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

Aide la mise en œuvre concernant la protection et la sécurité des données dans le cadre du DEP

Aide la mise en œuvre destinée aux responsables de la protection et de la sécurité des données des communautés et des communautés de référence

Berne, le 27 juin 2017

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

Impressum

Rédaction : Redguard AG, Eigerstrasse 60, 3007 Berne
Les personnes ayant participé à l'élaboration ou à la vérification de ce document sont mentionnées en annexe.

Informations supplémentaires et document auprès de :
www.e-health-suisse.ch

But et positionnement du présent document

L'aide la mise en œuvre a été élaborée par Redguard AG et encadrée techniquement par le groupe d'accompagnement. Le rapport peut être con-sulté sous www.e-health-suisse.ch. Les aides à l'exécution produites par eHealth indiquent aux acteurs concernés comment procéder dans l'envi-ronnement d'un réseau numérique. Les acteurs concernés sont libres de prendre à leur compte les propositions formulées dans ce document.

Pour faciliter la lecture du document, la forme générique est utilisée pour désigner les deux sexes.

Sommaire

1 Introduction

Dossier électronique du patient

Le dossier électronique du patient (DEP) a pour objectif de renforcer la qualité des traitements médicaux, d'améliorer les processus de traitement, d'augmenter la sécurité du patient, d'accroître l'efficience du système de santé et de promouvoir la culture sanitaire des patients.

La loi fédérale sur le dossier électronique du patient (LDEP) et les ordonnances d'exécution y relatives (ODEP, OFDEP, ODEP-DFI, annexes incluses) sont entrées en vigueur le 22 mars 2017. A partir de l'entrée en vigueur de la loi, les hôpitaux disposent de trois ans pour introduire le dossier électronique du patient, les établissements médico-sociaux et les maisons de naissance de cinq ans.

Les critères techniques et organisationnels applicables au DEP sont définis dans l'ordonnance. Les critères techniques et organisationnels de certification (CTO – Annexe 2 de l'ODEP-DFI) applicables aux communautés et communautés de référence en font également partie.

L'usage de l'informatique n'est pas suffisamment répandu en particulier dans les soins de santé ambulatoires : au niveau du corps médical, par exemple, seul un tiers, environ, des cabinets médicaux gère les informations des patients sous forme numérique (SISA II – Institut de médecine de premier recours de l'Université de Zurich). Il aura fallu pratiquement 20 ans pour atteindre ce degré de pénétration. Avec l'introduction du DEP, la situation ne manquera pas de changer et, selon toute probabilité, le nombre de prestataires de services qui opteront pour une documentation numérique augmentera rapidement. Le DEP constitue un changement important pour ces regroupements de professionnels de la santé et de leurs institutions que sont les communautés et les communautés de référence. Elaboré à partir de prescriptions de certification techniques et organisationnelles et en application de règles de bonnes pratiques internationales, le présent document a été conçu pour faciliter le travail des responsables de la protection et de la sécurité des données des communautés et communautés de référence.

Importance de la sécurité des données

Grâce au dossier électronique du patient, les professionnels de la santé seront en mesure d'accéder aux données de leurs patients que d'autres professionnels de la santé participant au processus thérapeutique auront établies. Ils pourront enregistrer ces données, saisies de manière décentralisée par les autres professionnels de la santé, dans les systèmes d'information de leur cabinet ou de leur clinique, en dehors du dossier électronique. Ils devront à cet effet s'affilier à une communauté ou à une communauté de référence certifiée et leurs patients devront leur accorder les droits d'accès nécessaires. Le dossier électronique du patient permettra en outre aux patients de consulter leurs propres données, de les rendre accessibles et de gérer les droits d'accès.

Le dossier électronique du patient est facultatif. Conformément au principe de l'autodétermination des patients en matière d'information, chaque personne décide elle-même de la tenue d'un dossier électronique et des droits d'accès qu'elle entend accorder aux professionnels de la santé en charge de ses traitements.

La protection des données traitées dans le cadre du dossier électronique revêt une importance majeure, en particulier en ce qui concerne la consultation non autorisée de données ou la fuite de données (confidentialité), les modifications non autorisées (intégrité) ou la mise à disposition de données en temps voulu. Un niveau de sécurité uniforme, applicable à toutes les organisations participantes, est ici visé. Cet objectif constitue une priorité absolue, d'autant plus que la confiance éprouvée par le patient représente un facteur de réussite essentiel. Il incombe à la communauté concernée d'assurer la protection des données et de garantir une sécurité adéquate des données.

1.1 Destinataires

Destinataires

Le présent document s'adresse en premier lieu aux responsables de la protection et de la sécurité des données des communautés et des communautés de référence.

Il s'adresse également aux fabricants et aux fournisseurs de produits ou de prestations en lien avec le DEP ainsi qu'aux organismes de certification.

1.2 Procédure

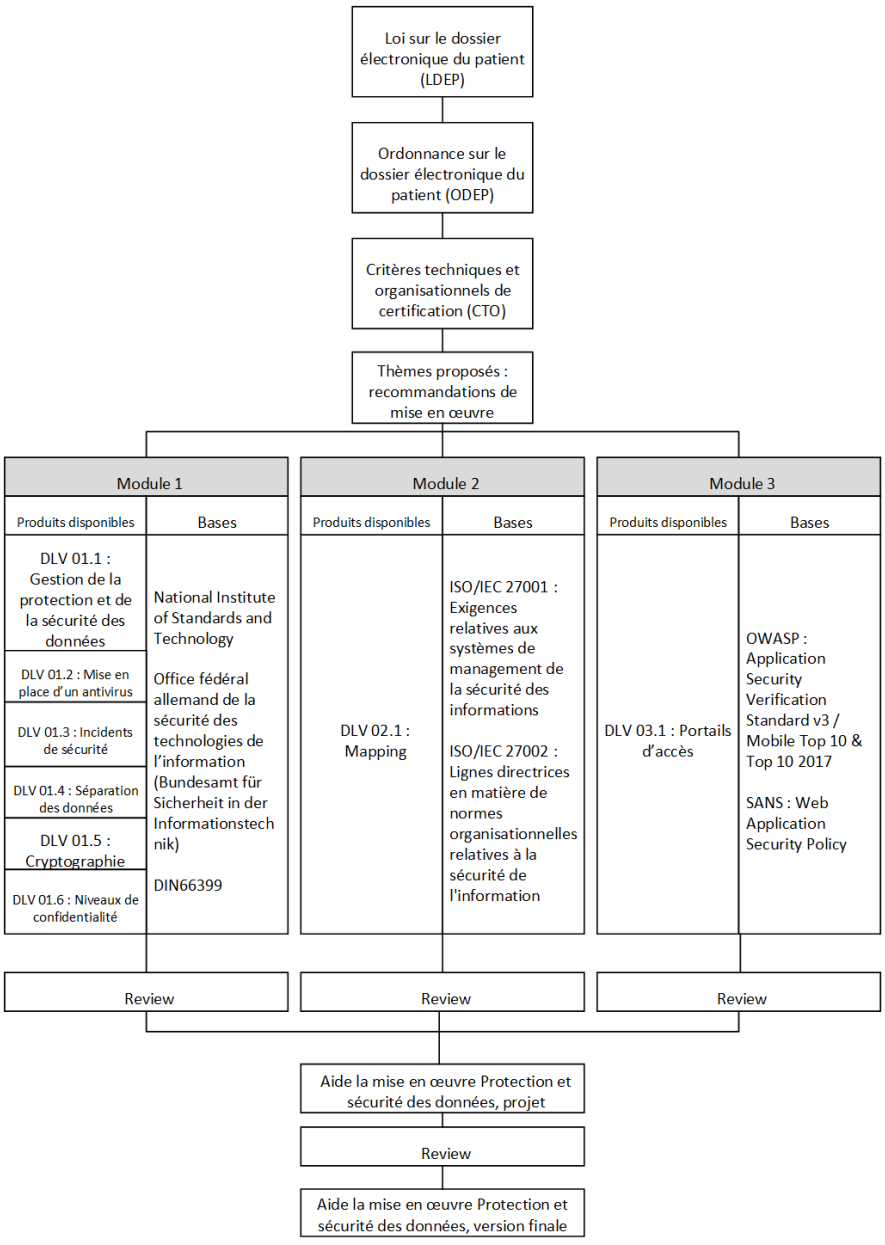

Figure 1 : Elaboration des aides à la mise en œuvre du DEP

1.3 Structure du document

Le présent document propose des aides à la mise en œuvre pour les thèmes suivants :

- Gestion de la protection et de la sécurité des données (structure selon CTO)
- Protection contre des logiciels malveillants
- Détection et traitement d'incidents de sécurité
- Séparation des données
- Cryptographie
- Protection contre la manipulation des niveaux de sécurité
- Sécurité des portails d'accès
- Tableau de mapping CTO/ISO

Les principaux contenus du document ont été définis conjointement avec le mandant et les membres du groupe d'accompagnement lors de l'élaboration de l'aide la mise en œuvre.

1.4 Délimitation

Délimitation

La présente aide la mise en œuvre :

- se limite à des aspects de protection et de sécurité des données ;
- couvre une sélection de thèmes mentionnés dans les CTO. Les thèmes retenus ont été définis au préalable avec le mandant et le groupe d'accompagnement ;
- ne prétend pas être exhaustive quant au contenu ni traiter les thèmes abordés dans leur intégralité ;
- se borne à formuler des recommandations sur la manière dont une situation spécifique peut être conçue ou réalisée ;
- requiert la collaboration de toutes les organisations impliquées en ce qui concerne la mise en œuvre des recommandations.
- ne garantit pas l'obtention de la certification, même si les mesures prévues sont mises en œuvre.

1.5 Bases

[LDEP]	Loi fédérale sur le dossier électronique du patient
[LPD]	Loi fédérale sur la protection des données
[ODEP]	Ordonnance sur le dossier électronique du patient
[CTO]	Annexe 2 : Critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence
[EPD-RA]	Bedrohungs- und Risikoanalyse Elektronisches Patientendossier

1.6 Instruments et références

[ISO27001]	ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements – non accessible publiquement
[ISO27002]	ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls - non accessible publiquement
[OWASP-Top10]	OWASP - Top 10 (2013)
[OWASP-MobileTop10]	OWASP - Mobile Top 10 (2016)
[OWASP-ASVS]	OWASP – Application Security Verification Standard 3.0
[OWASP-TLS-CS]	OWASP – TLS Cheat Sheet
[OWASP-TLS-TG]	OWASP – Testing Guide for SSL/TLS
[SANS-WASP]	SANS – Web Application Security Policy
[DIN66399]	DIN 66399 Technologie bureautique et des données – Destruction de supports de données – non accessible publiquement
[BSI-TR02102]	BSI – Kryptographische Verfahren: Empfehlungen und Schlüssellängen
[FIPS140.0]	Security Requirements for Cryptographic Modules
[NIST-SP-800-57]	Recommendation for Key Management
[Annonces CERT]	Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI BSI - CERT US-CERT

	Il existe également d'autres sources d'information, certaines payantes, relatives à la gestion des failles de sécurité et le traitement d'incidents de sécurité.
[CA-List]	Les listes suivantes peuvent être téléchargées à titre d'exemple : https://mozillacaprogram.secure.force.com/CA/IncludedCACertificateReport https://gallery.technet.microsoft.com/Trusted-Root-Certificate-123665ca
[Hardening-Guides]	NIST – Guide to General Server Security SANS – SCORE Checklists
[Incident-Handling]	ENISA – Good Practice Guide for Incident Management lers Handbook

1.7 Terminologie

Concept	**Définition dans le présent document**
Organisation	Communauté ou communauté de référence, tiers éventuellement concernés inclus
Infrastructure TIC	Environnement système en rapport avec le DEP, voir également CTO 4.6.2

2 Système de gestion de la protection et de la sécurité des données

2.1 Introduction

Introduction

La réalisation des exigences résultant des critères techniques et organisationnels de certification (CTO) implique la mise en œuvre de différentes mesures de sécurité.

La mise en œuvre et le maintien du niveau de sécurité qui a été défini requièrent une approche systématique. En conséquence, un système de gestion doit être élaboré pour administrer les principes et les mesures spécifiques des CTO.

Le système de gestion de la protection et de la sécurité des données contient tous les éléments indispensables pour atteindre et maintenir durablement le niveau de sécurité requis. Si une organisation possède déjà un système de gestion de la sécurité de l'information (ISMS) ou un système de gestion de la protection des données (SGPS), ceux-ci peuvent être complétés ou adaptés en tenant compte des critères spécifiques des CTO.

2.2 Gestion des professionnels de la santé et de leurs auxiliaires

Rubriques CTO applicables

1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.4.1, 1.6.2, 1.6.3

But du processus

Les processus de gestion des professionnels de la santé (auxiliaires inclus) garantissent que toutes les personnes ont été correctement identifiées et enregistrées et qu'elles se sont engagées à respecter les directives spécifiques et les instructions pratiques. Ils assurent par ailleurs que ces personnes disposent des moyens d'accès requis et des autorisations nécessaires, que ceux-ci sont actualisés tant que durent les rapports de service et révoqués en cas de sortie.

Activités

Obligation de respecter les directives : les aspects ci-dessous doivent être définis spécifiquement pour chaque organisation au moyen de directives internes et d'instructions pratiques :

- la gestion des caractéristiques d'authentification,
- l'utilisation de moyens informatiques,
- la gestion d'informations et de données sensibles,
- le point de contact pour toute question en rapport avec la sécurité.

Mise en œuvre : les processus de gestion des professionnels de la santé posent des exigences élevées en termes d'historisation. En conséquence, toutes les étapes des processus et les éventuelles décisions ou autorisations doivent être consignées. Pour limiter les erreurs de traitement et garantir l'historisation de toutes les étapes de traitement, il est recommandé d'exécuter autant que possible les processus administratifs au moyen d'un workflow assisté par ordinateur.

2.3 Gestion des risques

Rubriques CTO applicables

4.2.1 4.2.3

Le système de gestion des risques permet d'identifier, d'évaluer systématiquement et de traiter les risques pouvant mettre en danger la confidentialité, l'intégrité ou la disponibilité de données pertinentes du DEP. Il permet également de communiquer les éventuels problèmes non résolus à la personne qui supporte les risques.

Le processus de gestion des risques se présente sous la forme d'un cercle comprenant cinq phases, à savoir :

- l'identification des risques,
- l'analyse et l'évaluation des risques,
- la mise en œuvre de mesures,
- la surveillance.

Pour pouvoir gérer les risques, il faut d'abord les identifier. Ils doivent être identifiés aussi bien dans l'entreprise que dans le cadre d'un projet en cas de modifications. Il est également recommandé d'organiser au moins une fois par an un atelier dédié spécifiquement à la gestion des risques afin de dégager les risques existants et d'identifier d'éventuels nouveaux risques. Après avoir été identifiés, les risques doivent être évalués. A cet effet, il y a lieu d'élaborer un schéma d'évaluation uniforme permettant de se prononcer sur l'éventuelle survenance d'un risque et ses conséquences potentielles, pour l'organisation comme pour la personne concernée (patient). Il est important que l'évaluation se fasse selon un schéma uniforme au sein de l'organisation. Il faudrait également définir transversalement

des critères d'acceptation des risques (autrement dit, jusqu'à quel point un risque est considéré comme supportable et dans quelles conditions).

Il est préférable de traiter les risques en les regroupant par thème. De cette manière, les mesures s'appliqueront à l'ensemble d'un thème. Les risques restants devraient être communiqués à intervalles réguliers à celui qui les supporte en fonction de l'évaluation qui a été faite, mais au moins une fois par an ou après toute modification importante.

Tous les processus et étapes de traitement énoncés devraient être historisés au sein de l'organisation. Il est conseillé de prévoir des instruments adéquats pour les différentes étapes de traitement, comme des modèles ou des outils de support.

2.4 Sensibilisation du personnel

4.2.2

Rubrique CTO applicable

Information des collaborateurs

Pour qu'une communauté conserve durablement un niveau de protection des données élevé, les professionnels de la santé et leurs auxiliaires doivent être informés régulièrement des modifications techniques et organisationnelles qui ont été introduites, des prescriptions applicables et des procédures à observer. La sensibilisation des collaborateurs peut s'effectuer de différentes manières.

Moyens de communication à disposition

- **Formation au moment de l'entrée** : une formation concernant toutes les prescriptions pertinentes, les procédures et les outils disponibles devrait être proposée aux professionnels de la santé au moment de leur entrée dans la communauté. Pour une meilleure visibilité, cette formation devrait être dispensée par le responsable de la protection et de la sécurité des données.
- **Fiche d'information** : il est recommandé de remettre une fiche d'information sur le thème de la protection des données à tous les professionnels de la santé qui intègrent la communauté.
- **Portail de prescriptions** : toutes les prescriptions pertinentes en rapport avec la protection et la sécurité des données devraient être disponibles sur un portail centralisé. La présentation doit être simple et claire.
- **Communication des événements** : les événements relatifs à la sécurité et les mesures qui ont été prises devraient être communiqués rapidement aux collaborateurs (voir ch. 4).
- **Information des collaborateurs** : lorsque la protection et la sécurité des données font l'objet de modifications importantes (p. ex. à la suite de nouvelles dispositions légales), un courrier d'information correspondant devrait être adressé à l'ensemble des collaborateurs. Il s'agit de s'assurer que l'information est bien parvenue à tous les professionnels de la santé.
- **Formation continue** : étant donné que le rafraîchissement des connaissances participe à leur bonne assimilation, une formation consacrée à la protection et à la sécurité des données devrait être proposée régulièrement. Il est conseillé d'organiser au moins une formation par an. De cette manière, le sujet reste bien présent à

l'esprit des collaborateurs et les nouveautés peuvent être rapidement communiquées.

Le degré de sensibilisation des collaborateurs devrait être vérifié régulièrement. Des simulations et des tests peuvent être introduits à cet effet ; p. ex. par l'envoi de courriels fictifs de hameçonnage aux collaborateurs.

