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

Fiche d'information

Saisie de données médicales dans le DEP par un utilisateur technique

Dans les grandes institutions de santé en particulier, les données médicales sont d'abord transférées du système primaire (p. ex. système informatique hospitalier, SIH) vers un système d'archive (universelle). À partir de cette archive, l'enregistrement des données dans le dossier électronique du patient (DEP) au sein des établissements de santé affiliés à une communauté (de référence) DEP se fait de manière automatique – dans le rôle de l'acteur IHE *Document Source* –, sans l'intervention de professionnels de la santé interagissant avec le système. Ce cas de figure concerne les hôpitaux, mais aussi d'autres architectures de DEP. Il s'agit d'une « mise à disposition de documents par un utilisateur technique ».

La présente fiche d'information expose les conditions à respecter pour que la procédure de mise à disposition de documents par des utilisateurs techniques (rôle de *technical user*, « TCU ») soit conforme aux prescriptions légales. D'une manière générale, les règles à observer sont les mêmes que pour l'enregistrement de documents médicaux par des professionnels de la santé :

- la responsabilité au niveau des contenus des documents médicaux mis à disposition est soumise aux principes d'imputabilité (*accountability*) et de non-répudiation (*non repudiation*) ;
- la responsabilité pour la sélection/mise à disposition des documents médicaux est soumise aux principes d'imputabilité (*accountability*) et de non-répudiation (*non repudiation*) (cf. art. 10, al. 1, let. b, LDEP). Si la sélection et la mise à disposition ont lieu de manière automatique sur la base de critères prédéfinis, la personne responsable de la définition et de l'activation des critères doit pouvoir être identifiée sans équivoque, ce qui requiert une authentification forte à deux facteurs.
- Les patients doivent avoir la possibilité de révoquer le consentement présumé pour l'enregistrement de documents médicaux (cf. art. 3, al. 2, LDEP et art. 10, al. 2, let. a, ODEP).

Le respect de ces directives est vérifié dans le cadre de la certification.

Saisie de données médicales dans le DEP par des utilisateurs techniques : authentification

Lorsque des documents sont mis à disposition dans le DEP par un utilisateur technique, il est là aussi nécessaire de vérifier, avant le traitement des données (i. e. la saisie des données médicales), qu'il s'agit bien d'un utilisateur autorisé et authentifié. La communauté (de référence) doit donc garantir que les données sont transmises par un système autorisé et authentifié (acteur IHE, rôle *Document Source*) provenant d'une institution de santé affiliée (cf. ch. 4.6.2, let. j et ch. 4.6.3 de l'annexe 2 de l'ODEP-DFI).

En cas de « saisie par des utilisateurs techniques », la décision d'autorisation (*CH:ADR*) doit également être établie à l'aide de la configuration des droits d'accès *(« policy stack » ; CH:PPQ*). Par

conséquent, la communication du *Document Source* requiert une *CH:XUA User Assertion (User Authorization Token)* signée par le *X-Assertion Provider*, comme pour les utilisateurs physiques. Toutefois, il n'est pas possible pour un utilisateur technique de s'authentifier contre un *Identity Provider* (*User Authentication Provider, IdP*). Seules les personnes physiques peuvent le faire à l'aide d'une authentification à deux facteurs.

Pour que l'utilisateur technique (i. e. le système qui transmet les données ou l'application) puisse être identifié de manière claire et sûre, celui-ci doit être authentifié par un *CH:XUA User Authentication Token* (techniquement, une *SAML 2 Identity Assertion*). Le TCU génère lui-même la *SAML 2 Identity Assertion*, qui doit être signée par un certificat reconnu (p. ex. X-509) et enregistré dans la communauté (de référence). Le certificat doit être valable et permettre d'identifier sans équivoque le TCU. La gestion correcte de ces certificats, des attributions aux systèmes et, partant, de la fiabilité des identités déclarées des systèmes dans le rôle de TCU est du ressort de la personne responsable de la protection et de la sécurité des données pour la communauté (de référence).

