professionnels de la santé bénéficiant désormais d'une autorisation d'accès peuvent se trouver aussi bien dans la même communauté de référence que dans d'autres communautés.

Recommandation 8

Habilitation à attribuer des niveaux d'accès

Le patient peut habiliter des professionnels de la santé de sa communauté de référence pour attribuer un niveau d'accès à un autre professionnel de la santé à sa place. Les professionnels de la santé habilités ne peuvent attribuer au maximum que le niveau d'accès qu'ils possèdent eux-mêmes à ce moment.

Le processus d'habilitation doit être réalisé par voie électronique et journalisé en conséquence. Une habilitation est limitée dans le temps et peut en tout temps être révoquée par le patient.

L'habilitation à attribuer des niveaux d'accès en tant que représentant du patient ne peut pas être transmise par des professionnels de la santé. Le patient est informé de toutes les demandes et attributions de droits d'accès.

Représentation du professionnel de la santé

Si un patient consulte un remplaçant de son professionnel de la santé (par exemple pour cause d'absence ou de congé), la gestion des accès ne prévoit aucun mécanisme particulier. Comme ailleurs, le patient doit pour cela attribuer explicitement les droits d'accès au remplaçant de son professionnel de la santé.

Représentation du patient

Les règles usuelles du droit civil s'appliquent aux possibilités de représentation d'un patient en cas d'incapacité de discernement ou lorsque le patient est mineur.

2.5 Droits d'accès de groupes de professionnels de la santé

Aspect de groupe

Des institutions, des organisations ou des groupes virtuels (tels que des cabinets de groupe, des stations dans les hôpitaux, des services d'aide et de soins à domicile ou un groupe d'experts, par exemple un *Tumor Board*) sont souvent impliqués dans le processus de traitement. Il est alors nécessaire de pouvoir garantir à ces organisations ou groupes de professionnels de la santé le droit d'accès au DEP d'un patient.

Utilisation pratique pour le patient

Il faudrait par ailleurs que le patient ait la possibilité de trouver des groupes de professionnels de la santé dans un service d'interrogation et d'attribuer les droits d'accès de manière sommaire à tous les membres de ce groupe. Dans ce cadre, le patient peut exclure différents professionnels de la santé d'un groupe bénéficiant d'un accès. Selon le principe « l'accès est autorisé pour autant qu'il soit nécessaire à l'accomplissement des tâches requises », l'accès au DEP d'un patient devrait uniquement être attribué (même en cas d'attributions d'autorisations de groupes) aux personnes de chaque groupe qui ont effectivement besoin des données qu'il contient pour leur travail.

Groupes et service d'interrogation HOI

Un service d'interrogation doit permettre de savoir quels professionnels de la santé se trouvent dans un groupe. Ce service d'interrogation est le service « Health Organisation Index » (service HOI). Un Tumor Board peut par exemple être mentionné comme un « groupe virtuel » dans le HOI. Un professionnel de la santé peut appartenir à plus d'un groupe.

Recommandation 9

Illustration d'un groupe dans le service d'interrogation HOI

Il est possible de former des groupes de professionnels de la santé afin de simplifier la gestion des droits d'accès. Les membres d'un groupe doivent être représentés dans le HOI. Le département notifiant de la communauté certifiée est responsable de l'entretien d'un groupe.

Obligations d'information des organisations

Tous les professionnels de la santé enregistrés dans le HPI doivent être informés par leurs organisations lorsqu'ils doivent être intégrés nommément en tant que membre d'un groupe dans le HOI. Les professionnels de la santé peuvent renoncé à cette solution en invoquant la protection des données.

2.6 Mise à disposition de documents dans le dossier électronique du patient

Si une personne donne son accord pour l'ouverture d'un DEP, il est supposé, dans le cas d'un traitement et conformément au projet LDEIP, que cette personne accepte la saisie des données pertinentes en matière de traitement dans le DEP. Les communautés doivent garantir que ces données destinées aux professionnels de la santé soient accessibles avec les droits d'accès correspondants via le DEP. Il n'existe par conséquent aucun lien obligatoire entre les droits de lecture et les droits d'écriture.

Recommandation 10

Mise à disposition de documents

En cas de traitement, il est supposé que le patient approuve la mise à disposition des données pertinentes en matière de traitement dans le DEP. Il n'est pas nécessaire de requérir un consentement explicite.

Le patient peut cependant se prononcer en tout temps contre la mise à disposition de certains documents. Il doit informer les professionnels de la santé correspondants de sa décision.

3 Remarques finales et questions ouvertes

Résumé

Les « Recommandations V » concrétisent les règles de gestion des droits d'accès dans le DEP. L'objectif principal est ici que le patient conserve le contrôle sur ses données et qu'il définisse qui peut travailler avec celles-ci. Il faudra également trouver un équilibre judicieux entre les exigences en matière de protection des données, la simplicité d'utilisation et la sécurité de traitement. La gestion des droits d'accès devrait être facile à utiliser pour les patients et prévoir, dans l'intérêt de la sécurité du patient, des instruments permettant aux professionnels de la santé impliqués d'accéder de manière pratique aux données en cas de besoin médical.

Prochaines étapes

Les prochaines étapes seront consacrées aux domaines thématiques suivants liés aux travaux réalisés jusqu'à présent :

- Définition de l'ensemble des attributs de droits avec concrétisation des attributs nécessaires à la gestion des droits d'accès ;
- Définition des processus liés à la gestion des consentements des patients sur le plan intercommunautaire ;
- Définition des processus à l'ouverture ou à la fermeture d'un DEP.

Points ouverts

Lors de l'élaboration de ces recommandations sont apparus certains points pour lesquels il n'a pas été possible de trouver un consensus ou qui doivent encore faire l'objet d'une analyse approfondie :

- Question : comment est-il possible de garantir que le patient d'un groupe de professionnels de la santé puisse attribuer un droit d'accès sans devoir administrer toutes les modifications de la composition du groupe dans ses droits d'accès ?
- Question : comment est-il possible de garantir qu'un professionnel de la santé puisse être enregistré rapidement et simplement dans le HPI afin que le patient puisse attribuer ses droits d'accès ?
- Question : comment est-il possible de garantir que le HOI sera maintenu à jour facilement et en toute sécurité par les départements notifiants ? Quels seraient les processus nécessaires pour cela et ceux-ci sont-ils applicables aujourd'hui ?
- Question : les droits d'écriture d'un professionnel de la santé ne disposant pas de droits de lecture doivent-ils être valables dans le cadre du paramétrage par défaut ou sous forme d'option pour le patient ?
- Question : les profils prédéfinis proposés doivent-ils faire l'objet d'un contrôle de qualité et donc être soumis à une certification ?

- Question : comment la réglementation des représentations peut-elle être concrètement mise en œuvre ? Par exemple, comment une mère peut-elle bénéficier de l'accès au DEP de son enfant mineur ?

- Analyse : comment les mécanismes actuels de l'autorisation des accès dans un environnement hospitalier peuvent-ils être alignés sur les besoins en matière de gestion des accès du système du DEP ?

- Analyse : comment l'« Informed Consent » doit-il être structuré pour qu'il soit le plus facilement compréhensible aussi bien de manière générale que pour tous les protagonistes du système ?

- Analyse : comment les exigences élevées en matière de temps réel sont-elles techniquement réalisables pour la gestion des accès (par exemple évaluation de la matrice de droits actuelle ou actualité du HPI et du HOI) ?