Vérification régulière du degré de sensibilisation

La mise en œuvre de mesures de sensibilisation et la participation des professionnels de la santé à ces mesures devraient être historisées à des fins de vérification.

Traçabilité des activités de sensibilisation

2.5 Gestion des failles de sécurité

4.4.1, 4.4.2

Rubriques CTO applicables

Les communautés doivent disposer d'un système de gestion des failles de sécurité qui recueille en temps utile des informations sur la fragilité technique des moyens informatiques exploités. Il incombe également à ce système d'évaluer l'importance des failles de sécurité et de prendre les mesures qui s'imposent. La gestion des failles de sécurité comprend cinq phases, comme indiqué dans la figure qui suit.

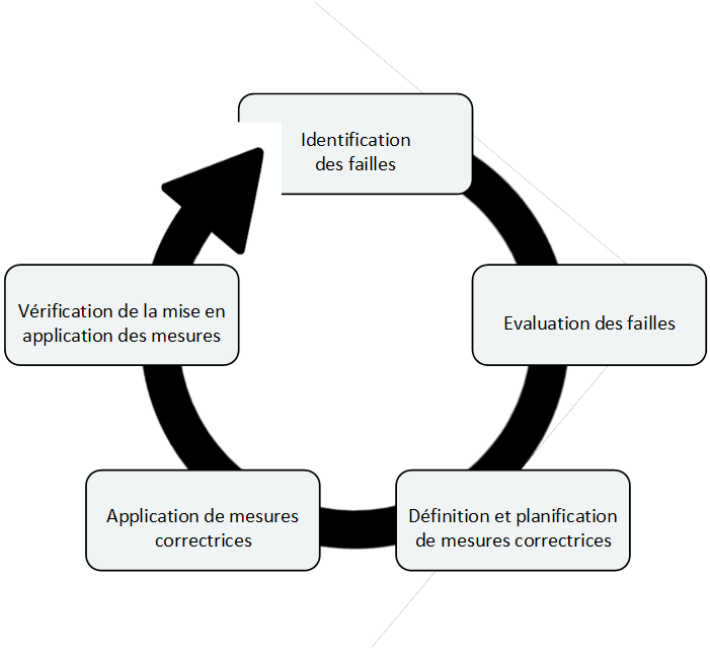

Figure 2 : Phases de la gestion des failles de sécurité

L'identification des failles de sécurité s'effectue au moyen d'un scanner de vulnérabilité (manuel ou automatique) ; tous les systèmes internes et externes sont analysés pour détecter d'éventuels points faibles. Les failles proviennent généralement de logiciels obsolètes, de configurations incorrectes ou d'erreurs de manipulation. Il est conseillé de procéder à une analyse du système une fois par mois.

L'appréciation devrait s'effectuer à l'aide d'un schéma prédéfini. Les failles de sécurité se répartissent généralement en quatre catégories :

- Risque critique : la confidentialité, l'intégrité et la disponibilité des données sont hautement menacées. Une intervention rapide s'impose d'urgence. C'est le cas, notamment, lorsqu'une faille de sécurité peut être exploitée par des outils automatiques.
- Risque élevé : la mise en danger est élevée. Elle implique toutefois que son auteur intervienne manuellement. Une intervention rapide s'impose néanmoins.
- Risque moyen : l'exploitation de la faille de sécurité nécessite un travail important ou n'est possible qu'en exploitant simultanément plusieurs autres failles indépendantes les unes des autres. La mise en danger doit être écartée à moyen terme mais ne requiert pas une intervention immédiate.
- Risque faible : le risque a peu d'impact sur les objectifs de protection / les failles de sécurité permettent à un auteur de collecter des informations supplémentaires via les systèmes. Dans la mesure du possible, les failles / risques de niveau « faible » devraient néanmoins être supprimés à moyen ou long terme.

Des mesures correctrices doivent être définies et planifiées rapidement, en fonction de la gravité des failles constatées. Le plan applicable comprend quatre étapes :

1. Estimation de la faille sur la base de l'appréciation faite lors de la phase d'évaluation.
2. Définition de mesures correctrices envisageables (également mesures compensatoires).
3. Appréciation et évaluation des mesures correctrices.
4. Test de fonctionnement après la mise en application de la mesure correctrice.
5. Planification de la mise en œuvre (phase opérationnelle)

Si l'on renonce à la mise en œuvre d'une mesure correctrice, les failles relevées doivent être répertoriées dans la gestion des risques ; la raison pour laquelle la mesure n'a pas été introduite doit être mentionnée. Toutes les failles de sécurité non encore traitées doivent être connues.

Les mesures correctrices qui ont été définies, planifiées et testées au préalable sont mises en œuvre sur la base de la planification antérieure.

La mise en application est vérifiée à la fin du processus. Les analyses effectuées régulièrement exercent aussi une fonction de contrôle. En cas de failles de sécurité jugées critiques, une analyse doit être effectuée rapidement après la mise en œuvre d'une mesure correctrice.

En outre, les éléments critiques devraient faire l'objet des tests de pénétration au moins une fois par an ou après l'introduction de modifications importantes. Si cela est possible, un programme de détection des bugs informatiques peut être créé dans le cadre du développement, en respectant toutefois les prescriptions et directives spécifiques à l'organisation considérée.

Enfin, il est conseillé d'exercer une surveillance passive des produits exploités. Il est possible de s'abonner à des feeds [messages CERT] signalant des failles de sécurité récentes. Les messages peuvent ensuite être comparés avec les données de l'inventaire.

2.6 Inventaire de l'infrastructure informatique

4.6.1, 4.6.2, 4.6.3, 4.6.5

Rubriques CTO applicables

Gestion de l'inventaire

L'ensemble des données, systèmes et dispositifs sensibles liés au dossier électronique du patient (CTO 4.6.1) est identifié, classifié, enregistré et tenu à jour dans un « inventaire de l'infrastructure informatique ». Il est conseillé de gérer l'inventaire dans un logiciel ad hoc. Les caractéristiques suivantes d'un élément devraient y figurer au minimum :

- le nom et la désignation,
- l'usage prévu,
- la classification,
- le lieu,
- le caractère physique ou virtuel du système,
- le propriétaire responsable,
- les autorisations d'accès à l'élément,
- les données d'identification (p. ex. ID système),
- les éléments d'adressage,
- les données relatives à la garantie et à la maintenance,
- les versions software exploitées (système d'exploitation, antivirus, applications et bibliothèques),
- les informations relatives aux certificats exploités.

Contrôle régulier

Le préposé à la sécurité des données procède au moins une fois par an au contrôle de l' « inventaire de l'infrastructure informatique ».

2.7 Procédure disciplinaire[1]

4.8.2

Rubrique CTO applicable

Infraction à la LPD

Les professionnels de la santé, leurs auxiliaires ou toute autre personne (p. ex. administrateur système) en contact avec des données du DEP qui enfreindraient la loi sur la protection de données (LPD) sont passibles de sanctions. Les sanctions peuvent être fixées sur une base contractuelle. Les contrats doivent non seulement prévoir des droits d'annulation, mais aussi des risques de responsabilité plus élevés et des peines conventionnelles supérieures en cas d'infractions à la législation sur la protection des données. La procédure suivante est conseillée :

1. identification de l'infraction,

[1] Correspond au processus de réglementation

2. estimation de l’importance de l’infraction,
3. définition de la sanction sur la base de l’estimation de l’infraction,
4. application de la sanction.

Il incombe à la communauté concernée de se prononcer sur la sévérité de la sanction.

Art. 35 Violation du devoir de discrétion

En cas de violation du devoir de discrétion, les sanctions peuvent également être fixées en application de l’art. 35 de la loi sur la protection des données : « La personne qui, intentionnellement, aura révélé d'une manière illicite des données personnelles secrètes et sensibles ou des profils de la personnalité portés à sa connaissance dans l'exercice d'une profession qui requiert la connaissance de telles données, est, sur plainte, punie de l'amende.

Est passible de la même peine la personne qui, intentionnellement, aura révélé d'une manière illicite des données personnelles secrètes et sensibles ou des profils de la personnalité portés à sa connaissance dans le cadre des activités qu'elle exerce pour le compte de la personne soumise à l'obligation de garder le secret ou lors de sa formation chez elle.

La révélation illicite de données personnelles secrètes et sensibles ou de profils de la personnalité demeure punissable alors même que les rapports de travail ou de formation ont pris fin. »

2.8 Gestion est surveillance de tiers

Rubriques CTO applicables

4.9.1, 4.9.2, 4.9.3, 4.9.4, 4.10

Le choix de l’offre la plus appropriée passe par une évaluation et une appréciation du fournisseur ainsi que des services proposés. Les aspects suivants doivent être étudiés :

- le respect des critères
- l’importance du domaine d’activité
- le traitement des données sur le plan géographique
- la juridiction applicable
- les références
- les évaluations indépendantes (audits de fournisseurs)

Tous les fournisseurs concernés qui accèdent à des données du dossier électronique du patient, les traitent, les enregistrent, les transmettent à des tiers ou qui proposent une infrastructure informatique à cet effet doivent être systématiquement enregistrés et agréés par le responsable de la protection et de la sécurité des données.

Contrat

La fourniture d’une prestation devrait être convenue par contrat. Le document doit prévoir au minimum les éléments suivants :

- le lieu de la prestation,
- le lieu de la conservation des données (également copies de sécurité et sites d’archivage secondaires),
- la définition de chiffres clé et les procédures de rapport,

- l’accessibilité (mesures),
- le respect de conditions légales et réglementaires (en particulier DEP et LPD),
- le respect de conditions générales et organisationnelles en matière de sécurité,
- le recours à des sous-traitants et leurs obligations,
- les exigences posées aux personnes concernées,
- la liste des personnes concernées,
- la gestion des modifications,
- la communication de modifications organisationnelles ou techniques,
- les moyens de communication et la hiérarchie d'escalade,
- la procédure en cas d’incident de sécurité,
- les dispositifs en cas d’urgence,
- le droit d’audit,
- les questions de responsabilité,
- les pénalités en cas de manquements,
- la fin du contrat (principalement l’exportation et l’effacement de données).

Gestion et surveillance

L’exécution de la prestation devrait faire l’objet d’une surveillance constante et être optimisée le cas échéant. A cet effet, on se référera aux valeurs qui ont été définies. La communauté doit vérifier les valeurs en permanence. Elle doit comparer mensuellement les valeurs réelles communiquées ou établies par le fournisseur avec les valeurs théoriques fixées. En cas d’écarts, des mesures adéquates doivent être prises. Des audits des fournisseurs devraient être effectués régulièrement, en plus du contrôle de la fourniture de la prestation. Il faut s’assurer que les conditions fixées sont respectées et que les prescriptions sont suivies correctement et dans leur intégralité. La régularité et le degré de détail des audits des fournisseurs doivent être définis en fonction des risques. Les fournisseurs stratégiques ou ceux qui ont un accès étendu aux systèmes doivent faire l’objet d’un audit tous les ans.

2.9 Gestion des modifications

4.10

Rubrique CTO applicable

La gestion des modifications pilote les modifications et les extensions de l’infrastructure informatique. Elle s’effectue en collaboration avec toutes les organisations participantes ; de ce fait, elle doit être définie et mise en œuvre transversalement. Les éléments suivants doivent être pris en considération :

- La gestion des modifications devrait s'effectuer en continu et être intégrée aux processus d'exploitation. Toutes les modifications devraient être soumise au processus correspondant et être systématiquement évaluées.
- Toutes les modifications apportées à l'infrastructure TIC devraient être contrôlées et introduites en veillant à minimiser les risques pour l'activité courante des domaines d'activité concernés.
- Les modifications ne doivent pas être source de perturbations ; elles doivent viser une meilleure efficience.
- Les modifications n'offrant pas de bénéfice, les modifications non souhaitées et celles qui doivent être abandonnées du fait qu'elles s'avèrent impossibles à réaliser doivent être évitées.
- Une procédure de secours (fallback procedure) doit être établie.
- La gestion des modifications doit réaliser un équilibre optimal entre la flexibilité et la stabilité des procédures.
- Toutes les modifications ainsi que les différentes étapes de traitement et d'autorisation devraient être rigoureusement historisées.

2.10 Responsable de la protection et de la sécurité des données

4.11.1, 4.11.2

Rubriques CTO applicables

Le responsable de la protection et de la sécurité des données est chargé des tâches suivantes au sein de la communauté :

Profil des tâches

• il élabore, entretient et optimise en permanence le système de gestion de protection et de sécurité des données,

• il surveille les mesures de sécurité quant à la réalisation effective et efficiente des exigences,

• il élabore des principes, des directives et des instructions de sécurité spécifiques à l'organisation,

• il recense, classe et évalue les risques en ce qui concerne les objets de protection (informations, données, applications, systèmes et procédures),

• il évalue et vérifie si des projets sont supportables en termes de protection et de sécurité des données,

• il traite les incidents de sécurité,

• il informe et sensibilise les personnes concernées en matière de sécurité,

• il est l'interlocuteur de référence pour les problèmes en lien avec la sécurité,

• il collabore avec les responsables de la sécurité d'autres communautés, les institutions du domaine de la santé et les tiers concernés (p. ex. fournisseurs).

Indépendance de la fonction

La fonction de responsable de la protection et de la sécurité des données inclut une fonction de contrôle ; l'indépendance de la fonction à l'égard des

personnes et des acteurs impliqués dans la sécurité des objets de protection est indispensable. Par principe, il est donc conseillé de rattacher cette fonction à l'état-major. Les rapports, réguliers et ponctuels, devraient être directement adressés à la direction de l'organisation.

Si la fonction est assurée au sein de l'union du personnel, on s'efforcera d'éviter tout conflit d'intérêt. Elle ne devra pas être combinée avec les postes suivants :

- fonction dirigeante au sein de la communauté ou de la communauté de référence,
- fonction dirigeante au sein de l'infrastructure TIC,
- fonction incluant une responsabilité opérationnelle TIC,
- professionnel de la santé quel qu'il soit.

La fonction peut être assurée par un collaborateur de l'organisation ou un tiers mandaté. Il convient de relever que, dans ce cas, l'organisation n'est pas déchargée de la responsabilité finale.

Connaissances indispensables

Le responsable de la protection et de la sécurité des données doit posséder de solides connaissances professionnelles et des compétences sociales étendues.

Connaissances professionnelles :

- Formation technique, économique ou juridique, avec une formation complémentaire dans les autres domaines
- Solides connaissances de l'environnement médical et expérience en la matière
- Connaissances et expérience dans le domaine de la sécurité des données et de la sécurité TIC
- Connaissances la législation suisse sur la protection des données
- Connaissances de la famille de normes ISO/IEC 2700x
- Expérience dans le domaine de la création et de la maintenance d'un système de gestion (sécurité des informations et protection des données)

Compétences sociales

- Expérience de direction, de préférence
- Sens des responsabilités et fiabilité
- Aptitude à exposer de manière simple, claire et précise des situations complexes, par oral et par écrit
- Aptitude à gérer des conflits et à s'imposer

2.11 Procédure de sauvegarde et de restauration

4.13.1

Rubrique CTO applicables

La sauvegarde des données, également appelée « backup », est élément important de la sécurité des données. Un backup doit pouvoir être lancé à tout moment pour permettre de restaurer rapidement les éléments touchés en cas de perte de données ou d'autres erreurs.

La sauvegarde devrait s'effectuer à la suite de toute modification, mais aussi à intervalles réguliers, indépendamment d'éventuelles modifications. La procédure de backup devrait être définie et décrite dans un concept ad hoc. Son déroulement devrait être automatique autant que possible et faire l'objet d'une surveillance au moyen d'outils adéquats et de procédures d'alarme.

Les backups s'effectuent sous forme cryptée et doivent être conservés séparément du système d'origine. Les sauvegardes ne doivent pas pouvoir être modifiées après coup ou leurs données être écrasées sans que l'on s'en aperçoive. Cette mesure de prudence est particulièrement importante dans le contexte actuel marqué par des attaques de logiciels rançonneurs (ransomware). Les backups sont exclusivement conservés en Suisse, auprès d'un fournisseur soumis à la législation suisse.

La restauration de backups devrait s'effectuer régulièrement à des fins de tests. Tous les trois mois, il y a lieu de restaurer un backup choisi au hasard. Le bon déroulement de la restauration doit être vérifié et historisé.

2.12 Destruction de supports de données

4.13.1

Rubrique CTO applicable

Destruction

Les supports de données qui ne sont plus utilisés doivent être éliminés correctement selon une procédure formelle.

Les supports de données du dossier électronique du patient doivent être détruits conformément à la norme DIN 66399 [DIN 66399]. Les données des patients étant considérées comme des données sensibles, celles du DEP sont attribuées, selon DIN 66399, à la classe de sécurité 3 qui prévoit uniquement les niveaux de sécurité 4 à 7.

- Degré de protection 4 : données sensibles – reproduction extrêmement compliquée
- Degré de protection 5 : données sensibles confidentielles – reproduction au moyen de méthodes incertaines
- Degré de protection 6 : données sensibles secrètes – reproduction techniquement impossible
- Degré de protection 7 : données sensibles ultra secrètes – reproduction impossible

Du fait que les données du dossier électronique du patient relèvent de la classe de sécurité la plus élevée selon DIN 66399, la destruction des supports doit être fiable ou assurer qu'une reproduction des données ne sera possible qu'au prix de difficultés exceptionnelles. Cela vaut pour tous les types de supports de données (mémoire flash et solid-state disks inclus). La destruction des supports de données doit être historisée.

2.13 Planification d'une réinitialisation

4.18

Rubrique CTO applicable

Le plan de réinitialisation permet de planifier la remise en état, dans les meilleurs délais, des principaux éléments de l'infrastructure informatique. Il s'efforce de décrire précisément, d'un point de vue technique, la manière de restaurer un système après un dommage d'une certaine importance. Les mesures de remplacement et la possibilité de recourir à d'autres infrastructures informatiques pour assurer la continuité de l'exploitation font aussi partie du plan.