Afin de pouvoir obtenir le nécessaire *CH:XUA User Authorization Token* du X-Assertion Provider, la validité, l'authenticité et l'intégrité du *User Authentication Token* préalablement établi et auto-signé doivent être confirmées par le *X-Assertion Provider*. Lorsque ce dernier peut confirmer la validité, l'intégrité et l'authenticité du *User Authentication Token* du TCU, il peut générer le *CH:XUA User Authorization Token* requis par le contrôle des droits d'accès. Le *CH:XUA User Authorization Token* généré par le *X-Assertion Provider* contient le rôle de « TCU » dans l'attribut (« *subject role* ») pour la personne qui agit. L'utilisateur technique agit dans le système « sur mandat » d'un professionnel de la santé. Du point de vue juridique, il joue un rôle analogue à celui d'un auxiliaire. Le professionnel de la santé responsable est mentionné dans l'attribut pour la personne responsable (« *principal name* »). Il s'agit ici de la responsabilité pour la mise à disposition des données, et non pas de la responsabilité des contenus (cf. ci-après). En cas de transmission automatisée par le TCU sur la base d'une règle donnée, il faut indiquer comme référence la personne qui assume la responsabilité juridique des règles définies. La responsabilité juridique ne peut être assumée que par des professionnels de la santé qui participent au DEP et sont inscrits dans le HPD.

Saisie de données médicales dans le DEP par des utilisateurs techniques : métadonnées

Lorsque des documents sont mis à disposition par des utilisateurs techniques, il convient là aussi de s'assurer que les utilisateurs autorisés ont accès en tout temps à l'information sur l'auteur des données médicales – personne ou unité d'organisation – que ce soit lors de la consultation du DEP (*Document Registry*) ou des données de l'historique (*CH:ATC*). À cet effet, les métadonnées devront au moins inclure une indication sur la division ou la clinique de l'institution de santé ayant établi les données médicales. Les métadonnées du document devront aussi permettre de voir quel professionnel de la santé est responsable de l'exactitude des données du point de vue médical (p. ex. l'attribut *authorPerson* contient le GLN et le nom de l'auteur). Éventuellement, cette information peut aussi être tirée des données sur l'auteur dans le document lui-même (informations visibles à l'ouverture du document). Les métadonnées pertinentes peuvent être livrées du système primaire au système d'archive ou être directement établies et complétées dans ce dernier.

Mise en œuvre de la révocation du consentement supposé lors de la saisie de données médicales dans le DEP par des utilisateurs techniques

La communauté et la communauté de référence adoptent des dispositions au plan organisationnel (ou technique) pour les cas où un patient ne souhaite pas que certaines données médicales liées à un

traitement soient enregistrées dans le DEP. Cette procédure doit aussi s'appliquer à la saisie de données médicales par des utilisateurs techniques.

Délai pour la saisie des données médicales dans le DEP

Pour l'heure, aucune prescription légale ne fixe de délai pour l'enregistrement des données de traitement pertinentes dans le DEP. Il appartient aux communautés et aux communautés de référence d'élaborer une directive interne pour la saisie des données dans le DEP et d'engager les institutions de santé à la respecter par voie contractuelle – sauf si des dispositions de rang supérieur le prévoient déjà (p. ex. des lois cantonales). Ce faisant, il importe de s'assurer que les délais sont définis de manière à ne pas contrecarrer les objectifs visés par le DEP (soutien des processus de traitement, promotion de la sécurité des patients, amélioration de la qualité des soins, etc.). Si nécessaire, il convient par ailleurs de prévoir des réglementations spéciales pour l'enregistrement de données sensibles, dont le patient ne devrait prendre connaissance qu'en présence d'un professionnel de la santé. La directive établie doit s'appliquer à la saisie de données médicales par les professionnels de la santé et par les utilisateurs techniques.

Nouvelles versions de métadonnées et/ou de documents

Les *Document Sources* ne pouvant obtenir de droits d'accès pour la lecture de données médicales dans le rôle de TCU, il n'est en principe pas possible d'actualiser des données déjà enregistrées (autrement dit de transmettre de nouvelles versions de documents ou de métadonnées). Techniquement, cela serait faisable tant que l'*UUID* de l'ensemble de métadonnées établi lors de la mise à disposition des données par le TCU n'a pas changé. Si entre-temps un nouvel ensemble de métadonnées a été généré avec un nouvel *UUID*, par exemple parce que le patient a modifié le niveau de confidentialité, la transaction échouera. Cela étant, il est recommandé de ne pas procéder à une actualisation des métadonnées après une première saisie par un TCU. Le cas échéant, cette possibilité peut être exclue par une consigne d'ordre technique et normatif (p. ex. pas d'autorisation de *XDS Metadata Update* dans le rôle de TCU).