Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

DEP : les dix mesures de sécurité essentielles

La protection et la sécurité des données (PSD) jouent un rôle essentiel dans le cadre du dossier électronique du patient (DEP). Les critères techniques et organisationnels de certification (CTO ; annexe 2 de l'ODEP-DFI) applicables aux communautés et aux communautés de référence comptent plus de cent exigences relatives à la PSD. Le processus formel de certification veille à garantir le respect de ces exigences.

Le DEP est soumis aux normes de sécurité les plus strictes, lesquelles ont une valeur juridique en raison de leur ancrage dans la loi. Cette fiche d'information présente dix mesures de sécurité importantes au niveau de l'application (A), de la technique (T) et de l'organisation (O).

Mesures de sécurité visant à protéger le **niveau de l'application (A) :**

A1	Identification sécurisée et authentification dite à deux facteurs (2FA) de tous les utilisateurs
A2	Gestion autonome par les patients de l'accès à leur DEP
A3	Historisation de tous les accès à un DEP
A4	Réglage par les patients de la durée de conservation des données dans leur DEP

Mesures de sécurité pour une exploitation sûre des **systèmes et réseaux techniques (T)** :

T1	Détection d'anomalies et alarme automatique
T2	Conservation cryptée des données en Suisse
T3	Lignes de communication sécurisées

Mesures de sécurité au **niveau organisationnel (O)** :

O1	Gestion continue de la sécurité, y compris obligation de déclarer les incidents de sécurité
O2	Choix et formation des utilisateurs et du personnel administratif
O3	Contrôles de sécurité

Cette liste n'est pas exhaustive. Elle devrait toutefois permettre de démontrer pourquoi le DEP figure à l'heure actuelle parmi les applications les plus sûres, et pourquoi il le restera à l'avenir.

Toute mesure de sécurité a ses limites ; c'est également le cas pour le DEP. Les tableaux suivants présentent une description des dix mesures de sécurité les plus importantes pour le DEP et évaluent non seulement leur efficacité en matière de sécurité, mais aussi leurs limites.

ehealthsuisse
Kompetenz- und Koordinationsstelle von Bund und Kantonen
Centre de compétences et de coordination de la Confédération et des cantons
Centro di competenza e di coordinamento di Confederazione e Cantoni

Schwarzenburgstrasse 157
CH-3003 Bern

www.e-health-suisse.ch

Mesures de sécurité au niveau de l'application (A)

A1	**Identification sécurisée et authentification à deux facteurs de tous les utilisateurs**
L'inscription au DEP requiert, en sus d'un mot de passe ou d'une caractéristique biométrique (facteur « savoir » ou « être »), un moyen d'identification sécurisé (facteur « avoir »). Ce moyen d'identification doit correspondre au niveau de confiance 3 défini dans la norme ISO/IEC 29115:2013 et doit être délivré par un fournisseur certifié (également appelé *identity provider*, ou IdP).	
Efficacité en matière de sécurité	L'authentification à deux facteurs constitue une mesure efficace pour lutter contre l'usurpation d'identité. Elle peut en particulier empêcher les pirates informatiques de se connecter au DEP d'un patient au moyen de données de connexion volées.
Limites	Les utilisateurs doivent veiller à ce que leur moyen d'identification soit conservé de manière sécurisée ; ils doivent ignorer les courriels d'hameçonnage et s'abstenir, dans ce contexte, de révéler des informations secrètes (p. ex. des mots de passe) ou d'exécuter des logiciels malveillants.
Références	Art. 7 LDEP ; art. 9, 17, 23 à 27 et 31 ODEP ; CTO points 1.4, 1.6.2, 4.13.1 et 8.3

A2	**Gestion autonome par les patients de l'accès à leur DEP**
Avant toute consultation d'un document contenu dans un DEP, le système vérifie que l'utilisateur dispose du droit d'accès requis. Seuls les patients disposent d'un accès complet à leur DEP : ils peuvent définir quels professionnels de la santé y ont également accès, pour quels niveaux de confidentialité des documents cet accès est valable et si celui-ci peut être transféré à d'autres professionnels de la santé. Les autres groupes de personnes (p. ex. caisses maladie, chercheurs, autorités) n'ont pas accès au DEP. S'ils le souhaitent, les patients peuvent déléguer leurs propres droits (y compris le droit de transmettre leurs droits) à un ou à plusieurs représentants (p. ex. à un membre de leur famille). Une description détaillée de la transmission des droits d'accès est disponible sur la page Internet consacrée au DEP, sous la rubrique www.patientendossier.ch/fr/population/informations/fonctions/transmettre-des-droits-dacces.	
Efficacité en matière de sécurité	Le système de contrôle d'accès du DEP donne aux patients le droit à l'autodétermination en matière d'information concernant leurs données médicales. La législation soutient également l'application de ce droit dans la mesure où tout accès abusif à un DEP est sanctionné par une lourde amende, en vertu de l'art. 24 LDEP.
Limites	Les professionnels de la santé doivent intégrer les documents pertinents pour le traitement dans leurs propres systèmes. En téléchargeant ces documents, ils sortent du champ d'application du contrôle d'accès au DEP ; dès lors, les procédures internes des différentes institutions de santé (hôpitaux, cabinets médicaux, etc.) sont applicables. L'autodétermination en matière d'information implique une responsabilité personnelle importante. Lors de la transmission de leurs droits d'accès, les patients doivent faire preuve de prudence et avoir confiance en leurs représentants.
Références	Art. 9 et 24 LDEP ; art. 1 à 4 ODEP ; CTO points 2.1 à 2.3