Le plan de réinitialisation doit tenir compte de deux éléments :

- le temps d'immobilisation maximal (RTO - Recovery Time Objectives),
- la perte maximale de données considérée comme acceptable (RPO - Recovery Point Objectives).

Le temps d'immobilisation de l'infrastructure doit être le plus court possible, les données des patients pouvant avoir une importance vitale dans des situations d'urgence. Quant à la perte de données acceptable, elle ne doit pas excéder la quantité de données générées entre le dernier backup et le moment de l'événement. La perte de données se limite à un minimum puisque des sauvegardes sont effectuées en permanence.

Un plan de réinitialisation devrait prévoir au minimum les éléments suivants :

- la structure, l'installation et la configuration des composants hardware nécessaires
- l'installation du logiciel système
- l'installation des logiciels d'application
- la restauration des données, y compris les fichiers de configuration de la sauvegarde de données
- la réinitialisation du système
- l'espace mémoire nécessaire
- la liste de tous les supports de sauvegarde de données nécessaires
- les contrôles et les mises à disposition

L'ordre de réinitialisation des systèmes et des applications, compte tenu des interactions existantes, constitue un aspect essentiel du plan. Il est conseillé d'élaborer des plans de réinitialisation basés sur des scénarios (p. ex. après une attaque par un logiciel de rançonnage).

Une mesure de prudence optimale serait d'élaborer et d'archiver un guide pratique pour les situations d'urgence dans lequel figureraient :

- les procédures applicables au traitement des situations d'urgence et les responsabilités,
- la liste des personnes responsables et leurs coordonnées,
- les plans de réinitialisation par scénario,
- les mesures de communication.

Le guide pratique devrait être conservé indépendamment de l'environnement DPE, de préférence offline. Sa mise à jour régulière doit être assurée, tout comme celle des droits d'accès de l'ensemble de personnes impliquées.

3 Protection contre les logiciels malveillants

3.1 Introduction

Programmes antivirus

Un logiciel malveillant est un programme conçu pour nuire au bon fonctionnement d'un système informatique. Une fois installé (attaque), il cherche, entre autres, à se propager dans le système et à collecter, endommager ou même détruire des données. Si un système n'est pas protégé en conséquence, il risque d'être attaqué par un logiciel malveillant, aussi appelé ver, virus ou cheval de Troie selon les cas. Ce type d'attaque peut être évité au moyen d'un logiciel antivirus. Un logiciel antivirus a trois fonctions : d'abord, il protège les systèmes des attaques de logiciels malveillants (appelés également malware, parfois maliciels). Les programmes antivirus scannent les pages Internet consultées, les courriers électroniques entrants, les supports de données connectés ainsi que les fichiers pour détecter la présence de virus. S'ils trouvent des fichiers suspects ou rencontrent des procédures douteuses, ils barrent la route aux virus ou, si ceux-ci se sont déjà introduits dans le système, ils restreignent leur accès aux fichiers et, par conséquent, limitent les dommages. Ensuite, les programmes antivirus ont pour mission d'analyser régulièrement les fichiers qui n'auraient pas été détectés au préalable par les programmes antivirus antérieurs. Enfin, ils ont pour fonction d'empêcher la prolifération de logiciels malveillants. Si un malware n'est pas détecté et s'il s'attaque au système, toutes les opérations effectuées à partir de l'ordinateur concerné représentent un risque pour les autres terminaux. Rappelons ici que les programmes antivirus ont une efficacité limitée. D'une part, parce que la détection de virus repose généralement sur des signatures et que, pour être détecté, le logiciel malveillant doit déjà être connu, d'autre part, parce que la majorité des programmes antivirus ne parvient pas à détecter les contenus malveillants des fichiers et des connexions réseau cryptées. Les programmes antivirus font régulièrement l'objet de controverses. L'installation d'un antivirus sur un système informatique implique que ce programme a accès à tous les fichiers et qu'il peut intervenir pour effectuer des modifications sur le système. Par ailleurs, par le biais des signatures, les programmes antivirus peuvent aussi être pilotés à distance, d'où un certain risque. Cela dit, il serait faux de renoncer entièrement et à large échelle aux programmes antivirus. Ces logiciels sont surtout indispensables lorsqu'un très grand nombre d'interactions sont effectuées à partir d'un équipement ou lorsque des utilisateurs travaillent directement sur l'ordinateur. Dans ces cas, une protection efficace contre les virus est conseillée.

Client, serveur, périmètre réseau

Les programmes antivirus peuvent être exploités à plusieurs niveaux. Fondamentalement, la zone opérationnelle peut se limiter aux éléments suivants : terminaux/clients, serveurs et composants réseau. Le concept antivirus d'une d'organisation doit tenir compte de l'ensemble de ces éléments en prenant spécifiquement en considération la situation à risque.

Etant donné que les terminaux/clients et les environnements de serveurs de terminaux interagissent directement avec l'utilisateur et qu'ils sont souvent en contact avec des logiciels potentiellement malveillants, ils devraient

offrir un niveau de protection maximum. Selon l'utilisation prévue, il est possible de réduire le recours aux programmes antivirus sur les serveurs et d'exploiter d'autres outils.

Les connexions réseau (entrées et sorties) devraient être analysées autant que possible quant à la présence d'éventuels contenus malveillants lors de leur entrée dans l'environnement système. En outre, les pages Internet contenant des virus devraient être bloquées temporairement ou être impossibles d'accès.

Les éléments indiqués sous TOZ 4.5a et 4.6.2 doivent être protégés contre les logiciels malveillants, par exemple en installant un programme antivirus ou en recourant à d'autres mesures (p. ex. renforcement de la plateforme, bastionnage du réseau).

Utilisation

4.5, 4.6.2

Rubriques CTO applicables

3.2 Recommandations

Etant donné qu'un programme antivirus ne parvient pas à détecter tous les logiciels malveillants en circulation, nous conseillons d'installer un antivirus spécialisé d'un fabricant sur le client et le serveur et un antivirus d'un autre fabricant sur le périmètre réseau. Cette façon de procéder augmente la probabilité d'identifier un malware.

Différents produits

Les programmes antivirus installés sur les périmètres réseau ont pour mission de barrer la route aux logiciels malveillants et de les empêcher de s'introduire dans le réseau interne. Le périmètre réseau constitue donc le premier niveau de défense ; la protection offerte doit être renforcée par l'installation de programmes antivirus supplémentaires sur les terminaux/clients.

Protection à plusieurs niveaux

La fréquence de mise à jour des programmes antivirus et des signatures malware doit être configurable. Elle doit s'effectuer à un rythme aussi soutenu que possible. Il est conseillé d'actualiser les signatures de programme toutes les heures, mais au minimum une fois par jour. Les programmes antivirus doivent être mis à jour régulièrement.

Mise à jour du software

On Access Scanning désigne l'analyse (scan) en temps réel du système par des programmes antivirus dans l'optique de détecter des malware. Toutes les opérations effectuées en temps réel, par exemple l'accès à un document, sont analysées. Il est recommandé de régler la procédure de manière à vérifier au préalable toutes les interactions (également les lectures). En particulier, il y a lieu de vérifier l'accès en écriture au stockage de documents (Document Repositories).

On Access Scanning

Méthode heuristique

Malgré l'installation de logiciels antivirus, le système n'est pas à l'abri de programmes malveillants. C'est le cas notamment lorsque le logiciel malveillant est encore inconnu du programme de détection lors de l'analyse antivirus. Jusqu'au moment de la mise à disposition des signatures correspondantes, les programmes de détection de virus devraient être équipés de dispositifs permettant de repérer les malware encore inconnus. Cette procédure, appelée « recherche heuristique », devrait être activée dans le dispositif de sécurité du terminal/client puisqu'elle permet précisément de détecter des programmes malveillants encore inconnus. La procédure heuristique peut être à l'origine de fausses alertes. Une procédure d'analyse et de traitement de ces « faux positifs » est recommandée.

Full scan

Puisque des programmes malveillants peuvent malgré tout contaminer les systèmes, il est conseillé de procéder régulièrement à un full scan. Toutes les données existantes doivent être analysées. Etant donné que le programme antivirus est actualisé en permanence et qu'il reçoit régulièrement de nouvelles signatures, une analyse complète du système permet de détecter des logiciels malveillants non identifiés jusque-là. Dans une optique de performance, il est conseillé d'effectuer l'analyse à un moment où les ressources système ne sont pas trop fortement sollicitées. Il serait souhaitable que le software analyse le degré de sollicitation de l'ordinateur et qu'il exécute le scan automatiquement lorsqu'aucun traitement n'est en cours. Le full scan devrait être effectué une fois par semaine et porter sur tous les supports de stockage local de données.

Configurations non modifiables

La configuration, en particulier celle des terminaux/clients, devrait être protégée de manière à ce que les utilisateurs ne puissent pas modifier les paramètres d'un antivirus, ce qui permet d'éviter toute incidence sur la sécurité. Il faut notamment s'assurer que les utilisateurs ne peuvent pas désactiver complètement, ou même pour certains répertoires ou fichiers seulement, les programmes de protection contre les virus informatiques.

Mise en quarantaine d'un logiciel malveillant

Si le programme antivirus détecte un malware potentiel ou si l'on soupçonne que des données ont été corrompues, le fichier concerné doit être mis en quarantaine. Dans la mesure du possible, il s'agira ensuite d'éliminer le virus. Si l'opération est impossible, le fichier doit être supprimé. L'utilisateur doit être informé d'une mise en quarantaine ou de la suppression d'un fichier. En cas de doute quant à l'élimination intégrale du malware, il est conseillé de réinstaller le système d'exploitation.

Mesures supplémentaires de renforcement de la sécurité

Etant donné que les données du DEP sont des données sensibles, il y a lieu, parallèlement à l'installation d'antivirus, de prendre des mesures supplémentaires pour renforcer la sécurité des composants du système. Les mesures suivantes peuvent être appliquées à tous les éléments, serveurs, clients et réseaux :

- **Liste blanche d'applications (whitelisting)** : le terminal ou le serveur peut uniquement exécuter des applications qui ont expressément été approuvées. Les applications non approuvées et, par conséquent, les logiciels potentiellement malveillants, ne sont pas exécutés.
- **Pare-feu client (host based firewall)** : il s'agit d'un dispositif qui confère une sécurité supplémentaire à un équipement. Il permet de restreindre les activités réseau (en entrée et en sortie) uniquement pour l'équipement hôte considéré et, par conséquent, de réduire les dommages dus à une attaque malveillante.
- **Mise à jour du software:** le software devrait être actualisé régulièrement, en principe à intervalles de quelques jours.
- **Désactivation de services** : la désactivation de services et d'applications réduit les possibilités d'accès malveillants. Autrement dit, les services et les applications qui ne sont pas indispensables devraient être désactivés, voire désinstallés.
- **Droits minimums** : l'exécution des services indispensables devrait s'effectuer avec le moins d'autorisations possibles.
- Mesures de protection supplémentaires selon le système d'exploitation considéré, conformément aux recommandations usuelles de bonnes pratiques. Voir à ce propos la liste des instruments envisageables [Hardening-Guides].

4 Détection et gestion des incidents de sécurité

4.1 Introduction

Les capacités de réaction sont cruciales

Des incidents de sécurité peuvent se produire même si des mesures appropriées ont été mises en place au niveau de la technologie et de l'infrastructure utilisées, de l'organisation ou encore du personnel. Disposer d'une procédure rapide et ciblée pour traiter ces incidents et, en amont, pour les détecter revêt donc une importance critique pour réussir à maintenir en permanence un niveau de sécurité adéquat.

Une organisation peut se protéger contre des événements dommageables par des mesures préventives. Celles-ci diminuent la probabilité que des dommages surviennent ou limitent les conséquences des dommages survenus, réduisant ainsi le risque global. Mais la complexité des structures actuelles ne permet souvent pas de réduire totalement le risque. Les responsables de la sécurité doivent ainsi faire l'hypothèse que certains risques peuvent se concrétiser malgré toutes les mesures de prévention. Il faut donc avoir des procédures organisationnelles et techniques, ainsi que des outils

dédiés, pour détecter les incidents de sécurité potentiels, les traiter dans les plus brefs délais et circonscrire le dommage le plus étroitement possible.

Un incident de sécurité peut survenir dans les secteurs suivants d'une communauté :

- sécurité physique ;
- environnement TIC utilisé ;
- utilisateurs et catégories d'ayants droit ;
- applications et systèmes.

En conséquence, il faut définir et mettre en place dans ces trois secteurs des dispositifs et des mesures ayant pour objet de détecter et de traiter les incidents de sécurité.

Les priorités sont définies en se basant sur les risques et en fonction des spécificités de l'organisation. En raison de leur diversité, les communautés recourent à des solutions individuelles pour mettre le dossier électronique du patient à disposition sur leur réseau. L'accès à l'application et au système sur lequel elle tourne est mis en œuvre par un grand nombre d'utilisateurs différents, sur des terminaux différents eux aussi. Il faut donc définir clairement les modalités de gestion des incidents de sécurité et s'attacher à les optimiser en permanence auprès de tous les acteurs.

Vue d'ensemble

Le présent chapitre décrit les différentes étapes de la procédure de détection et de traitement ciblé des incidents de sécurité. Chaque description contient des éléments techniques, des éléments organisationnels et des recommandations concernant les outils à mettre en place. On déterminera des scénarios d'incident réalistes avant d'élaborer les outils correspondants. Il est recommandé de prendre en compte au minimum les scénarios suivants :

- hameçonnage (*phishing*) ;
- failles critiques dans le hardware ou le software ;
- attaques DDoS sur un portail d'accès ;
- logiciels malveillants (p. ex. logiciels de rançonnage ou ransomware) ;
- consultation de données non autorisée ;
- pertes de données ;
- compromission de clés cryptographiques.

La procédure générale de détection et de traitement des incidents de sécurité comporte les cinq phases suivantes :

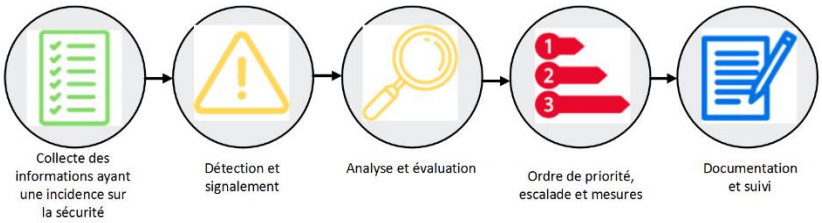

Figure 1 : Procédure de détection et de traitement des incidents de sécurité

Une procédure de référence possible est proposée sous le chiffre **Fehler! Verweisquelle konnte nicht gefunden werden.**.

4.2 Collecte des informations ayant une incidence sur la sécurité

4.3.1, 4.3.2, 4.3.3, 4.6.1, 4.6.2

Rubriques CTO applicables

Le critère de la capacité de détection des incidents de sécurité suppose d'avoir une connaissance approfondie de l'environnement dans lequel on évolue. Il faut avoir repéré et documenté les structures, les failles et les risques ainsi que les catégories d'ayants droit impliqués avant qu'un incident ne survienne. Pour se préparer, on collectera et on actualisera des informations sur les points suivants :

- installations concernées ;
- structure des éléments pertinents, à savoir paysage des systèmes TIC et des applications ainsi qu'environnement réseau (selon CTO 4.6.1. et CTO 4.6.2)
- attribution de la responsabilité des éléments ;
- actifs informationnels et ensembles de données, avec leur criticité et leur répartition dans le paysage des systèmes ainsi que le niveau de classification des informations ;
- utilisateurs et catégories d'ayants droit ;
- failles et risques connus.

Il est indispensable de vérifier au minimum une fois par an ou après toute modification importante si toutes ces données sont complètes et valables.

Sur le plan technique, il faut avoir un lieu de stockage central distinct du système d'origine pour les données historisées pertinentes ainsi que des procédures automatisées pour évaluer en permanence les données et détecter les anomalies. Il est recommandé d'utiliser une solution de gestion des journaux (*log management*) ou de gestion des incidents de sécurité et des événements (*security incident and event management*, SIEM).

4.3 Détection et signalement

4.3.1, 4.3.2, 4.3.3

Rubriques CTO applicables

Il existe une multitude de possibilités techniques pour détecter automatiquement les incidents de sécurité potentiels. Les mesures suivantes doivent être mises en œuvre dans l'environnement du DEP :

Détection par surveillance automatisée

- utilisation de logiciels antivirus et d'un système d'alerte automatique en cas de détection d'un logiciel malveillant (cf. ch. 3).
- surveillance systématique des fichiers d'historisation (*log files*), détection des anomalies et alerte (*log management* et SIEM) ;

- évaluation de la communication réseau au moyen de pare-feu (*firewalls*) et de systèmes de détection et de prévention des intrusions (*intrusion detection and prevention systems*, IDS / IPS) ;
- surveillance de tous les accès en lien avec le DEP et des modifications des données pertinentes, avec alerte active en cas d'anomalie ;
- surveillance des modifications des autorisations, avec alerte active en cas d'anomalie ;
- surveillance du fonctionnement des composants pertinents, avec alerte active en cas de défaillance.

Pour assurer une surveillance ciblée, il faut préalablement définir les événements pertinents devant faire l'objet d'une alerte (*events of interest*, EOI ; exemples tirés des CTO : authentifications dans le système, transactions intercommunautaires via les points d'accès des communautés et recherche de patients). On vérifiera régulièrement si cette liste d'événements est à jour et si elle n'a pas besoin d'être complétée. Il est en outre indispensable d'uniformiser l'ampleur et le degré de détail des historisations dans l'ensemble des éléments afin de pouvoir retrouver partout les informations pertinentes en cas de besoin.

