Politique de sécurité de l'information (PSI)

Afin d'atteindre les buts qu'elle s'est fixé, l'association « Communauté de Référence Dossier électronique du patient de Neuchâtel » (CR DEP NE) s'engage à :

- Établir des objectifs de sécurité de l'information
- S'assurer de la compatibilité des objectifs de sécurité de la CR DEP NE avec le contexte légal
- Mettre à disposition les ressources matérielles, humaines et financières requises pour honorer les présents engagements
- Communiquer sur l'importance de disposer de politiques et de procédures efficaces garantissant la sécurité et la protection des données
- Identifier les risques potentiels de sécurité et mettre en place des moyens de remédiation
- S'assurer de l'atteinte des objectifs fixés au travers d'une politique d'amélioration continue

À cette fin, la CR DEP NE délègue la réalisation des tâches organisationnelles, techniques et financières lui incombant selon la Loi fédérale sur le Dossier Électronique du Patient (LDEP), ses ordonnances et annexes à l'association « Structure Porteuse de la Communauté de référence Dossier Électronique du Patient de Neuchâtel » (SP DEP NE).

Ainsi, la SP DEP NE se dote d'une politique de sécurité de l'information (PSI) et réalise un concept SIPD (Sûreté de l'Information et Protection des Données) servant de base à la définition des mesures de sécurité de l'information et de protection des données. Le concept SIPD, basé sur les bonnes pratiques de la norme EN ISO/IEC 27001:2017, décrit notamment les risques résiduels liés à l'exploitation du DEP, l'organisation de la CR DEP NE / SP DEP NE et le concept d'urgence. Ce concept SIPD, aussi appelé Système de Management de la Sécurité de l'Information (SMSI), est porté par le Responsable de la Sécurité des Systèmes d'Information (RSSI ou CISO – Chief Information Security Officer), en collaboration avec le Responsable de la Protection des Données (RPD ou DPO – Data Protection Officer).

La politique de sécurité de l'information est publique, le concept SIPD, les directives et procédures associées n'étant cependant communiqués qu'aux parties prenantes garantissant la sécurité de l'information.

Objectifs stratégiques

- Protéger l'information par la mise en œuvre de mesures proportionnées visant à assurer le niveau de sécurité requis en termes de confidentialité, d'intégrité, de disponibilité et de concordance
- Respecter toutes les exigences légales, contractuelles et internes nécessaires à l'obtention et au maintien de la certification au sens de la LDEP

- Définir le domaine d'application, les objectifs stratégiques ainsi que les responsabilités nécessaires pour atteindre l'objectif de protection visé par le concept SIPD

Objectifs opérationnels

Les objectifs opérationnels définis ci-dessous soutiennent et renforcent les objectifs stratégiques.

- **Confidentialité : objectif d'aucune (=0) perte de confidentialité sur une année**

Afin de remplir cet objectif, la SP DEP NE met en œuvre les mesures suivantes.

En ce qui concerne la plateforme « Mon Dossier Santé », la SP DEP NE transfère le risque à son fournisseur, celui-ci étant en l'occurrence couvert par le Concept SIPD de La Poste. De plus, la SP DEP NE a signé avec elle un NDA contenant des pénalités en cas de non-respect de celui-ci.

La SP DEP NE s'assure de la confidentialité des données sensibles qu'elle traite dans le cadre de ses processus de travail liés au DEP. Une fuite éventuelle d'informations provenant du personnel administratif est découragée par le secret de fonction inclus dans les contrats de travail.

De plus, la confidentialité des informations traitées est garantie par le secret médical (dans la majorité des cas) et/ou un accord de confidentialité systématique entre l'institution et la personne accédant au DEP. La confidentialité du stockage des informations sensibles traitées par la SP DEP NE s'appuie sur l'infrastructure informatique sécurisée du Service Informatique de l'Entité Neuchâteloise (SIEN).

Des mesures de sécurité physiques et logiques empêchent les accès non-autorisés à l'information, que ce soit au niveau des locaux, de l'exploitation ou des communications.

Le document « Informations aux patients utilisant Mon Dossier Santé » indique aux patients les bonnes pratiques pour garantir la confidentialité de leurs données. La SP DEP NE sensibilise également les professionnels et auxiliaires de la santé aux risques découlant de la perte de confidentialité des données sensibles traitées dans le cadre des processus de travail liés au DEP, en plus des contraintes fortes de sécurité qui leur sont imposées. Des politiques spécifiques d'accès à l'information, ainsi que des directives d'écran verrouillé et de bureau propre, sont également appliquées par la SP DEP NE.