A3	Historisation de tous les accès à un DEP
Chaque accès à un document contenu dans un DEP est historisé. Les patients peuvent à tout moment se rendre sur le portail d'accès qui leur est destiné et voir qui a accédé quand à quel document. Ils peuvent en outre être activement informés (p. ex par SMS) des accès en cas d'urgence ou des changements dans la composition des groupes de professionnels de la santé. Les données du protocole sont conservées pendant dix ans et ne peuvent pas être supprimées – même par le patient.	
Efficacité en matière de sécurité	L'historisation assure un degré très élevé de traçabilité ; elle a également un effet préventif et dissuasif, car toute personne accédant au DEP doit s'attendre à devoir prouver la légalité de l'accès.
Limites	Si l'historisation permet de détecter et de poursuivre en justice tout accès abusif, elle ne permet pas de les empêcher ou de les effacer rétroactivement.
Références	Art. 10 LDEP ; art. 9 et 18 ODEP ; CTO points 2.10 et 9.3

A4	Réglage par les patients de la durée de conservation des données dans leur DEP
Sauf demande contraire du patient, les données contenues dans son DEP sont supprimées automatiquement après 20 ans. Les patients peuvent toutefois effacer leurs données à tout moment ou les exclure du délai d'effacement.	
Efficacité en matière de sécurité	Les procédures de sauvegarde mises en place par les communautés (de référence) garantissent que les données médicales contenues dans le DEP ne soient pas perdues. Ces mesures n'affectent toutefois aucunement l'autodétermination des patients en matière d'information, en particulier leur « droit à l'oubli ».
Limites	Les professionnels de la santé doivent conserver les documents pertinents pour le traitement dans leurs propres systèmes. En téléchargeant ces documents, ils sortent du cadre juridique du DEP. Dès lors, les délais de conservation prévus par les législations cantonales s'appliquent.
Références	Art. 10 ODEP ; CTO points 9.4.1 et 10

Mesures de sécurité au niveau technique (T)

T1	Détection d'anomalies et alarme automatique
Chaque communauté (de référence) dispose d'un SIEM (*Security Information and Event Management*), qui permet de surveiller les données du protocole en permanence – y compris les journaux des événements techniques. Un ensemble de règles permet de détecter les modèles inhabituels (anomalies) qui indiquent une cyberattaque ou un accès abusif, déclenchant ainsi une alarme. Chaque communauté (de référence) dispose d'un processus de gestion des incidents de sécurité afin d'analyser l'alarme et, en cas de besoin, de prendre les contremesures nécessaires.	
Efficacité en matière de sécurité	L'identification automatique de potentiels incidents de sécurité permet de réagir rapidement face à une tentative d'attaque ou à un accès abusif.
Limites	Le système d'alarme DEP ne peut parfois que limiter un dommage, et non l'éviter.
Références	Art. 12 ODEP ; CTO points 4.3 et 4.15.6

T2	Conservation cryptée des données en Suisse
Les données contenues dans le DEP (y compris toutes les sauvegardes) sont enregistrées sous forme cryptée et conservées auprès d'entreprises sises en Suisse et donc régies par le droit national. Ces entreprises ne sont pas autorisées à utiliser les données à d'autres fins et ne peuvent être contraintes par une autorité étrangère à les transmettre.	