Pour le lancement d'alertes actives et en cas d'événements ayant une incidence sur la sécurité, il est recommandé de prévoir un signalement direct au responsable de la protection et de la sécurité des données. Pour cela, on utilisera dans toute la mesure du possible les processus d'exploitation existants et les moyens d'exploitation correspondants (p. ex. outil de gestion des incidents [*incident management tool*], de création de tickets d'incident [*ticketing system*], etc.).

Détecter les incidents de sécurité potentiels sur la base des données historisées est une tâche complexe. Les personnes qui l'accomplissent doivent non seulement avoir des compétences techniques solides et étendues, mais aussi connaître à fond l'environnement des systèmes. Il faut en outre veiller à compartimenter les tâches : la surveillance de la sécurité informatique et l'organisation d'exploitation proprement dite doivent être confiées à des personnes différentes.

Signalements provenant d'utilisateurs

En principe, tout membre du personnel peut déclencher le signalement d'un incident de sécurité. Les notifications des utilisateurs portent typiquement sur la présence supposée ou réelle d'un virus dans le terminal, la perte de données ou la modification d'informations. Pour leur part, les administrateurs signalent les dérangements qu'ils constatent dans le système. Un centre de contact doit être mis en place pour recevoir le signalement de ces incidents de sécurité potentiels. Il peut s'agir du service d'assistance existant de l'organisation d'exploitation.

Signalements provenant d'autres organisations

Il est important de traiter dans les meilleurs délais les signalements envoyés par d'autres organisations participantes (p. ex. exploitants externes, autres communautés) qui ont remarqué un incident et fournissent des informations à ce sujet. C'est pourquoi il faut mettre en place à cet effet des plates-formes d'échange d'informations et les utiliser. La rapidité des notifications et l'application des enseignements et des mesures qui en découlent permettent aux communautés de gagner un temps précieux.

Outils

Cette étape du processus peut s'appuyer sur les outils suivants :

- instruments techniques de surveillance et de monitoring ;
- procédures de signalement d'événements ayant une incidence sur la sécurité ;
- échanges réguliers avec les organisations participantes au sujet des incidents de sécurité et des enseignements qui en ont été tirés.

4.4 Analyse et évaluation

Rubriques CTO applicables

4.4.1, 4.4.2, 4.5

Critères à remplir

Un incident de sécurité potentiel a été détecté et l'information a été communiquée aux personnes responsables. Il faut d'abord analyser les facteurs en cause afin de pouvoir prendre des mesures ciblées, circonscrire l'incident et communiquer à ce sujet. Les outils nécessaires à cet effet doivent avoir été élaborés préalablement, sous la forme de listes de contrôle ou de cahiers de consignes (*run books*).

Recueil de données sur les facteurs en cause

Pour analyser et évaluer l'incident de sécurité, il faut recueillir des données sur les facteurs suivants :

- Quels sont les éléments touchés par l'incident de sécurité ?
- Qui a constaté et signalé l'incident ?
- Quels sont les cercles d'utilisateurs / les données touchés par l'incident de sécurité (taille, criticité, etc.) ?
- Faut-il engager des actions juridiques ?
- Quels autres éléments peuvent être touchés par l'incident de sécurité ?
- Quels dommages secondaires peuvent être induits par le fonctionnement en réseau des différents systèmes TIC des communautés ?
- Pour quels éléments peut-on exclure des dommages secondaires ?
- Quelle peut être l'ampleur des dommages directs et des dommages secondaires dus à l'incident de sécurité (tenir compte en particulier de la dépendance des éléments de chaque communauté) ?
- Qu'est-ce qui a déclenché l'incident de sécurité (p. ex. inattention, attaque, panne de l'infrastructure de sécurité, etc.) ?
- Quand et où l'incident de sécurité est-il survenu ?
- L'incident de sécurité ne concerne-t-il que des personnes en interne ou aussi des patients ?
- Combien d'informations sur l'incident de sécurité sont déjà arrivées à la connaissance du public ?

Si l'analyse et l'évaluation établissent que l'incident de sécurité peut avoir des conséquences graves, il faut immédiatement enclencher la procédure d'escalade interne à l'organisation.

Lorsque la collecte des données sur les facteurs en cause est terminée, il convient d'examiner les options d'action qui s'offrent. Celles-ci se divisent

en mesures immédiates et mesures complémentaires. Il est impératif de tenir compte dans le processus du délai nécessaire pour appliquer chaque mesure, du coût des mesures ainsi que des ressources dont il faut disposer pour résoudre l'incident et rétablir le bon fonctionnement.

Cette étape du processus peut s'appuyer sur les outils suivants :

Outils

(voir aussi [Incident-Handling]

- réglementation des responsabilités ;
- listes de contrôle ou cahiers de consignes basés sur des scénarios pour analyser et évaluer systématiquement les incidents potentiels ;
- échelles d'évaluation uniformes ;
- définition des voies de communication.

4.5 Ordre de priorité, escalade et mesures

4.3.1, 4.3.2, 4.3.3

Rubriques CTO applicables

Critères à remplir

En règle générale, un incident de sécurité résulte d'un enchaînement de plusieurs causes. Il touche souvent des processus de gestion, des applications et des systèmes différents. Il est donc important que des priorités aient été établies à l'avance afin de pouvoir définir dans quel ordre les difficultés et les problèmes recensés doivent être résolus.

Etablir les priorités avant de résoudre l'incident

Les priorités sont fonction de chaque organisation et de l'incident de sécurité. Pour les établir, il faut donc répondre aux questions suivantes :

- Quels sont les éléments touchés, de quelle protection ont-ils besoin et quelle est leur criticité pour le système dans son ensemble ?
- Y a-t-il des dépendances fonctionnelles ?
- Les conséquences de l'incident peuvent-elles être limitées par des mesures immédiates ?
- Y a-t-il des facteurs internes et externes qui jouent un rôle dans l'établissement des priorités ?
- Faut-il sécuriser des preuves ?

Pour répondre à ces questions, il est intéressant de s'aider de l'analyse des risques relatifs au dossier électronique du patient, qui décrit les dommages potentiels et les catégorise en fonction du degré de protection qu'ils demandent. Il est recommandé d'établir préalablement des priorités sur la base des scénarios.

Définition et mise en œuvre de mesures

Certaines mesures peuvent être mises en œuvre avant l'obtention des résultats détaillés des analyses en cours : ce sont les mesures immédiates, par exemple, l'isolement ou l'interruption de certains services ou systèmes. La prise de ces mesures (déclenchement de procédures souvent prédéfinies) a pour but de circonscrire en grande partie l'incident de sécurité. Elle permet également de poser des bases pour les mesures plus étendues qui découleront des enseignements apportés par les analyses et des décisions prises par les personnes responsables.

On élaborera pour chaque scénario, à partir des informations ayant une incidence pour la sécurité qui ont été collectées, une liste (non exhaustive) de mesures prédéfinies qui apportera un soutien essentiel pour agir vite et de manière adéquate en cas de sinistre

Escalade et dispositif de signalement

Il est important de définir clairement et de documenter la hiérarchie d'escalade en place, y compris les critères d'escalade et les canaux de communication à l'intérieur de l'organisation. Il faut vérifier que cette hiérarchie est toujours d'actualité au moins une fois par an ou à chaque adaptation de l'organisation ; le cas échéant, elle sera adaptée. Ces informations doivent être mises à la disposition de tous les collaborateurs de l'organisation sous une forme simple et facile à trouver.

Selon l'étendue de l'incident de sécurité, il peut être nécessaire d'informer des tiers participants ou d'autres organisations extérieures. Dans cette perspective, il est important que la hiérarchie d'escalade indique clairement les niveaux auxquels un incident de sécurité peut donner lieu à une communication et quelles informations peuvent être partagées avec les organisations participantes.

Il faut mettre en place un dispositif pour signaler les incidents de sécurité à l'organisme de certification et à l'OFSP. A cet effet, on définira des critères spécifiques à l'organisation pour déterminer dans quels cas un signalement est effectué et quelles sont les procédures à appliquer.

En cas d'atteinte aux droits de la personnalité (p. ex. consultation de dossiers sans autorisation), la personne concernée doit en outre être informée de l'incident.

En cas d'incidents de sécurité de grande portée (p. ex. consultation ou perte de données), le public doit être informé de l'incident et des mesures prises. A cet effet, il est utile de préparer des prises de position afin de fournir rapidement une information précise et correcte sur le fond.

Outils

Cette étape du processus peut s'appuyer sur les outils suivants :

- listes de contrôle ou cahiers de consignes basés sur les scénarios (parties traitant de la priorisation des incidents de sécurité) ;
- listes de mesures basées sur les scénarios (mesures immédiates et mesures complémentaires) ;
- hiérarchie d'escalade et procédures de signalement ;
- règles applicables aux échanges d'informations (quelles informations peut-on échanger avec quelles organisations ?) ;
- règles de communication pour l'information du public.

(voir aussi [Incident-Handling]

4.6 Documentation et suivi

4.3.1, 4.3.2, 4.3.3

Rubriques CTO applicables

Une fois l'incident de sécurité maîtrisé, il faut le documenter et en assurer le suivi. La documentation consigne les principales caractéristiques de l'incident (cause, effets, éléments concernés, mesures prises, enseignements, actions de communication). Il faut également déterminer s'il est nécessaire de mettre à jour ou d'étoffer les processus et les outils existants suite à l'événement maîtrisé. De même, l'analyse des risques et les éventuelles consignes et directives doivent être adaptées aux nouveaux enseignements.

Critères à remplir

On s'assurera que le suivi est effectué avec l'attention et le degré de priorité requis en réglant clairement les responsabilités.

Les enseignements que l'on tire de l'incident de sécurité (*lessons learned*) sont les connaissances théoriques ou pratiques nouvelles que l'incident a permis d'acquérir. Ils peuvent découler d'expériences positives comme d'expériences négatives et décrivent un potentiel d'optimisation se rapportant à la situation en question.

Enseignements (*lessons learned*)

Pour obtenir le bénéfice escompté, il faut effectuer les travaux suivants dans le cadre de la procédure générale de gestion des incidents de sécurité :

1. recenser et compiler les données empiriques avec la participation des personnes impliquées ;
2. analyser, évaluer et documenter les données empiriques, en indiquant leur domaine de validité ;
3. mettre les valeurs empiriques documentées à la disposition des catégories d'ayants droit concernées, sous une forme facilitant les recherches.

Evaluation

On commencera par compiler les informations suivantes et effectuer une synthèse des résultats de la compilation, que l'on présentera dans un rapport :

- Que s'est-il passé précisément et quand ?
- Comment l'organisation touchée a-t-elle fait face à l'événement ? A-t-elle utilisé des procédures documentées ? Ces procédures étaient-elles adéquates ?
- De quelles informations aurait-il fallu disposer plus tôt ?
- Des mesures prises ou des actions effectuées ont-elles entravé le rétablissement du bon fonctionnement ?
- Que faudrait-il faire différemment à l'avenir ?
- Comment peut-on améliorer les flux d'information avec d'autres organisations ?
- Quelles mesures peut-on prendre pour empêcher qu'un incident similaire se reproduise ?
- Quelles nouvelles interactions ont été observées ?
- Quels processus ou indicateurs faut-il mieux surveiller pour détecter précocement des incidents similaires (p. ex. actualisation des événements devant faire l'objet d'une alerte [*events of interest*]) ?

- Quelles ressources ou instruments supplémentaires sont requis pour améliorer la détection, l'analyse et la maîtrise des incidents de sécurité ?

Mise à jour des listes de contrôle et des consignes

Les décisions qui sont prises sur la base des enseignements tirés de l'incident et qui entraînent des adaptations dans les processus, les listes de contrôle et les instructions doivent être rajoutés dans la documentation existante. Les documents actualisés doivent être republiés et faire l'objet d'une nouvelle communication.

Communication

La communication suite à une mise à jour doit être proactive. On adaptera la nature et le volume de l'information aux besoins de chaque catégorie d'ayants droit : les informations fournies à d'autres communautés seront bien plus détaillées que le communiqué destiné au public.

Outils

Cette étape du processus peut s'appuyer sur les outils suivants :

(voir aussi [Incident-Handling]

- réglementation des responsabilités ;
- listes de contrôle ou cahiers de consignes basés sur les scénarios (parties traitant de la documentation et du suivi des incidents) ;
- modèles et instructions ;
- règles applicables aux échanges d'informations (quelles informations peut-on échanger avec quelles organisations ?) ;
- règles de communication pour l'information du public.

4.7 Procédure de référence

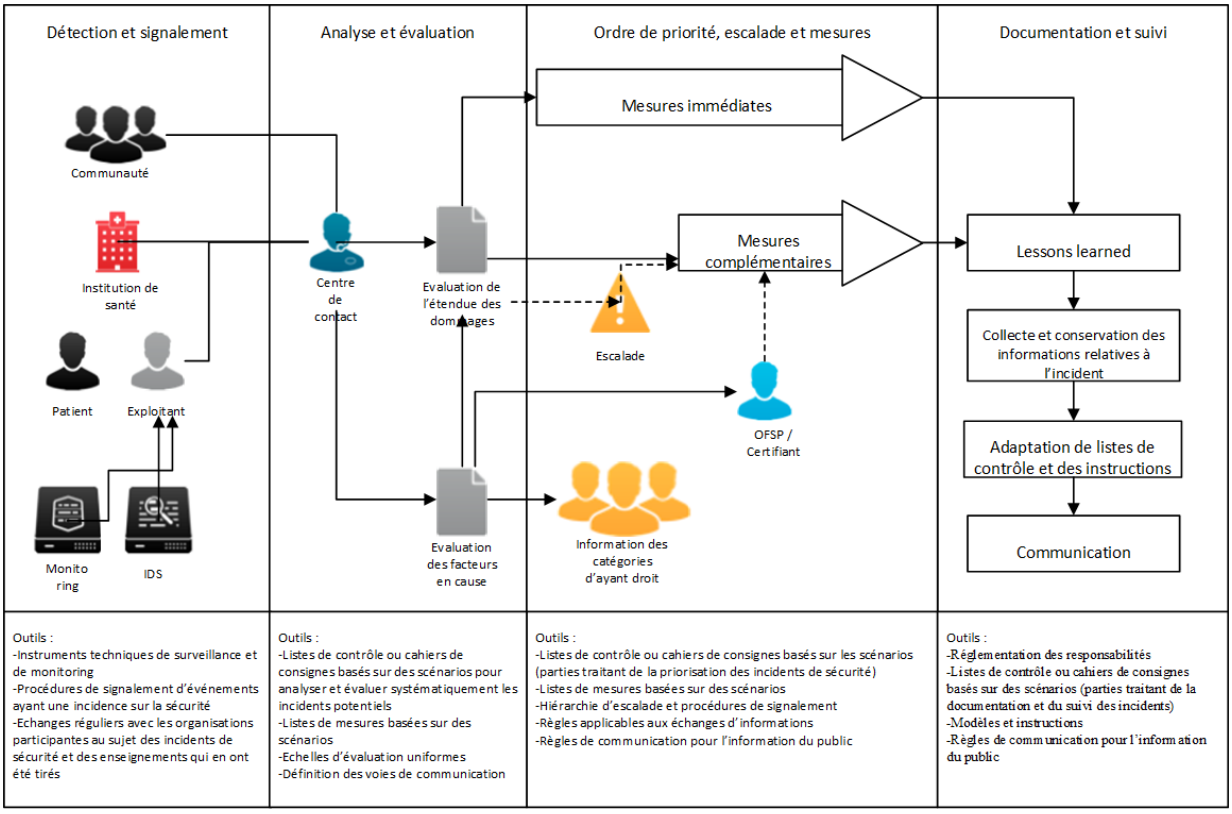

Figure 2 : Procédure de référence

5 Séparation des données

5.1 Introduction

Contexte

En application des prescriptions légales relatives au dossier électronique du patient (art. 10, al. 1, let. b, ODEP) et des critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence (CTO 2.4b), les communautés doivent garantir que, dans les lieux de stockage, les données médicales contenues dans le dossier électronique du patient (DEP) sont enregistrées séparément des autres données de sorte qu'elles ne puissent pas être utilisées abusivement à d'autres fins. Il faut donc mettre en place une séparation qui isole les données relatives au DEP.

Le concept de séparation des données peut être interprété de différentes manières. Dans ce document, nous faisons une distinction entre la tenue séparée de données, à savoir le stockage de données, et le traitement séparé de données, qui autorise uniquement un traitement séparé des données. Les prescriptions de l'ODEP visent uniquement une tenue séparée des données et autorisent explicitement le traitement des données au moyen d'une surface commune. De ce fait, l'utilisation hybride de lieux de stockage sur le même équipement, le même système d'exploitation et la même banque de données est possible.

Ensembles de données

Les données provenant de systèmes d'information des hôpitaux (SIH) et de cabinets médicaux (SICM), par exemple, doivent être séparées des données du DEP. La solution DEP doit être utilisée pour stocker ou traiter uniquement les données pertinentes pour le dossier électronique du patient. Cette gestion séparée des données doit être implémentée à tous les niveaux de la solution. Elle concerne le système primaire aussi bien que les systèmes secondaires, comme l'archivage, les sauvegardes et les plates-formes de stockage ou d'échange de données.

Avantages de la séparation des données

Les ensembles de données doivent être gérés séparément afin que les responsabilités soient partagées clairement entre le DEP et les institutions affiliées aux communautés, selon les modalités suivantes :

- La **souveraineté** sur les données figurant dans les systèmes d'une institution appartient à cette institution. Toutefois, la souveraineté sur les données du DEP appartient au patient. Celui-ci peut en particulier interdire la saisie de documents spécifiques ou demander l'effacement de données déjà saisies.
- La **responsabilité** d'assurer une sécurité et une protection adéquates aux données figurant dans les systèmes d'une institution incombe à cette institution ; elle l'assume conformément à ses directives et à ses normes. Les documents enregistrés dans le DEP, en revanche, sont soumis au système de gestion de la protection et de la sécurité des données de la communauté ; ce système doit satisfaire aux critères de l'ODEP et des CTO.