Pour toutes ces situations, un indicateur peut être retenu, par exemple l'absence de fuite dans les médias (information devenant publique). Des contrôles réguliers auprès des prestataires de soins, ainsi que des audits internes et externes de la CR DEP NE, garantissent que les données ne sont pas compromises. Dans le cas contraire, la SP DEP NE doit pouvoir rapidement prendre les mesures adaptées ; la gestion des incidents en lien avec la perte de confidentialité est prise en charge par une cellule de crise composée de membres de la SP DEP NE, du SIEN, du CIGES et de La Poste, selon que l'origine de l'incident soit le système primaire ou le système secondaire exploité par La Poste. Il est également possible que des personnes externes soient appelées en renfort (p. ex. comité de sécurité intercommunautaire, NCSC, etc.)

Un plan de communication en cas de crise est défini dans le plan d'urgence.

- **Intégrité : objectif d'aucune (=0) perte d'intégrité sur une année**

Afin de remplir cet objectif, la SP DEP NE met en œuvre les mesures suivantes.

En ce qui concerne la plateforme « Mon Dossier Santé », la SP DEP NE transfère le risque à son fournisseur, celui-ci étant en l'occurrence couvert par le Concept SIPD de La Poste.

En ce qui concerne les moyens d'identification pour l'accès au DEP, la SP DEP NE transfère le risque aux fournisseurs d'identité électronique autorisés, le risque étant couvert par l'obligation de certification de ces fournisseurs selon l'annexe 8 ODEP-DFI.

Néanmoins, le principal risque en lien avec les pertes d'intégrité est lié aux processus et à la bonne gestion des droits d'accès à l'information (non-ségrégation, révocation, mutation) et aux erreurs des utilisateurs de la plateforme Mon Dossier Santé (formations nécessaires).

Les archives de la SP DEP NE sont hébergées auprès du SIEN, qui dispose de toutes les mesures de sécurité nécessaires pour assurer l'intégrité de ces données.

Le document « Informations aux patients utilisant Mon Dossier Santé » indique aux patients les bonnes pratiques pour garantir l'intégrité de leurs données

Pour tous les prestataires de soins affiliés à la CR DEP NE, un niveau de sécurité physique et logique est exigé selon la LDEP, comprenant au minimum des logiciels de sécurité (i.e. antivirus, firewall) et des politiques restrictives de droits d'accès.

- **Disponibilité : disponibilité maximale de la plateforme « Mon Dossier Santé »**

Afin de remplir cet objectif, la SP DEP NE met en œuvre les mesures suivantes.

En ce qui concerne la plateforme « Mon Dossier Santé », la SP DEP NE a conclu avec son fournisseur, La Poste, un Service Level Agreement (SLA) « gold » de 99.9% de disponibilité et de 6 pannes par an au maximum. Ce SLA est le même en ce qui concerne l'accès des patients et prestataires de soins à la plateforme « Mon Dossier Santé ».

La SP DEP NE évalue annuellement la disponibilité effective de la plateforme durant l'année écoulée. Si celle-ci est inférieure au SLA conclu, elle est en droit d'exiger les pénalités prévues. La gestion des incidents est assurée par La Poste (cf. Concept SIPD de La Poste), qui est apte à réagir rapidement et de manière adéquate.

Les locaux de la SP DEP NE sont toujours disponibles (accès 24/7), sauf cas de force majeure (i.e. incendie). La disponibilité de l'infrastructure informatique est maximale et basée sur le principe du « best effort » fourni par le SIEN. De plus, le SIEN appliquant les mesures préventives / correctives durant les week-ends, la SP DEP NE n'est quasiment pas impactée en termes de disponibilité.

L'exploitation des prestations informatiques fournies par le SIEN est assurée de la manière suivante :

- Du lundi au vendredi, de 08h à 12h et de 13h30 à 17h
- En-dehors de ces intervalles, le traitement se fait le prochain jour ouvrable (NBD - Next Business Day)

Les prestataires de soins sont responsables de la disponibilité de leurs propres équipements (matériel, logiciels, connexion internet, etc.).

- **Concordance : stockage des données médicales relatives à un patient dans le bon compte DEP**

Afin de remplir cet objectif, la SP DEP NE s'assure que la base de données patients (MPI - Master Patient Index) de la CR DEP NE est à jour et que sa base de données des professionnels de la santé (HPD – Health Professionals Database) est bien synchronisée avec le HPD national. Des évaluations régulières prévoient une procédure de clearing en cas de doublons dans le système. Celles-ci permettent également de s'assurer que les bons documents sont attribués au DEP du bon patient, notamment grâce à l'utilisation d'un identifiant unique (NIP – Numéro d'identification du patient).