Efficacité en matière de sécurité	Le cryptage des données enregistrées permet de les protéger efficacement contre tout contournement du contrôle d'accès.
Limites	Seul un nombre restreint de personnes dont l'identité est connue (appelées *golden key holder* dans le jargon technique) peuvent obtenir un accès direct aux données. Les CTO définissent toute une série de mesures techniques et organisationnelles dans le domaine de la sécurité opérationnelle destinées à réduire autant que possible le risque lié à ces « insiders ».
Références	Art. 10 et 12 ODEP ; CTO points 2.5.b, 13 à 15 et 19

T3	**Lignes de communication sécurisées**
Les communautés (de référence) constituent avec les institutions de santé affiliées un espace de confiance qui, grâce à des systèmes de cryptage basés sur les protocoles TLS (*Transport Layer Security*), est isolé d'Internet. La configuration sécurisée de l'ensemble des points d'accès TLS est régulièrement vérifiée à l'aide de détecteurs de failles (ou *vulnerability scanner*s).	
Efficacité en matière de sécurité	Une utilisation systématique de la MTLS (*Mutually authenticated Transport Layer Security*) permet d'empêcher que des lignes de communication indésirables soient établies avec l'espace sécurisé du DEP ou que des lignes de communication soient mises sur écoute au sein de cet espace.
Limites	Afin que le cryptage soit efficace, il est nécessaire que tous les participants à l'espace sécurisé du DEP gèrent leur clé de communication secrète conformément aux prescriptions légales.
Références	Art. 10 ODEP ; CTO points 2.5.a, 4.12 et 4.15

Mesures de sécurité au niveau organisationnel (O)

O1	**Gestion continue de la sécurité, y compris obligation de déclarer les incidents de sécurité**
Dans chaque communauté de référence, un responsable PSD veille à ce que les risques en matière de sécurité soient continuellement identifiés, évalués et limités. Il échange régulièrement des informations avec les autorités et ses collègues des autres communautés (de référence) et peut, en cas de besoin, ordonner des mesures de sécurité allant au-delà des dispositions légales. Le responsable PSD gère également la procédure prescrite par la loi pour l'annonce immédiate à l'OFSP des incidents en lien avec la protection et la sécurité des données.	
Efficacité en matière de sécurité	Une organisation de la sécurité solide avec des procédures établies assure la base indispensable pour améliorer continuellement le dispositif de sécurité et l'adapter à son environnement en constante évolution. Pour la première fois dans le domaine de la santé, le DEP introduit au niveau national une obligation de déclarer les incidents de sécurité ; la transparence et le pilotage des mesures en matière de protection et de sécurité des données sont ainsi encouragés.
Limites	Même avec une excellente gestion de la sécurité, il est impossible d'atteindre un niveau de sécurité absolu.
Références	Art. 12 ODEP ; CTO points 4.2, 4.3.3.a et 4.11

O2	**Choix et formation des utilisateurs et du personnel administratif**
La formation PSD (*Awareness Training*) est un élément obligatoire de la formation DEP destinée à l'ensemble des professionnels de la santé et du personnel administratif (p. ex. centres d'assistance, exploitants du système). Tous ces groupes de personnes, pour autant qu'ils ne soient pas déjà soumis au secret médical, doivent signer une déclaration de confidentialité. La sélection minutieuse du personnel des communautés (de référence) et de leurs fournisseurs de plateformes inclut également l'examen obligatoire des registres des poursuites et des casiers judiciaires.	

Efficacité en matière de sécurité	Toutes les personnes disposant d'un accès au DEP sont conscientes du caractère particulièrement sensible des données qu'elles traitent. Elles disposent d'une formation de base sur le traitement des données de ce type et connaissent les dispositions pénales en cas de comportement fautif, ce qui réduit la probabilité d'infractions intentionnelles et non intentionnelles au strict minimum.
Limites	Il est impossible d'éviter complètement les erreurs d'utilisation concernant le DEP.
Références	CTO points 4.2.2, 4.8, 4.9

O3	**Contrôles de sécurité**
Chaque communauté (de référence) dispose d'outils et de processus lui permettant d'identifier les failles en matière de sécurité (p. ex. logiciels obsolètes, patchs manquants, configurations non sécurisées) et de les réparer. Après chaque modification en matière de sécurité, et en particulier avant l'introduction d'une nouvelle version d'un logiciel, les accès au DEP sont par ailleurs vérifiés par des entreprises spécialisées (aussi appelées *white hat hacker*) afin d'identifier toute faille potentielle.	
Efficacité en matière de sécurité	Les erreurs de programme ou de configuration sont détectées et corrigées avant que l'application devienne accessible depuis Internet – et donc potentiellement sujette à une attaque.
Limites	Même les détecteurs de failles actuels (*vulnerability scanner*) et les *white hat hacker* les plus compétents ne sont pas en mesure de garantir de la détection de toutes les failles avant qu'un tiers y parvienne. Les failles récentes (ou *zero day exploits*), pour lesquelles aucun patch de sécurité n'est encore disponible, sont particulièrement dangereuses.
Références	CTO points 3.4.1, 3.4.2, 4.4, 4.5