- La **surveillance** des institutions, y compris leurs systèmes et leurs données, incombe aux cantons ou, s'agissant d'institutions privées, à la Confédération. La surveillance des systèmes et des données du DEP incombe à la Confédération, qui certifie les communautés conformément aux prescriptions de la LDEP, de l'ODEP et des CTO.

Outre qu'elle clarifie les responsabilités, la séparation des données présente les avantages suivants :

- **Protection et sécurité des données du DEP :** l'isolation des ensembles de données permet de (mieux) empêcher que des systèmes d'une institution (SIH ou SICM p. ex.) soient utilisés pour accéder directement aux données du DEP en contournant les contrôles d'accès du DEP.
- **Protection et sécurité des données des systèmes d'une institution :** l'isolation des données permet de (mieux) empêcher que les accès aux registres du DEP depuis Internet ou depuis d'autres institutions ou communautés portent atteinte à la disponibilité et à la sécurité des données des systèmes primaires.
- **Tolérance aux erreurs :** un processus de réplication ordonnée permet de mieux réduire la probabilité que des documents sans rapport avec le traitement soient enregistrés par erreur dans le DEP et deviennent accessibles de l'extérieur.
- **Cycle de vie des données :** la séparation des données facilite l'accomplissement des obligations de conservation et d'effacement, qui sont différentes pour les données du DEP et pour les données des institutions.
- **Travail de certification :** la certification d'une communauté peut être limitée à des secteurs isolés des institutions affiliées, ce qui en accroît l'efficacité.

Possibilités de séparation des données

La tenue séparée des données fait une distinction entre la séparation physique des données, c'est-à-dire l'utilisation de matériel différent pour chaque domaine d'utilisation, et la séparation logique des données, qui isole les données indépendamment du matériel utilisé. Les conditions-cadre en vigueur admettent les deux procédés, le cas échéant une combinaison des deux.

5.2 Explications concernant la séparation des données

Prévention des défaillances d'isolation

La séparation a pour but d'isoler les documents du DEP par rapport aux autres ensembles de données. Un cloisonnement est mis en place pour empêcher, par des moyens techniques, toute « perméabilité » non intentionnelle (« défaillance de l'isolation »). Que la séparation soit réalisée physiquement ou logiquement (p. ex. séparation des banques de données, machines virtuelles, séparation des clients, etc.), il faut que le cloisonnement des lieux de stockage des documents secondaires par rapport aux données primaires des systèmes primaires assure une protection efficace et garantisse, par des moyens techniques, qu'il n'y aura pas de perméabilité non intentionnelle.

Niveaux de séparation des données

La figure ci-contre schématise le déroulement d'un traitement de données. L'utilisateur final (p. ex. le patient ou le professionnel de la santé) édite ou saisit des données dans une application. L'application stocke les données dans la banque de données prévue à cet effet. Ces éléments tournent sur un ou plusieurs systèmes d'exploitation, comme par exemple Windows ou Linux. Le système d'exploitation lui-même peut tourner virtuellement, sur la base d'une plate-forme de virtualisation, ou sur un serveur physique. Toutes les données sont stockées dans un système de stockage. Les données du DEP ou d'autres données peuvent être traitées à chaque niveau. La séparation physique ou logique des données peut s'effectuer à chaque niveau. Une séparation logique requiert des mesures de sécurité visant à éviter une défaillance de l'isolation. Une séparation des données au plus haut niveau possible (utilisateur final, application) peut renforcer la sécurité des données. A partir de la séparation, les données de niveaux inférieurs ne peuvent plus être traitées ensemble.

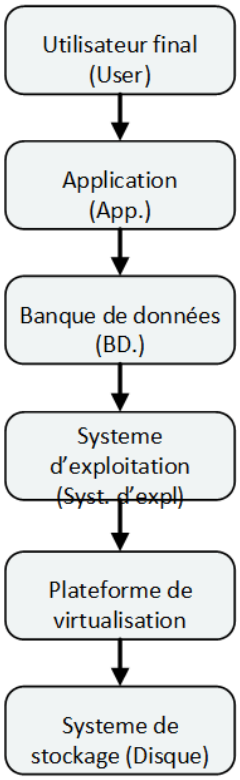

Figure 3 : Niveaux de séparation des données

Séparation physique des données

La séparation physique des données suppose la mise en place d'un environnement dédié au DEP : tous les éléments de cet environnement sont utilisés exclusivement pour traiter les données du DEP. La séparation physique des données est la variante maximale ; elle assure un niveau élevé d'isolation des données du DEP. Une séparation physique complète à tous les niveaux entraîne aussi un traitement séparé des données et une charge administrative plus importante étant donné que les données du DEP, comme les autres données, doivent être gérées et mises à jour.

Séparation logique des données

La séparation logique des données ne requiert pas de séparer physiquement les données : elle peut être obtenue en partitionnant les ressources matérielles existantes. Au lieu de séparer les données physiquement, on les isole virtuellement. Par nature, la séparation logique est plus vulnérable à une défaillance de l'isolation. Les risques afférents doivent être assumés ou compensés par des mesures de sécurité supplémentaires. Il est possible de prendre des mesures techniques et, par exemple, de renforcer la sécurité de la plate-forme (*hardening*) ou d'auditer l'environnement ; on peut aussi prendre des mesures organisationnelles et par exemple compartimenter les tâches (*segregation of duties*).

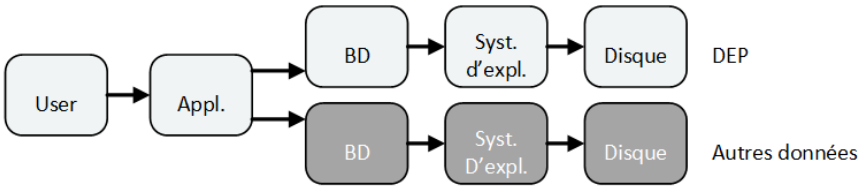

Figure 4 : Séparation logique

Représentation de la séparation logique

Séparation cryptographique

La séparation des données peut être effectuée ou complétée de manière cryptographique. Il est possible d'appliquer des mesures cryptographiques à tous les éléments, mais une séparation efficace requiert des mesures au minimum au niveau de l'application ou, mieux, au niveau de l'utilisateur final. Lorsque les données sont encryptées par l'utilisateur final et qu'elles ne peuvent être décryptées que par lui-même ou par des personnes autorisées par lui, on a un cryptage de bout en bout. Il est recommandé de crypter les données dès le stade du stockage dans l'application afin qu'elles ne puissent être décryptées qu'au moyen de la clé de l'application. Un tel dispositif permet de protéger les données contre les accès au niveau du système d'exploitation, de la banque de données et du stockage.

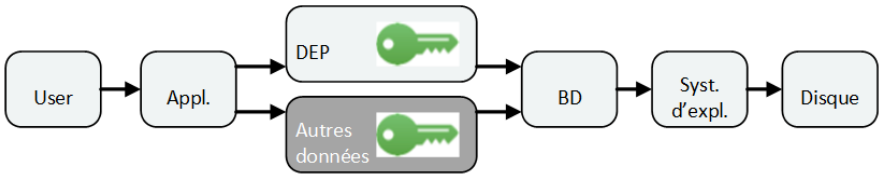

Figure 5 : Séparation cryptographique

Représentation de la séparation cryptographique

Comparaison et évaluation des solutions

Les trois possibilités de tenue séparée des données présentent des niveaux de complexité différents et n'offrent pas la même protection. Si l'on étudie de plus près les principes de la séparation logique et de la séparation physique, force est de constater que la seconde est la variante maximale. La séparation logique réduit les coûts de matériel grâce au partitionnement de l'infrastructure ; il faut toutefois veiller à réduire les risques de défaillance de l'isolation. Les mesures cryptographiques offrent la protection la plus large car elles mettent les données à l'abri à tous les niveaux subséquents. Leur implémentation est coûteuse, mais elle offre une plus grande protection. Combiner une séparation physique ou logique avec des mesures cryptographiques complémentaires accroît la protection des données. Légalement, les trois variantes ou une combinaison de ces variantes sont envisageables. Pour répondre aux exigences de protection des données, la variante cryptographique avec un cryptage au minimum au niveau de l'application s'impose.

5.3 Organisation de la séparation des données du point de vue des communautés

Enregistrement des données

Les données doivent être stockées séparément dès le stade de la saisie (enregistrement), avec une solution au niveau de l'application ou de l'organisation. Des avertissements ou la succession des étapes de travail doivent indiquer clairement à l'utilisateur qu'il traite des données du DEP. Parallèlement aux procédures prévues pour les professionnels de la santé (saisie, téléchargement), un seul rôle peut bénéficier de privilèges système correspondants. Pour réduire le nombre de transmissions non autorisées, les accès correspondants ou clés de l'application doivent être sécurisés de manière appropriée et être protégés par des mesures organisationnelles supplémentaires (p. ex. compartimentage des tâches, principe du double contrôle). Il convient de mettre à disposition des procédures d'importation ou d'autres procédures automatisées dédiées au DEP et d'en assurer la surveillance.

Utilisation de l'application

La tenue séparée de données n'exclut pas que les deux catégories de données puissent être traitées dans la même application. Mais leur traitement doit être séparé dans toute la mesure du possible.

Les étapes de travail impliquant de fusionner les deux catégories de données sont réduites au strict minimum et sont toutes connues sans exception. Elles sont réservées à un cercle d'utilisateurs choisis (professionnels de la santé DEP). Il faut éviter de stocker durablement des ensembles de données fusionnées.

Tenue des données

La tenue des données doit comporter au minimum une séparation logique au niveau du système d'exploitation. Il est donc possible de continuer à utiliser un système de stockage existant ou une plate-forme de virtualisation. En ce qui concerne les données du DEP, les aspects suivants doivent être pris en compte :

- Au niveau du système de stockage, le lieu de stockage est séparé de manière logique. Cette zone séparée est dotée d'un domaine d'autorisations pour les administrateurs système qui lui est propre et qui est conforme aux exigences du DEP.
- Le système d'exploitation est fourni sous la forme d'une machine virtuelle autonome. L'interaction avec d'autres machines ainsi qu'avec la plate-forme de virtualisation sous-jacente est aussi restreinte que possible. Afin de limiter au maximum le risque de défaillance de l'isolation au niveau de la virtualisation, il y a lieu d'exploiter exclusivement des logiciels de virtualisation éprouvés et actualisés. Le disque virtuel est entièrement encrypté. Il est également possible de crypter le lieu de stockage au niveau du système de stockage.

Archivage

L'archivage des données doit comporter au minimum une séparation logique. Il est donc possible de continuer à utiliser un système d'archivage existant. Au niveau du système de stockage, le lieu de stockage est séparé de manière logique. Cette zone séparée doit être dotée d'un domaine d'autorisations pour les administrateurs système qui lui est propre et qui est conforme aux exigences du DEP. Le disque virtuel doit être entièrement encrypté. Il est également possible de crypter le lieu de stockage séparé logiquement au niveau de la zone affectée au DEP.

5.4 Organisation de la séparation des données du point de vue de l'hébergeur externe (*outsourcing provider*)

Principe

L'hébergeur externe qui traite des données du DEP provenant de différentes communautés ou institutions doit en principe les traiter et les stocker séparément. La séparation est établie à la fois entre les données des différentes communautés et entre celles des communautés et des autres clients de l'hébergeur externe. La meilleure manière d'implémenter cette séparation obligatoire est de recourir à une mesure logique.

Fonctionnalité multi-clients de l'application

L'application doit permettre de gérer plusieurs clients séparément les uns des autres. La fonctionnalité multi-clients a les caractéristiques suivantes :

- Les lieux de stockage sont séparés, excluant la possibilité d'échanges de données entre les clients ou de défaillance de l'isolation.
- Chaque client a un domaine d'autorisations dédié.
- Les transactions sont effectuées en circuit fermé à l'intérieur de la partition de chaque client.
- L'application a une configuration spécifique pour chaque client
- L'historisation et le stockage des données historisées sont propres à chaque client.
- Chaque client a une solution spécifique pour l'effacement des données (ainsi que pour les sauvegardes et les données historisées).

Séparation cryptographique

La fonctionnalité multi-clients doit être doublée d'une séparation cryptographique entre les différents ensembles de données. Elle est assurée par l'utilisation de cryptages dédiés au niveau de l'application : toutes les données d'un client sont chiffrées et stockées avec une clé de cryptage spécifique. En cas de défaillance de l'isolation au niveau de l'application, les données ont ainsi une protection supplémentaire. Elles sont en outre protégées contre la consultation par des personnes non autorisées au niveau de l'infrastructure par les administrateurs système.

Séparation physique

Il est également possible que les données du DEP bénéficient chez l'hébergeur d'une séparation physique totale, ce qui satisferait au critère de la fonctionnalité multi-clients. Dans ce cas, les données doivent en outre être cryptées au minimum au niveau du support de données. Le cryptage des données au niveau de l'application est recommandé.

6 Emploi de la cryptographie

6.1 Introduction

2.5, 4.12	Rubriques CTO applicables
La cryptographie est un aspect important de la sécurité de l'information. Il s'agit essentiellement de chiffrer les données, les messages et les communications afin que les informations ne puissent pas être lues ni manipulées. Voici comment on peut décrire les buts généraux de la cryptographie.	Introduction
Grâce au chiffrement ou cryptage, le contenu d'un fichier ou d'un message reste inaccessible à la personne non autorisée qui détiendrait ce fichier ou ce message sans en avoir la clé.	Confidentialité
L'application de mesures cryptographiques rend impossibles ou fait ressortir les modifications non autorisées de données. L'intégrité des données peut être garantie par le fait que les modifications non autorisées sont visibles.	Intégrité
La signature électronique personnelle qualifiée établit sans ambiguïté l'identité de la personne qui envoie un message ou qui crée un fichier.	Authenticité
Les systèmes cryptographiques recommandés dans le présent document peuvent être considérés comme sûrs actuellement et dans un avenir proche compte tenu de l'état de la technique. Mais comme celle-ci évolue très vite (p. ex. calculateurs quantiques), il se peut que de nouvelles évolutions rendent obsolètes ces recommandations. Le présent document prévoit une marge de sécurité pour le choix des procédés de chiffrement et de leurs paramètres système (p. ex. longueur des clés) : une durée d'utilisation d'environ dix ans devrait être assurée, sous réserve d'évolutions nouvelles impossibles à anticiper.	Validité et durée d'utilisation

6.2 Principes de la cryptographie

Il faut s'abstenir de développer ou d'adapter soi-même des algorithmes ou des procédés cryptographiques. En effet, il est indispensable que les algorithmes utilisés et leur implémentation aient été contrôlés par un ensemble d'experts aussi étendu que possible afin de minimiser le risque de failles.	Pas de développement en interne
Selon le principe de Kerckhoffs, la sécurité d'un système cryptographique repose sur le secret de sa clé, et non pas sur le secret de son algorithme. Un algorithme connu publiquement présente l'avantage de pouvoir être soumis de toutes parts à des tests indépendants visant à rechercher des failles éventuelles. En outre, un grand nombre d'experts peuvent contribuer à le développer et à le faire évoluer. Dans le contexte du DEP, il convient par conséquent de privilégier les systèmes de chiffrement publics.	Utilisation de systèmes de chiffrement publics
Il existe sur le marché un grand nombre de procédés cryptographiques qui ne sont pas en contradiction avec les deux principes énoncés ci-dessus et qui peuvent donc être employés. En cas d'emploi de procédés cryptographiques dérogeant aux présentes recommandations, il convient de respecter les normes FIPS [FIPS140.0].	Procédés autorisés

6.3 Cryptage des systèmes de stockage

2.5

Rubrique CTO applicable

Description

Les données du DEP doivent toujours être conservées sous forme cryptée.

6.4 Cryptage des transmissions

2.5, 4.15.3, 4.15.4

Rubriques CTO applicables

Description

Les données du DEP doivent être protégées par cryptage non seulement dans le contexte du dossier électronique, mais aussi pendant leur transmission. Une méthode typique d'attaque des transmissions de données consiste à s'interposer entre deux interlocuteurs et à prendre le contrôle de la transmission des données (« *man in the middle* »). Si l'auteur de l'attaque ne détourne que des données cryptées, il ne peut rien en faire sans connaître la clé correspondante.

Pour chiffrer les transmissions de données, on utilise le protocole de sécurisation de la couche de transport TLS (*Transport Layer Security*). Voir les recommandations au ch. 6.11.

6.5 Systèmes cryptographiques

Définition

On entend par « systèmes cryptographiques » des algorithmes, des mécanismes et des procédés servant à chiffrer des informations. On distingue les systèmes symétriques et les systèmes asymétriques ainsi que les systèmes hybrides, qui combinent les deux premiers types. Dans le contexte du dossier électronique du patient (DEP), on utilise les deux types de systèmes. En voici donc une brève présentation.

Cryptographie symétrique

Le système symétrique utilise une même clé pour chiffrer et déchiffrer les informations. Il est peu gourmand en ressources et relativement simple à implémenter.

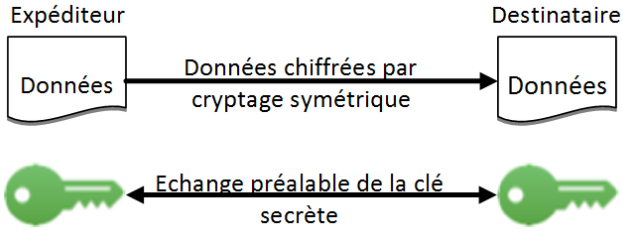

Figure 6 : Cryptage symétrique

Principe de fonctionnement

La cryptographie symétrique utilise une clé unique (clé secrète ou privée), que l'expéditeur et le destinataire doivent avoir en leur possession. Ces procédés de chiffrement s'exécutent donc rapidement et offrent un niveau de sécurité approprié si la clé est suffisamment longue. La difficulté réside dans la distribution préalable de la clé aux deux communautés qui échangent des données. Si un attaquant intercepte la communication lors de la transmission de la clé, les informations cryptées ne sont plus protégées puisque l'attaquant peut lui aussi les décrypter. Un attaquant peut aussi s'emparer d'une clé si l'une des deux communautés ne l'a pas stockée avec un niveau de protection suffisant.