- **Traçabilité : légitimité et suivi des accès au compte DEP d'un patient**

Afin de s'assurer que les accès aux DEP des patients sont légitimes, la SP DEP NE, avec le concours de la Poste, peut s'appuyer sur la traçabilité de toute action effectuée sur la plateforme. Ceci s'applique aussi bien pour les actions effectuées par les patients et leurs représentants que par les professionnels et auxiliaires de santé et les administrateurs de la plateforme. En cas de plainte de la part d'un patient, il est ainsi possible d'identifier les accès abusifs et de prendre les mesures nécessaires.

Revue des objectifs

Une revue de la politique de sécurité de l'information est effectuée au minimum une fois par année par le RSSI et le CoDir de la SP DEP NE, afin d'évaluer si les objectifs fixés sont toujours :

- Pertinents
- En adéquation avec les attentes des parties prenantes
- Correctement mis en œuvre
- Disponibles pour toute personne concernée
- Efficaces

Dans le cas contraire, les objectifs sont réactualisés et/ou des modifications sont effectuées suite à l'analyse de risques associée.

Mise en œuvre de la politique de sécurité de l'information

Conformément à la LDEP, la SP DEP NE s'engage à mettre en œuvre la présente politique et toutes les mesures permettant de réduire les risques liés à la sécurité et la protection de l'information, qu'ils soient internes, externes, environnementaux, volontaires ou fortuits.

Une analyse de risques est effectuée au minimum une fois par année, afin de s'assurer que les objectifs de protection sont bien atteints :

- Les scénarii de menaces sont alignés sur les objectifs stratégiques
- L'analyse de risques permet de comparer les coûts engendrés par les mesures de réduction du risque aux bénéfices obtenus, afin de décider de la réduction ou de l'acceptation du risque identifié
- La mise en œuvre des mesures de réduction du risque est validée par la SP DEP NE

Afin de pouvoir estimer l'efficacité globale des mesures de sécurité mises en place dans le cadre de l'amélioration continue, la SP DEP NE utilise différents indicateurs évaluant :

- L'efficacité des plans de formation, sensibilisation du personnel administratif et médical à la sécurité de l'information (questionnaires de satisfaction et tests de connaissances)
- Les mesures de sécurité physique mises en place afin de limiter, uniquement au personnel autorisé, l'accès aux locaux et systèmes informatiques
- L'efficacité du secret de fonction, applicable au personnel de la SP DEP NE et aux membres de la CR DEP NE (cf. CGU « Mon Dossier Santé »), qui sont également soumis au secret médical
- L'efficacité des accords de confidentialité et non-divulgation (NDA) conclus avec le fournisseur de la SP DEP NE (La Poste), permettant ainsi la rétention (vs. Fuite) d'informations
- Le respect du SLA conclu avec La Poste pour la plateforme « Mon Dossier Santé »
- La sécurisation (adéquation) du matériel informatique via le nombre de pertes d'intégrité et de confidentialité atteint en une année (objectif = 0)

Afin d'assurer la sécurité de l'information, la SP DEP NE édicte une documentation spécifique et s'assure que celle-ci soit connue de tous ses partenaires. Elle se compose des documents suivants :

- La présente politique de sécurité de l'information (stratégie de sécurité générale de la CR DEP NE)
- Les tâches et exigences spécifiques : indications et instructions relatives à la sécurité de l'information pour les membres de la CR DEP NE (cf. Contrats d'affiliation, déclarations de consentement)

- Les documents d'informations aux patients et au prestataires de soins accompagnant les déclarations de consentement et les contrats d'affiliation (CGU)
- Les processus, directives et procédures nécessaires à la mise en œuvre pratique de la sécurité de l'information dans le cadre des activités quotidiennes des prestataires de soins et des parties prenantes de la CR DEP NE, si pertinent

Il est important que chacune des parties prenantes soit consciente du rôle qu'elle joue dans la protection et la sécurité de l'information, et plus particulièrement le personnel qui utilise ou gère des informations au quotidien. Cela implique certaines exigences pour les prestataires de soins, qui font partie intégrante du contrat d'affiliation et qui sont décrites dans les CGU « Mon Dossier Santé » (Institutions) et (Professionnels et auxiliaires). Ces CGU sont disponibles sur le site internet www.mondossiersante.ch et transmises avec les contrats d'affiliation des institutions et des professionnels de la santé. Il est de la responsabilité de chaque institution de faire appliquer à l'interne lesdites CGU. Des contrôles d'audit interne sont régulièrement menés par la SP DEP NE pour s'en assurer.