Echange de clés

Il est donc important d'utiliser une connexion sécurisée pour échanger des clés cryptographiques ou de procéder sous forme cryptée (p. ex. utilisation de procédures asymétriques).

Voir ch. **Fehler! Verweisquelle konnte nicht gefunden werden.**

Advanced Encryption Standard (AES)

Si l'on choisit la cryptographie symétrique, il est recommandé de recourir à AES. Ce procédé est compatible avec différents modes d'opération et paramètres système.

Modes d'opération

Recommandations concernant le choix du mode d'opération :

- Pour effectuer un chiffrement par bloc, il est recommandé d'utiliser le mode *Cipher Block Chaining* (CBC).
- Si le cryptage doit être accompagné d'une authentification des données, on utilisera le mode *Galois Counter Mode* (GCM).
- Pour effectuer un chiffrement par flot, il est recommandé d'utiliser le mode *Counter Mode* (CTR).
- Si un vecteur d'initialisation (*initialization vector*, IV) est requis, il doit être généré à chaque nouveau chiffrement. Il est essentiel que le

vecteur d'initialisation ne se répète pas à l'intérieur d'une période de changement de clés et qu'il ne soit pas prévisible.

Le procédé AES peut être utilisé avec des longueurs de clé variables. Il est recommandé d'employer au minimum AES-256, avec une longueur de clé de 256 bits.

Longueur minimale des clés

Si l'on choisit un système AES-256, il est recommandé d'utiliser le mode d'opération *Cipher Block Chaining* (CBC) ; avec un protocole TLS, on utilisera la procédure *Galois Counter Mode* (GCM).

Recommandation concernant la cryptographie symétrique

La cryptographie asymétrique utilise deux clé différentes dépendantes l'une de l'autre. Cette paire est composée d'une clé publique et d'une clé privée. C'est pourquoi les procédés asymétriques sont aussi appelés procédés de chiffrement à clé publique.

Cryptographie asymétrique

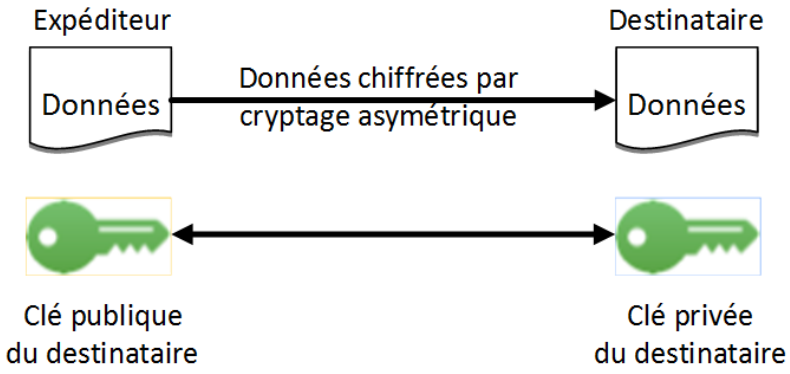

Figure 7 : Cryptage asymétrique

Les informations cryptées à l'aide d'une clé publique ne peuvent être décryptées qu'avec la clé privée correspondante. Le possesseur de la paire de clés doit donc garder la clé privée secrète. L'expéditeur qui veut envoyer un message chiffré au destinataire a besoin de la clé publique de ce dernier. La clé publique utilisée pour crypter le message ne peut plus être utilisée pour le décrypter (fonction unidirectionnelle) ; pour déchiffrer le message, il faut la clé privée du destinataire. Il est important dans ce procédé que la clé privée soit tenue secrète. Si un attaquant parvient à s'emparer de la clé privée, il peut alors accéder aux produits cryptés et les décrypter.

Principe de fonctionnement

Dans la cryptographie asymétrique, la distribution des clés est plus facile que dans la cryptographie symétrique. Mais les procédés asymétriques requièrent une plus grande puissance de calcul que les procédés symétriques. C'est pourquoi la cryptographie asymétrique est souvent utilisée pour transmettre les clés de cryptographie symétrique.

Distribution des clés

Voir ch. **Fehler! Verweisquelle konnte nicht gefunden werden.**

Si l'on choisit la cryptographie asymétrique, il est recommandé d'utiliser le procédé RSA avec une longueur de clé de 4096 bits ou plus.

Recommandation concernant la cryptographie asymétrique

6.6 Hachage

Rubriques CTO applicables

2.10, 4.3.1, 4.13.1, 10.2.3

Introduction

Le hachage (*hashing*) constitue un domaine à part entière de la cryptographie. C'est un outil important pour protéger des informations. La longueur de la valeur de hachage est exprimée en bits. Les données à hacher (message) peuvent être constituées d'un seul caractère, d'une phrase ou d'un fichier complexe. La chaîne de caractères générée par le hachage est appelée, selon le contexte, empreinte numérique, somme de contrôle cryptographique, condensat (*message digest, MD*) ou code d'authentification de message (*message authentification code*, MAC). On emploie aussi le terme générique de valeur de hachage (*hash*). Le hachage n'a pas pour but premier d'opérer un chiffrement. Il en découle que les fonctions de hachage n'ont pas toutes des propriétés cryptographiques.

Critères à remplir par une fonction de hachage

Une fonction de hachage est considérée comme cryptographique lorsqu'elle remplit les critères suivants :

1. Univocité
   Une même séquence de caractères aboutit à la même valeur de hachage.
2. Irréversibilité
   Il est impossible de retrouver le message (chaîne de caractères hachée) par rétrocalcul à partir de la valeur de hachage.
3. Résistance aux collisions
   Deux chaînes de caractères différentes ne peuvent pas délibérément donner la même valeur de hachage.

Recommandation concernant le hachage

Si l'on choisit le hachage, il est recommandé d'utiliser les algorithmes ARAGON2 ou PBKDF2 avec Salz pour mémoriser les mots de passe. Lorsqu'une vitesse de traitement élevée est requise, p. ex. pour TLS, on utilisera les fonctions SHA-512 ou SHA3-512.

6.7 Remplacement de procédés cryptographiques ayant des failles connues

Remplacement de procédés cryptographiques

Si des failles sont détectées dans un procédé cryptographique utilisé et que ces failles ne permettent plus de remplir intégralement les objectifs définis dans le concept de sécurité (cf. ch. 6.1), il faut s'efforcer de remplacer rapidement le procédé en question.

Transparence sur les composants utilisés

Il est recommandé de surveiller en permanence les composants logiciels et les procédés de chiffrement pour détecter d'éventuelles failles. Pour ce faire, les informations indispensables (p. ex. versions software exploitées) doivent être connues et figurer dans l'inventaire (voir ch. 2.6). Les outils ci-dessous peuvent être exploités dans un environnement de développement :

- OWASP Dependency Check
- Versions-Plugin pour Maven

Enfin, il faut examiner régulièrement les signalements des CERT ainsi que les bases de données de vulnérabilité connues. Une liste des sources d'informations figure dans les signalements CERT.

6.8 Gestion des clés

Génération de clés

Pour générer des clés de chiffrement, on veillera à utiliser des modules cryptographiques si possible compatibles avec la norme FIPS 140.0-2 [FIPS140.0] et configurés en conséquence. Toutes les clés cryptographiques doivent être générées dans ces modules. De manière générale, il est bon de préférer les modules matériels aux modules logiciels.

Echange de clés

Il faut veiller que l'échange de clés se fasse via une liaison sécurisée ou sous forme cryptée (p. ex. en exploitant des procédures asymétriques).

Stockage des clés

Pour le stockage des clés, il faut veiller aux points suivants :

1. Les emplacements du matériel de clé cryptographique (dans l'application et sur les supports de données) doivent être connus du cercle de personnes nécessaires.
2. Les clés sont protégées par des modules cryptographiques, que ce soit sur le support de données utilisé pour leur conservation ou sur les systèmes intermédiaires où elles transitent.
3. Le matériel de clé n'est pas conservé sans être crypté.
4. Dans la mesure du possible, toutes les clés sont conservées dans un coffre-fort cryptographique, comme un module matériel de sécurité (*hardware security module*, HSM) ou un service de cryptographie isolé.
5. S'il est prévu de stocker des clés dans une base de données, il faut s'assurer que ces clés sont chiffrées au moyen de clés de chiffrement de clés (*key encryption keys*, KEK) avant leur transfert sur le support de données. Les KEK doivent avoir une force de chiffrement au moins égale aux clés qu'elles protègent.
6. Il faut s'assurer que l'intégrité des clés stockées dans une base de données est protégée. On peut utiliser à cet effet un algorithme à double fonction, qui supporte à la fois le cryptage et le code d'authentification de message (MAC).
7. Il faut s'assurer que le code standard des applications utilise non pas des clés cryptographiques, mais des bibliothèques de gestion de clés (*key management libraries*).
8. Il faut s'assurer que les opérations sur les clés et les opérations cryptographiques sont toujours exécutées à l'intérieur d'un coffre-fort protégé. Cela concerne l'accès aux clés, le chiffrement et le déchiffrement ainsi que l'apposition des signatures.

Sauvegarde des clés

Les fichiers chiffrés dont on a perdu la clé ne pourront plus être restaurés. Il est donc crucial d'avoir une gestion adéquate de la sauvegarde des clés. Il faut pouvoir, dans certaines conditions, restaurer des données du DEP.

Lorsqu'un fichier de sauvegarde de clés est créé, il faut le doter d'un module cryptographique au moins conforme à la norme FIPS 140.0-2 [FIPS.140.0].

6.9 Responsabilité des clés et audit

Identification

Réglementer les responsabilités implique d'identifier tous les utilisateurs et les administrateurs système qui, dans le cadre du développement système et de l'exploitation du DEP, ont accès aux clés cryptographiques ou les contrôlent durant leur cycle de vie. Une définition claire des responsabilités permet de prévenir une mauvaise utilisation générale des clés et de limiter l'ampleur des dommages en cas d'utilisation abusive.

Avantages d'une réglementation des responsabilités

Dans le contexte du DEP, réglementer les responsabilités en ce qui concerne les accès à l'ensemble du matériel de clé apporte aux communautés les avantages suivants:

1. Si une utilisation abusive est détectée, la réglementation de la responsabilité de la clé en cause permet de déterminer rapidement quelles personnes sont impliquées dans l'incident de sécurité et comment celui-ci est survenu.
2. Une définition claire des responsabilités assure une protection supplémentaire aux clés car leurs utilisateurs sont informés qu'ils devront rendre des comptes en cas d'incident, ce qui les incite à la prudence.
3. Savoir quelles données étaient protégées par une clé utilisée abusivement facilite le processus de restauration des données lors du traitement de l'incident de sécurité, qui peut être à l'origine d'une perte d'intégrité.

Principes

Pour que la réglementation des responsabilités apporte effectivement les avantages évoqués, il faut respecter les principes suivants :

1. Toutes les clés sont identifiables de manière univoque.
2. L'utilisateur d'une clé est identifiable de manière univoque.
3. Toute utilisation d'une clé est enregistrée (date, heure, utilisateur, données auxquelles il a été accédé).

Critères d'audit

L'audit doit être pratiqué en utilisant deux méthodes différentes et complémentaires. D'une part, il faut auditer régulièrement les procédures utilisées et la gestion des clés en général [NIST-SP-800-57] ; d'autre part, il faut auditer régulièrement les mécanismes de protection concrets et se demander s'ils sont adaptés aux données qu'ils protègent. Il s'agit ici d'une recommandation d'audit supplémentaire, indépendante de l'audit de certification et d'éventuels audits de fournisseurs.

Adaptations permanentes

Lors des travaux d'audit, il faut toujours penser aux nouvelles formes que prennent les technologies et les attaques afin de pouvoir réagir précocement aux menaces possibles. Il est important en outre de tenir compte du fait que la sécurité de la technologie utilisée dépend fortement du facteur humain. Les personnes impliquées doivent donc être formées et sensibilisées régulièrement (cf. ch. **Fehler! Verweisquelle konnte nicht gefunden werden.**).

6.10 Compromission de clés et restauration de fichiers compromis

Une clé compromise doit être bloquée dans les plus brefs délais. Cela signifie que les données auxquelles elle donne accès doivent être dotées d'une nouvelle clé pour éviter tout accès non autorisé. Il faut également faire l'hypothèse que les contenus des fichiers auxquels la clé compromise donnait accès peuvent avoir été modifiés.

Procédures préventives

Les communautés doivent mettre en place les procédures suivantes dans le DEP pour réduire les possibilités de compromission des clés et permettre de circonscrire un possible dommage :

1. Il faut limiter le temps pendant lequel une clé de cryptographie symétrique est disponible en clair, que cette clé se trouve dans une banque de données ou dans un système intermédiaire.
2. Dans toute la mesure du possible, les utilisateurs et les administrateurs système ne doivent pas pouvoir consulter les clés sous une forme non chiffrée.
3. Il faut mettre en place et appliquer une réglementation des responsabilités et enregistrer systématiquement les utilisations des clés et les accès aux clés.
4. Les clés doivent faire l'objet d'un contrôle d'intégrité (MAC ou signatures numériques).
5. Il faut utiliser un système d'horodatage fiable (*time stamps*). L'heure officielle METAS doit être utilisée (voir CTO 2.9.30)
6. Une procédure-type doit être mise au point pour la restauration des fichiers compromis dans le système de la communauté qui gère le DEP.

Cahier de consignes

Ce dernier point – l'utilisation d'un cahier de consignes (run book) au sein de la communauté qui gère le DEP – est essentiel pour pouvoir réagir vite et bien en cas d'incident de sécurité. Pour pouvoir élaborer un tel instrument, il faut disposer des éléments suivants :

1. identification et données de contact du personnel à informer en cas d'incident ;
2. identification et données de contact du personnel requis pour restaurer les fichiers ;
3. définition de la méthode utilisée pour attribuer de nouvelles clés ;
4. tenue d'un inventaire de toutes les clés et de leur but (p. ex. emplacement de tous les systèmes de certificats) ;
5. formation du personnel sur les processus de compromission et les procédures de restauration ;
6. implémentation de directives (*policy*) sur l'application des différentes procédures de révocation de clés ;
7. surveillance de toutes les opérations d'attribution de nouvelles clés *re-keying*) pour s'assurer que toutes les clés concernées ont été révoquées et que les fichiers correspondants ont été restaurés ;
8. listage de toutes les autres procédures dépendant de la communauté dans le cadre de la révocation et de la restauration :

a. inspection physique des appareils et du matériel informatique ;
b. identification de toutes les informations pouvant avoir été compromises ;
c. identification de toutes les signatures pouvant avoir été compromises ;
d. distribution des nouvelles clés.

(Voir également ch. 4)

6.11 Utilisation du protocole *Transport Layer Security* (TLS)

4.15.3, 4.15.4

Rubriques CTO applicables

Application

Les CTO prescrivent l'utilisation du protocole TLS pour sécuriser la transmission de données par HTTPS. TLS permet de protéger des données contre la lecture et les modifications non autorisées durant leur échange entre deux systèmes.

Recommandations générales

Recommandations générales :

- TLS est toujours utilisé dans sa version la plus récente.
- La procédure d'échange de clés emploie le procédé Diffie-Hellmann de négociation de clés éphémères (*Diffie-Hellman Ephemeral*, DHE).
- Utilisation de Perfect Forward Secrecy (PFS)
- L'utilisation de CBC est à éviter.
- Toutes les pages et leurs ressources sont proposées par HTTPS.
- On utilise systématiquement le champ d'en-tête *Strict Transport Security* de HTTP (*Strict Transport Security Header*, HSTS).
- Les cookies sont dotés de l'attribut *secure* (*secure flag*).
- La mise en cache de données est désactivée.
- La configuration de TLS est conforme aux recommandations en vigueur d'OWASP [OWASP-TLS-CS].

Certificats de serveur

Recommandations concernant l'utilisation de certificats de serveur :

- Il faut utiliser au minimum des certificats officiels à validation étendue (*Extended Validation)*.
- Les certificats utilisés supportent tous les noms de domaine nécessaires (p. ex. https://www.example.ch et https//example.ch).
- Les certificats contiennent uniquement des noms de domaine complètement qualifiés (*fully qualified domain names*, FQDN).
- Les certificats ne contiennent aucun joker (métacaractère ou *wild card*).
- Les certificats ne contiennent pas d'adresses IP privées (RFC 1918 zone d'adresses).
- On fait appel uniquement à des autorités de certification (*certification authorities*, CAs) connues et dignes de confiance.

Une fois le système installé et configuré, il est recommandé de tester la configuration du TLS conformément au guide de tests (*Testing Guide*) de l'OWASP [OWASP-TLS-TG].

7 Protection contre la manipulation des niveaux de confidentialité

7.1 Introduction

Niveaux de confidentialité

Toute personne est libre d'adhérer au système du dossier électronique du patient (DEP). Si elle opte pour le DEP, elle dispose pleinement de ses données de patient, mais en assume aussi la responsabilité. Les données médicales peuvent être attribuées à l'un des trois niveaux de confidentialité suivants :

- normal,
- restreint,
- secret.

Si le patient ne prévoit aucun niveau de confidentialité, le niveau « normal » est automatiquement attribué aux nouvelles données. Il est toutefois possible que des professionnels de la santé considèrent que des données non expressément attribuées à un niveau de confidentialité par le patient sont des données sensibles et qu'ils les classent dans la catégorie des données à accès restreint.