Chacune des politiques, directives et procédures du concept SIPD est attribuée à un propriétaire, qui la développe, l'évalue et la passe en revue régulièrement.

Contexte de la communauté de référence

Situation initiale

Le 15 avril 2017, l'assemblée fédérale suisse a mis en application la loi fédérale sur le dossier électronique du patient (LDEP).

L'association « Communauté de Référence Dossier Électronique du Patient de Neuchâtel » (CR DEP NE), soumise à l'application de cette loi ainsi qu'aux différentes ordonnances et annexes qui en découlent, a délégué la réalisation de toutes les tâches techniques, organisationnelles et financières qui lui incombent à l'association « Structure Porteuse de la Communauté de Référence Dossier Électronique du Patient de Neuchâtel » (SP DEP NE).

Principales références légales

La LDEP est la principale législation dans le cadre du dossier électronique du patient, qui est complétée par différentes ordonnances et annexes. Plus particulièrement, l'annexe 2 ODEP-DFI détaille toutes les exigences envers les communautés et communautés de référence. Les législations suivantes s'appliquent également (liste non exhaustive) :

- RS 220 Code des obligations (CO, 01.01.1912)
- RS 311.0 Code pénal suisse (CPS, 01.01.1942)

- RS 235.1 Loi fédérale sur la protection des données (LPD, 01.07.1993)
- 150.30 Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE, 09.05.2012)

Principaux acteurs pour la sécurité du DEP

Les principaux acteurs de la sécurité des systèmes d'information associés au projet du DEP ainsi que leurs rôles sont les suivants :

Acteurs	Rôle / Responsabilité
CIGES	Service informatique des principales institutions de santé du canton de Neuchâtel, exploitant et responsable de la sécurité informatique de leur système primaire, de leur support et de la sensibilisation du personnel à la protection et la sécurité de l'information.
Communauté de Référence Dossier Électronique du Patient Neuchâtel (CR DEP NE)	Communauté de Référence pour le Dossier Électronique du Patient dans le canton de Neuchâtel au sens de la LDEP, composée de prestataires de soins. La CR DEP NE délègue toutes ses tâches à la SP DEP NE.
KPMG	Auditeur pour la certification de la CR DEP NE selon la LDEP
La Poste	Fournisseur technique de la plateforme « Mon Dossier Santé » et responsable de la sécurité de celle-ci.
Office Fédéral de la Santé Publique (DFI / OFSP)	Législateur pour le DEP (LDEP, ODEP, ODEP-DFI, annexes ODEP-DFI), responsable d'édicter les exigences de sécurité du DEP.
Patients	Bénéficiaires du DEP, responsables de la sécurité de leurs ordinateurs.
Prestataires de soins	Institutions et professionnels / auxiliaires de santé reconnus et autorisés par les patients à accéder à leurs DEP, responsables de suivre les directives et procédures de sécurité de l'information édictées par la SP DEP NE.
SIEN	Fournisseur de l'infrastructure informatique et d'une solution d'archivage des documents sensibles (GED) pour la SP DEP NE. Responsable de la sécurité de l'infrastructure soutenant les traitements effectués par la SP DEP NE, du service d'assistance et des politiques de sécurité pertinentes.

	Responsable de la sécurité des infrastructures soutenant les systèmes primaires dont le CIGES est responsable.
Structure Porteuse Dossier Électronique du Patient Neuchâtel (SP DEP NE)	Structure portant la construction et l'exploitation de « Mon Dossier Santé » (=DEP), sous mandat de la CR DEP NE. Elle est notamment responsable de valider les divers documents requis et de promouvoir la sécurité du DEP via la réalisation de directives et procédures à l'intention des membres de la CR DEP NE.

De plus, seules les personnes physiques ou morales suivantes sont inclues dans le domaine d'application :

- La CR DEP NE et ses membres (p. ex. institutions, cabinet médicaux, professionnels de la santé, auxiliaires de santé, personnel administratif des institutions)
- La SP DEP NE et son personnel (p. ex. personnel administratif de la cellule Cybersanté)
- Les adhérents à « Mon Dossier Santé » (p. ex. patients, représentants légaux)
- Les partenaires et fournisseurs en relation d'affaires avec la CR DEP NE ou la SP DEP NE

Politique approuvée lors de la Management Review de la SP DEP NE le 09.03.2023.