Droits d'accès

Le patient peut accorder les droits d'accès à un professionnel de la santé ou à un groupe de professionnels de la santé. Ces droits sont valables tant que le patient ne les révoque pas. Si la loi ne prévoit pas de durée limite, il est toutefois possible de prévoir une telle limite. La durée des droits d'accès attribués à des groupes est pour sa part limitée. De cette manière, on peut s'assurer que les professionnels de la santé qui n'interviendront vraisemblablement qu'une fois dans un traitement, ou alors seulement pour une brève période, n'auront pas accès pour un temps illimité au dossier électronique du patient. Cette disposition réduit également le risque d'oublier que des droits d'accès ont été attribués.

Autorisation accordée à un groupe

Lorsque des droits d'accès sont accordés à un groupe, tous les professionnels de la santé qui le rejoignent obtiennent automatiquement les droits d'accès accordés au groupe. Lorsqu'un professionnel de la santé quitte un groupe, il perd automatiquement aussi les droits d'accès associés au groupe. Le patient peut demander à être informé de l'entrée d'un professionnel de la santé dans un groupe auquel il a accordé un droit d'accès.

Urgence médicale

En cas d'urgence médicale, les professionnels de la santé sont habilités à accéder aux données du niveau de confidentialité « normal ». Afin d'empêcher un abus d'accès pour motif d'urgence médicale, par exemple accès automatique à un terminal, il est recommandé d'exiger du professionnel de la santé qu'il confirme l'accès en urgence au moyen d'une interaction non automatique, reproductible et manuelle (ch. 2.2. let. a, annexe 2 ODEP-DFI). On pourrait imaginer un élément de sécurité supplémentaire, comme l'obtention d'un mot de passe à usage unique, ou la répétition de la saisie d'un autre critère de sécurité. Le patient doit être informé dans un délai raisonnable de tout accès aux données de son dossier lié à une urgence médicale. L'obligation d'informer incombe à la communauté ; l'information s'effectue par SMS, courrier postal ou courrier électronique. L'obligation d'informer peut être déléguée aux institutions de santé concernées.

Professionnel de la santé autorisé / Représentant

Le patient peut autoriser un professionnel de la santé de sa communauté de référence à transmette son droit d'accès à d'autres professionnels de la santé. Le professionnel concerné peut uniquement transmettre des droits d'accès équivalents à ceux dont il dispose. Le patient a également la faculté de désigner un ou plusieurs représentants. Le représentant peut accéder au dossier électronique du patient et attribuer des niveaux de confidentialité ainsi que des droits d'accès. Il doit posséder un moyen d'identification propre pour accéder au dossier électronique de la personne qu'il représente. Une représentation par des proches ou des personnes de confiance est conseillée pour les enfants et les personnes âgées.

Liste d'exclusion

Les patients peuvent non seulement retirer à des professionnels de la santé les droits d'accès à des niveaux de confidentialité, mais aussi refuser à certains d'entre eux tout accès à leur dossier. Les personnes concernées sont alors placées sur une liste d'exclusion. Cette liste prime les autres dispositions, même en cas d'urgence médicale.

Sensibilisation des patients

Lors de l'enregistrement du dossier électronique, il y a lieu d'attirer l'attention des patients sur le fait qu'ils portent l'entière responsabilité de leur dossier. Ils doivent avoir clairement conscience que le patient a la pleine maîtrise de ses données, notamment en ce qui concerne la question de l'accès aux données. Le patient doit également savoir qu'en l'absence de configuration manuelle du dossier électronique, les données sont automatiquement attribuées au niveau de confidentialité « normal » et que, en conséquence, un cercle potentiellement étendu d'utilisateurs peut y accéder.

7.2 Mesures de sécurité

Surveillance des comptes utilisateurs

Il est recommandé d'implémenter une procédure destinée à vérifier les comptes utilisateurs. Dans ce cas, le système contrôle quand, où, à quelle fréquence et à partir de quel terminal un patient ou un professionnel de la santé accède à un dossier électronique. En cas d'anomalies, comme une annonce depuis l'étranger ou des accès multiples, la personne est avisée par courrier électronique (ou par tout autre moyen).

Enregistrement et évaluation des mutations

Il convient également d'exploiter un système capable d'enregistrer et d'analyser toutes les modifications apportées au DEP. Si l'analyse révèle des anomalies, comme un nombre statistiquement significatif de données de patients dont le niveau de confidentialité a été revu à la baisse en l'espace de peu de temps, le responsable de la protection et de la sécurité des données de l'institution de santé ou de la communauté ou communauté de référence doit en être informé. Il incombe à l'institution concernée de s'interroger sur les raisons de cette anomalie.

Authentification supplémentaire en cas d'actions critiques

Afin que la rétrogradation des niveaux de confidentialité soit plus compliquée et les risques moins grands, il est recommandé de demander aux patients de procéder à une authentification supplémentaire lorsqu'ils modifient le niveau de confidentialité de leurs données. En d'autres termes, sitôt qu'une personne rétrograde ses données de patient du niveau de confidentialité « secret » à celui de « normal », elle reçoit un courriel (ou un autre message) l'invitant à confirmer la modification apportée au dossier électronique. En cas de perte passagère du compte utilisateur, il devient impossible de modifier les niveaux de confidentialité, les paramètres ayant trait à la sécurité

et les données. Les documents restent alors inaccessibles tant que la confirmation n'a pas été effectuée,

Contrôle régulier par le patient

Les patients reçoivent régulièrement, mais au minimum une fois par an, un courrier électronique (ou un autre message) leur rappelant que les niveaux de confidentialité de leur dossier électronique doivent être vérifiés. Ce rappel a pour objectif de les inciter à vérifier eux-mêmes les droits d'accès à leurs données quant à des anomalies potentielles et à avoir une vue d'ensemble des éventuels changements dans les groupes d'ayants droit, par exemple l'entrée ou la sortie d'un professionnel de la santé d'une communauté.

Informations supplémentaires en cas de modifications ayant une incidence sur la sécurité de la part du patient

La responsabilité du patient à l'égard de son dossier électronique entraîne également des risques. Les personnes insuffisamment informées peuvent être amenées à attribuer un niveau de confidentialité erroné à leurs données de patient. Une sécurité minimale doit donc être prévue à cet effet. Etant donné qu'il est légitime d'attribuer d'emblée un niveau de confidentialité « normal » à ses données de patient, aucun dispositif ne saurait bloquer automatiquement ce choix. Pour cette raison, nous proposons de poser trois ou quatre questions relatives aux conditions d'utilisation pour s'assurer que le patient a compris la portée du dossier électronique. En outre, en cas de rétrogradation du niveau de confidentialité, une fenêtre de navigation indiquant brièvement les conséquences de cette mesure devrait systématiquement apparaître. On peut imaginer, par exemple, le message suivant : « Etes-vous sûr de vouloir rétrograder les données sélectionnées au niveau de confidentialité « normal » et permettre ainsi à tous les professionnels de la santé d'y avoir accès ? » Ces mesures participent à une plus grande responsabilisation de la personne et à une meilleure compréhension du système du dossier électronique du patient. Il faut toutefois veiller à ne pas transmettre des données sensibles par des canaux peu fiables.

8 Sécurisation des portails d'accès

8.1 Introduction

Risques liés aux portails d'accès

Les portails d'accès constituent un élément critique pour la sécurité de l'ensemble du dossier électronique du patient. Composés d'applications Web et d'applications mobiles, ils sont vulnérables et permettent d'accéder à des données sensibles. Une attaque dirigée activement contre un portail d'accès peut nuire durablement à la confidentialité et à l'intégrité des données du DEP ou porter atteinte à la disponibilité du système dans son ensemble. OWASP Top 10 y compris Mobile [OWASP-Top10] et [OWASP-MobileTop10] présentent les principaux risques ; ces risques doivent être limités par des mesures appropriées.

Le présent document couvre les principales mesures permettant de réduire les risques. Les mesures portent sur différents aspects, comme l'architecture et le design, le développement et la mise à disposition d'applications.

Les recommandations énoncées s'appliquent en partie aussi à d'autres éléments de l'infrastructure TIC. Pour offrir une bonne vue d'ensemble, ces éléments sont indiqués dans la figure ci-dessous.

Application

Délimitation

L'objectif consiste à assurer un transfert sécurisé des données ainsi que la transmission de données entre les données sensibles du DEP et l'utilisateur (professionnel de la santé ou patient) via le portail d'accès.

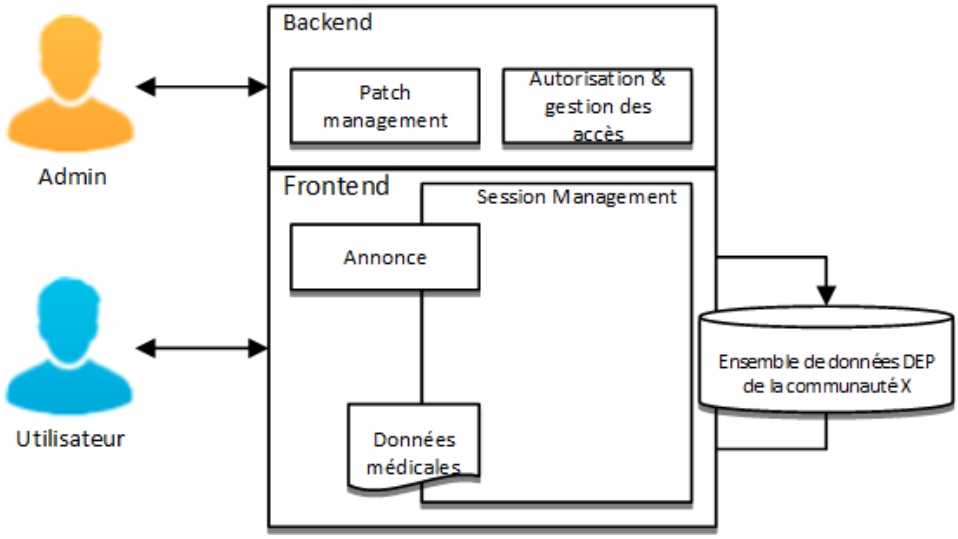

Figure 8 : Portails d'accès

Les terminaux des utilisateurs jouent un rôle déterminant en termes de sécurité des données. Les équipements qui accèdent aux données du DEP via un portail d'accès devraient au minimum répondre aux exigences suivantes :

- Le système d'exploitation et, au minimum, le navigateur Web, le lecteur PDF, le logiciel antivirus et les composants intervenant dans la reproduction de contenus extraits d'Internet doivent être actualisés en permanence.

- Les signatures des logiciels antivirus exploités sont actualisées en permanence.
- Les supports de données sont cryptés.
- Le navigateur Web est configuré strictement de manière à offrir une sécurité maximale, selon les possibilités techniques existantes et l'environnement dans lequel il opère. Dans la mesure du possible, il y a lieu d'utiliser des navigateurs préconfigurés et renforcés.

8.2 Architecture, design et scénarios de menaces

But

Afin de limiter au maximum la surface d'attaque, il y a lieu d'exploiter exclusivement les composants nécessaires au traitement des données. L'architecture et le code doivent être harmonisés de manière utile.

Rubriques CTO applicables

3.1, 3.2, 3.3, 9.1, 9.2, 9.3, 9.4, 9.5, 14.4.2

Développement sûr et estimation continue des risques

Le processus de développement doit garantir que :

- des principes assurant un développement software en toute sécurité s'appliquent pendant toute la durée de vie du produit ;
- le code source est géré de manière centralisée et que l'accès à ce code est limité, contrôlé et historisé ;
- l'application comprend un scénario de menaces et une analyse des risques faisant l'objet d'un suivi permanent. Conformément aux CTO, les risques suivants doivent être traités activement : la manipulation de données, l'altération de l'intégrité des données (tampering), la simulation d'une identité (spoofing), la contestation d'une action (repudiation), la perte de confidentialité (information disclosure) et l'extension des droits liés à une fonction ou à l'identité (elevation of privilege) ;
- aucune donnée productive ne se trouve dans les environnements de développement et de test ;
- tous les composants opérationnels (p ex. bibliothèques) sont connus et documentés, proviennent d'une source fiable et peuvent être exploités ; voir également ch. 6.7 ;
- qu'aucun service de messagerie ou d'analyse n'est exploité ou intégré (Google Analytics, etc.).

Design et architecture

L'architecture et le design de l'application doivent garantir que :

- l'application fait une nette distinction entre le data layer, le control layer et le display layer ;
- tous les contrôles de sécurité (y compris les bibliothèques qui accèdent à des services de sécurité externes) ont une implémentation centrale ;
- le code client ne contient pas de données sensibles, de clés secrètes ou d'informations protégées par des droits de propriété intellectuelle ;
- l'application et les différentes étapes de traitement suivent une logique séquentielle conformément au processus de gestion, toutes les étapes devant être traitées chronologiquement à des intervalles de temps réalistes.

8.3 Authentification et vérification

L'identité de chaque utilisateur est vérifiée ; seules personnes autorisées ont accès au dossier électronique du patient.	But
1.4.1, 1.4.2, 1.4.3, 1.6.2, 8.2.2, 8.3.1, 8.4.1, 8.4.2	Rubriques CTO applicables
Les éléments suivants doivent être pris en considération lors de l'élaboration des contrôles d'authentification : • Les moyens d'identification employés remplissent les critères du niveau de confiance LoA 3 de la norme ISO/IEC 29115:2013(E). Voir également art. 23bis, 26 ODEP. • Les pages et les ressources (non prévues pour être accessibles publiquement) exigent systématiquement une authentification valable, requise exclusivement par le serveur. • Les données d'authentification sont exclusivement transmises sous forme cryptée ; les pages et les fonctions uniquement accessibles à des cercles restreints d'utilisateurs peuvent seulement être consultées via des canaux cryptés. • Les canaux cryptés sont dotés d'un système de gestion des erreurs fort (error handling) et récupèrent en cas d'échec (fail-safe). • Le nombre de requêtes est limité dans le temps (throttling). • Toutes les tentatives d'authentification, abouties ou non, présentent un temps de réaction moyen identique. • Toutes les tentatives de connexion (réussies ou non) sont historisées. • Toutes les fonctions de gestion des comptes présentent une protection identique à celle de l'authentification.	Conception de l'authentification
Les éléments suivants doivent être pris en considération en ce qui concerne une éventuelle action sur un mot de passe : • Le mot de passe n'apparaît pas en clair lors de la saisie. • Les champs de saisie supportent des mots de passe longs et complexes (au moins 50 caractères, pas de restriction par rapport à des caractères spécifiques). • Les mots de passe ne sont pas mémorisés en clair ; ils sont protégés par des procédures de hachage fiables (hashing) (voir ch. 6.6). • Des mots de passe forts et complexes (au moins 10 caractères avec majuscules/minuscules, signes spéciaux et exclusion de mots évidents) doivent être utilisés.	Entrer le mot de passe
Lorsqu'un utilisateur a oublié son mot de passe ou s'il souhaite le modifier, les éléments suivants doivent être pris en considération avant toute réinitialisation ou modification : • L'utilisateur ne doit pas avoir à répondre à des questions confidentielles ou relevant de la sécurité sur la base d'informations accessibles publiquement. Les questions doivent lui être spécifiquement posées (p. ex. liste déroulante).	Réinitialiser ou modifier le mot de passe

- La fonction de restauration du mot de passe et d'autres techniques de restauration doivent s'effectuer au moyen d'un jeton souple, d'un push mobile ou d'un mécanisme de restauration offline.
- La réinitialisation d'un mot de passe ne doit pas permettre d'établir un lien avec le mot de passe actif.
- Le nouveau mot de passe ne doit pas être transmis en clair à l'utilisateur.
- La réutilisation d'anciens mots de passe n'est pas possible en cas de changement du mot de passe.

Stockage de caractéristiques d'authentification

Les éléments suivants doivent être pris en considération en ce qui concerne le stockage (sauvegarde) de caractéristiques d'authentification :

- Toutes les données d'authentification donnant accès à des services externes sont cryptées et stockées dans un lieu de stockage protégé.
- Les clés API et les mots de passe ne figurent pas dans les répertoires de codes source ou les répertoires de codes source en ligne.

Anti énumération

Aucune fonction (en particulier en cas d'enregistrement, de login, de restauration de mot de passe) ne doit se prêter à une énumération des informations.

En d'autre termes, un utilisateur qui possède un compte ou qui échoue dans son authentification reçoit systématiquement le même message d'erreur.

8.4 Gestion des sessions

Les sessions doivent être régénérées à chaque nouvel accès au portail DEP ; il ne doit pas être possible de les partager ou de les deviner. Elles doivent être fermées complètement en fin de tâche.	But
4.16.1, 4.16.2	Rubriques CTO applicables
Les éléments suivants doivent être pris en considération en ce qui concerne la manière de concevoir la gestion d'une session : • Un gestionnaire de session connu et performant est exploité (dans la mesure du possible, pas de développement interne). • En cas de déconnexion par l'utilisateur ou d'expiration d'une session (timeout), la session doit être entièrement terminée. • Le nombre de sessions actives simultanément est limité.	Gestion de session
La gestion des identifiants de session s'effectue en tenant compte des éléments suivants : • Les ID de session sont générés de manière à ne pas pouvoir être devinés. • L'ID de session n'apparaît pas dans une URL, dans un message d'erreur ou dans un historique. Un rewriting d'URL n'est pas possible pour les cookies de session. • Toutes les authentifications et nouvelles authentifications réussies génèrent une nouvelle session et un nouvel ID de session. • Si des ID de session sont sauvegardés dans des cookies, le chemin de validation doit être aussi restreint que possible. • Les jetons d'authentification portent les instructions HttpOnly et secure.	ID de session
L'utilisateur dispose des possibilités suivantes : • Toutes les pages requérant une authentification proposent une fonction de déconnexion simple à utiliser et clairement visible pour l'utilisateur. • Un listing actif des sessions effectuées est indiqué dans le profil de l'utilisateur ou dans un emplacement similaire. L'utilisateur doit pouvoir achever toute session active. • La dernière annonce est indiquée : « dernière annonce jj.mm à hh.mm »	Contrôle des sessions par l'utilisateur

8.5 Contrôle et gestion des accès

Les utilisateurs doivent posséder des données d'authentification valables pour accéder aux portails d'accès. La gestion des autorisations s'effectue sur la base du rôle de l'utilisateur et se limite aux fonctions et aux données nécessaires à cet effet.	But
1.3.4, 1.3.5, 1.4.1, 1.6.2, 2.2, 2.3.2, 4.8.1, 4.8.2, 4.8.3, 4.13.1	Rubriques CTO applicables
Tous les portails d'accès sont régis par les principes spécifiques applicables aux niveaux d'autorisation et de confidentialité ainsi qu'à la consultation de données. Le contrôle d'accès doit implémenter ces exigences dans l'application. Cela vaut pour l'ensemble des fonctions, fichiers, URL, contrôleurs, services et autres ressources de l'application.	Gestion des accès
La consultation de répertoires sur le serveur Web ne doit pas être possible. Les applications ne doivent pas permettre de consulter des métadonnées de fichiers ou de répertoires.	Consultation de répertoires
Tous les accès doivent être contrôlés. Un contrôle efficace prévoit les mesures suivantes : • Le contrôle des accès exploite un système de gestion des erreurs fort (fail-safe). • Les principes régissant les accès sont requis par le serveur. • Un dispositif central du contrôle des accès est mis en place (Policy Decision Point et Policy Enforcement Point). • Toutes les requêtes d'authentification (y compris les décisions négatives) sont historisées.	Contrôle des accès
Les points suivants doivent être pris en considération pour éviter une manipulation indésirable des données : • Les caractéristiques utilisateurs et données ainsi que les directives d'accès ne sont pas modifiables par l'utilisateur. • Tous les accès et toutes les requêtes sont vérifiés au moyen des autorisations accordées à l'utilisateur connecté au système.	Protection contre les manipulations
L'application ou le framework exploite un dispositif de protection des transactions fort (p. ex. jetons anti-CSRF aléatoires).	Protection des transactions

8.6 Validation des entrées

Toute entrée est validée et vérifiée quant à son exactitude. Les données provenant de sources externes sont à considérer avec prudence et les actions malveillantes doivent être traitées en conséquence.	But
4.5, 4.7.3	Rubriques CTO applicables
Pour que les données soient stockées correctement et en toute sécurité, les éléments de validation suivants doivent être pris en considération : • Les entrées erronées ou non validées (input) ne sont pas traitées. • La validation des inputs est requise par le serveur. • Une validation de l'input est effectuée pour tous les types de données. • L'ensemble des entrées doit être validée ; cela ne s'applique pas uniquement aux champs du formulaire HTML, mais à toutes les sources d'entrée, comme accès REST, paramètres d'interrogation, HTTP-Headers, cookies, fichiers batch, RSS-Feeds, etc.	Validation
Les éléments suivants doivent être pris en considération en ce qui concerne les attaques par injection : • Tous les SQL-Queries, HQL, OSQL, et NOSQL, les procédures sauvegardées et leur sollicitation sont protégés par des instructions ou des paramètres d'interrogation (empêcher une attaque par injection SQL). • Les injections LDAP ou les injections OS Command sont impossibles. • Les Remote File Inclusion (RFI) ou Local File Inclusion (LFI) ne doivent pas être exposées à des attaques malveillantes. • L'application n'est pas exposée aux attaques courantes XML, comme des manipulations XPath, ou aux attaques par injection XML.	Protection contre des attaques par injection
Les variables string utilisés dans les HTML ou d'autres codes Web client sont correctement cryptés.	Protection contre des attaques de type Cross-Site Scripting
L'environnement d'exécution (interpréteur, JVM, etc.) n'est pas exposé à dépassements de tampon (buffer-overflows).	Protection contre les dépassements de tampon (buffer-overflows)
Le transfert de données d'un contexte DOM à un autre s'effectue uniquement à l'aide de méthodes JavaScript fiables, comme .innerText et .val.	Contexte DOM
Les données authentifiées provenant de la mémoire client sont supprimées, p. ex. le navigateur DOM, une fois la session terminée.	Suppression des données à la fin de la session

8.7 Cryptographie

Les modules cryptographiques doivent être utilisés de manière sûre, selon les recommandations applicables.	But
2.5.1, 4.12	Rubriques CTO applicables
Les procédures cryptographiques utilisées et leur application s'effectuent conformément au ch. 5.	Fiabilité de la cryptographie

8.8 Gestion des erreurs et historisation

Les interactions système relevant de la sécurité doivent être historisées pour garantir une traçabilité. Les erreurs et les divergences évidentes doivent être traitées selon une procédure définie.	But
2.10, 4.13.1, 4.13.3	Rubriques CTO applicables
L'application ne doit pas générer des messages d'erreur ou des enregistrements de journaux contenant des données sensibles. Les ID de session, les versions software ou framework, les informations relatives au système d'exploitation ainsi que les informations personnelles et les données médicales sont concernés.	Données sensibles (données médicales)
Les éléments suivants doivent être pris en considération en ce qui concerne l'historisation : • Tous les événements mentionnés dans les [CTO] ainsi que les indications et informations correspondantes sont historisés. • Tous les symboles non imprimables et les signes de séparation dans les journaux sont correctement codés.	Historisation
Les mesures suivantes doivent être mises en œuvre pour protéger les journaux : • Tous les journaux sont protégés de manière à les mettre à l'abri d'accès non autorisés et de modifications. Les modifications effectuées ultérieurement doivent être visibles et historisées. • Les journaux, en particulier les données qu'ils contiennent, ne doivent pas être exécutés dans le journal des événements (log-viewing software). • La sauvegarde des logs s'effectue sur une autre partition pendant l'exécution de l'application. Il est recommandé de stocker les journaux dans un lieu central indépendant du système d'origine. Le dispositif utilisé à cet effet est protégé de manière à empêcher l'effacement de données ou l'enregistrement de modifications. Son intégrité est assurée par une fonction de hachage (hashing).	Protection des données historisées (journaux)

8.9 Protection de données sensibles

Les données doivent être protégées selon le degré de sensibilité qu'elles présentent ; elles peuvent uniquement être mises à la disposition d'un cercle défini d'utilisateurs. Toutes les données doivent être protégées de manière à empêcher une consultation ou une modification non autorisées.	But
2.1, 4.17, 10.2.1, 10.2.2, 10.2.3	Rubriques CTO applicables
Toutes les données sensibles (données permettant d'identifier une personne et données médicales) sont correctement identifiées et protégées en conséquence.	Identification de données sensibles
Les mesures suivantes doivent être mises en œuvre pour empêcher tout accès non autorisé à des données sensibles : • Les données sensibles sont transmises par HTTP Message Body ou Header (les paramètres URL ne sont pas utilisés pour transmettre des données sensibles). • Les données sensibles ne sont pas sauvegardées temporairement ou durablement sur le terminal client. • L'anti-caching-header est utilisé pour les données sensibles. • Les données sensibles faisant l'objet d'une sauvegarde intermédiaire sont protégées contre tout accès non autorisé et effacées dès que la transaction est achevée. • Si des données sont téléchargées à partir de l'application (exportation), l'utilisateur doit être informé qu'elles quittent l'environnement protégé.	Protection de données sensibles
Les accès trop fréquents à des données sensibles et un nombre inhabituellement élevé de demandes de saisie de données doivent être détectés et signalés.	Détecter des accès inhabituels

8.10 Transmission de données

Toutes les transmissions de données s'effectuent au moyen du protocole TLS. Une configuration éprouvée et un système de cryptage fort sont requis.	But
2.5, 4.15.3, 4.15.4, 4.15.6	Rubriques CTO applicables
Les éléments suivants doivent être pris en considération pour assurer une protection efficace des données sensibles (p. ex. données médicales) : • Toutes les transmissions (y compris les liaisons backend) s'effectuent au moyen du protocole TLS. • Toutes les transmissions requièrent une authentification.	Cryptage des transmissions (Voir ch. **Fehler! Verweisquelle konnte nicht gefunden werden.**)
Pour les certificats, voir les points énoncés au ch. **Fehler! Verweisquelle konnte nicht gefunden werden.**.	Utilisation de certificats

8.11 Configuration de sécurité HTTP

Le protocole HTTP est réduit aux méthodes indispensables et renforcé.	But
Pas de rubrique directement applicable	Rubriques CTO applicables
Les points suivants doivent être pris en considération en ce qui concerne la configuration de sécurité HTTP : • L'application accepte les méthodes HTTP Request qui ont été définies (p. ex. GET et POST) ; les méthodes non utilisées (p. ex. TRACE, PUT et DELETE) sont expressément interdites. • Le jeu de caractères doit être défini dans le header HTTP. • Les headers HTTP intégrés par un Proxy ou un SSO doivent également être authentifiés par l'application. • Les headers HTTP ne contiennent aucune information relative au système ou aux versions exploitées. • Content Security Policy (V2 – CSP) doit être opérationnel. Inline JavaScript est complètement désactivé, ou alors exécuter un contrôle d'intégrité sur Inline JavaScript sous la forme de CSP Noncing ou Hashing. • Le header X-XSS-Protection: 1; mode = block est également transmis.	Configuration de sécurité HTTP

8.12 Fichiers et ressources

Les fichiers potentiellement corrompus doivent être traités dans un environnement protégé. Les fichiers provenant de sources non fiables sont conservés hors du webroot.	But
3.3, 9.4.2	Rubriques CTO applicables
Les points suivants doivent être pris en considération en ce qui concerne les fichiers et les ressources intégrés dans l'application : • La redirection ou le forwarding d'URL est uniquement possible pour des objectifs expressément autorisés ; un message correspondant est affiché en cas de forwarding vers des contenus potentiellement corrompus. • Le système traite uniquement les formats de fichiers définis dans les CTO. • Toutes les entrées de données sont validées et vérifiées pour s'assurer qu'elles ne contiennent pas de virus. • Les fichiers sont conservés séparément de l'application, p. ex. hors du répertoire webroot. • L'accès à des ressources ou à des systèmes à distance extérieurs au serveur Web ou au serveur d'application doit être le moins fréquent possible. • Il faut s'abstenir d'utiliser des technologies Flash, Active-X, Silverlight, NACL ou Client qui ne sont pas nativement supportées par les standards du navigateur W3C.	Gestion de fichiers et de ressources

8.13 Applications mobiles (Apps)

Les données traitées au moyen d'applications mobiles doivent présenter le même degré de protection que celui offert par les applications Web classiques. Les éventuelles sauvegardes (temporaires ou permanentes) doivent être limitées. La communication doit être intégralement cryptée.	But
Pas de rubrique directement applicable	Rubriques CTO applicables
Les points suivants doivent être pris en considération en ce qui concerne les applications mobiles (apps) : • Les valeurs ID enregistrées dans l'appareil qui peuvent être sollicitées par d'autres applications, notamment le code UDID ou IMEI, ne doivent pas être utilisées comme jetons d'authentification. • Les données du DEP ne doivent pas être mémorisées dans l'appareil sous forme non cryptée. • Tous les contenus ayant fait l'objet d'une sauvegarde intermédiaire doivent être protégés.	Applications mobiles (Apps)

8.14 Services Web

Tous les services web requièrent un système d'authentification et un système approprié de gestion des sessions. Tous les paramètres doivent être intégralement validés.	But
2.5, 2.9.26, 4.15.3, 4.15.4, 4.15.6	Rubriques CTO applicables
Les points suivants doivent être pris en considération en ce qui concerne les services Web : • Un système de cryptage identique est utilisé pour le client et le serveur (UTF-8). • L'accès aux fonctions d'administration et de gestion est limité. • Un schéma XML ou JSON est utilisé. Toutes les entrées sont vérifiées sur cette base. • Toutes les entrées sont validées et possèdent des restrictions de taille correspondantes. • Les services Web exploitant la norme SOAP sont compatibles avec l'interopérabilité des services Web (WS-I) et supportent le cryptage TLS. • Toutes les sessions sont authentifiées. L'utilisation de clés API statiques ou de logiciels similaires doit être évitée. • L'intégrité des messages entrant est vérifiée.	Services Web

8.15 Configuration et maintenance

Les librairies et les plateformes doivent être régulièrement actualisées. Un processus de gestion des patchs doit être défini et appliqué à cet effet. L'objectif consiste à réaliser une configuration de base répondant au principe « Secure by Default » pour tous les composants et configurations exploités.	But
Pas de rubrique directement applicable	Rubriques CTO applicables
Les points suivants doivent être pris en considération en ce qui concerne la configuration de composants : • La version et la configuration les plus récentes sont systématiquement exploitées ; il y a lieu de s'assurer que le degré de sécurité reste identique. • Les configurations, fichiers, applications à titre d'exemple et utilisateurs standard non nécessaires sont effacés. • La communication entre les composants est authentifiée et cryptée. • L'utilisation de sandboxes ou de conteneurs permet de mettre des applications séparément à disposition.	Configuration
Des administrateurs autorisés doivent pouvoir vérifier l'intégrité des configurations en lien avec la sécurité afin de garantir que celles-ci n'ont pas été manipulées.	Intégrité de la configuration
Tous les composants d'application sont signés.	Utilisation de composants signés

9 Annexe

9.1 Rédaction

Redguard AG
Eigerstrasse 60
CH-3007 Berne
+41 (0)31 511 37 50
https://www.redguard.ch

Responsable de projet :
Alexander Hermann, Managing Partner

9.2 Membres du groupe d'accompagnement

Nom	Organisation
Cedric Michelet	Hôpital du Valais
Damiano Boppart	CCC-ZH
Frank Calcavecchia	Hôpitaux Universitaires de Genève
Heinz Schütz	BINT GmbH
Hernani Marquez	CCC-ZH
Jan Zbinden	Kanton Basel-Stadt
Johannes Gnägi	eHealthSuisse
Klaus Pirker	-
Lucas Schult	Health Info Net (HIN) AG
Martin Bruderer	Universitätsspital Basel
Martin Smock	Swisscom Health AG
Mauro Rudi	Kanton Basel-Stadt
	Swisscom Health AG
Stefan Beyeler	Spital Emmental
Thomas Menet	Kanton Aargau
Volker Birk	CCC-ZH
Walid Ahmed	Office fédéral de la santé publique

Tableau 1 : Groupe d'accompagnement

9.3 Liste des abréviations

Abréviation	Signification
AES	Advanced Encryption Standard
API	Application programming interface
ASLR	Adress space layout randomization
ASVS	Application Security Verification Standard
CAs	Certification Authorities
CBC	Cipher-Block Chaining
CERTs	Computer emergency response team
CORS	Cross-Origin Ressource Sharing
CSP	Content Security Policy
CSRF	Cross-Site Request Forgery
CTR	Counter Mode
DEP	Data Execution Prevention
DOM	Document Object Model
DHE	Diffie-Hellman Ephermal
DSMS/GPD	Datenschutzmanagement / Gestion de la protection des données
FIPS	Federal Information Processing Standard
GCM	Galois Counter Mode
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HQL	Hibernate Query Language
HSM	Hardware Sicherheits Modul
HSTS	HTTP Strict Security Header
ID	Identifier (Identifiant)
IDS	Intrusion Detection System
ICT	Information and Communication Technology
IMEI	International Mobile Equipment Identity
IPS	Intrusion Prevention System
ISMS	Informationssicherheitsmanagementsystem / Système de gestion de la sécurité des informations
IV / VI	Initialisierungsvektor / Vecteur d'initialisation
JSON	JavaScript Object Notation
JVM	Java Virtual Machine
KEK	Key Encryption Keys
LDAP	Lightweight Directory Access Protocol
LFI	Local File Inclusion
MAC	Message Authentification Code
MD	Message Digest
NACL	Bibliothèque programmes
Noncing	Nonce → „used only once“
NOSQL	Not only SQL

OS	Operating System
OSCP	Online Certificate Status Protocol
OSQL	Object-Structured Query Language
OWASP	Open Web Application Security Project
PFS	Perfect Forward Secrecy
REST	Representational State Transfer
RFC	Request for Comments
RFI	Request for Information
RPO	Recovery Objectives
RSA	Rivest, Shamir und Adleman – Procédure de cryptographie asymétrique
RSS	Rich Site Summary / Really Simple Syndication → Web-Feed
RTO	Recovery Time Objectives
SHA	Secure Hash Algorithm
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSO	Single Sign-on
TLS	Transport Layer Security
U-DID	Unique Device-ID
URLs	Uniform Resource Locator
W3C	World Wide Web Consortium
WS-I	Web Services Interoperability
XML	Extensible Markup Language
X-Path	Langage d'interrogation pour évaluer des parties d'un document XML
XSS	Cross-Site-Scripting

Tableau 2 : Liste des abréviations

9.4 Mapping CTO/ISO

Voir annexe 1_CTO/ISO_Mapping_v1.00.xlsx

9.5 Suspens

Les thèmes suivants sont en suspens et doivent être pris en considération pour les remaniements à venir.

N°	Description
P1	Dans la pratique, l'attribution de la fonction de responsable de la protection et de la sécurité des données sera vraisemblablement couplée à des fonctions existantes. Les expériences faites dans ce domaine devraient également être intégrées ultérieurement dans la présente aide la mise en œuvre.
P2	Dans quelle mesure est-il possible d'éliminer automatiquement des documents d'un ensemble de données ou de les bloquer (en cas de soupçon d'un logiciel malveillant) ? Il peut arriver que des données

	médicales vitales deviennent inaccessibles ou qu'elles soient effacées. Cette question est à étudier sous l'angle juridique.
P3	Examen d'autres procédures d'authentification
P4	Applicabilité des dispositions (en particulier en ce qui concerne les portails d'accès) à des systèmes primaires avec une forte intégration DEP.