# Directive interne de sécurité en lien avec le DEP

## Introduction

Le présent document a pour but de décrire la nécessité de tenir une directive interne relative à la sécurité et à la protection des données dans le cadre de l’utilisation du Dossier Électronique du Patient (DEP), ainsi que de lister les différentes directives, processus et procédures appliquées par [Nom de l’institution].

## Principes généraux

Tous les documents devant être communiqués à la CR DEP NE (communauté proposant « Mon Dossier Santé », le DEP neuchâtelois) font partie intégrante de cette directive de sécurité en lien avec le DEP. Cela comprend notamment, mais n’est pas limitée à :

* Liste des coordonnées des responsables au sein de l’institution (annonces, formation, sécurité)
* Processus d’entrée, de gestion et de sortie des utilisateurs du DEP
* Engagements individuels à l’usage du DEP signés par chaque utilisateur
* Document prouvant que les utilisateurs du DEP sont soumis au secret médical et/ou professionnel (p. ex. contrat de travail type)
* Accord avec un fournisseur de moyen d’identification électronique (MIE) (p. ex. contrat de prestations)
* Critères d’identification des collaborateurs autorisés à accéder au DEP (= matrice des droits d’accès)
* Liste à jour des utilisateurs du DEP
* Plan de formation des utilisateurs du DEP

Ce recueil de documents constitue les preuves devant être apportées par [Nom de l’institution] lors d’audits internes et/ou externes à la CR DEP NE.

## Mesures de sécurité applicables

Conformément au ch. 2.3 des CGU de Mon Dossier Santé, [Nom de l’institution] s’engage à ne mettre à disposition des utilisateurs du DEP que des terminaux sûrs, répondant aux exigences suivantes :

* Utilisation de logiciels contre les programmes malveillants (p. ex. Antivirus) et de réseaux informatiques sécurisés (p. ex. Firewall)
* Mise à jour régulière et forcée des systèmes d’exploitation et des composants logiciels
* Gestion restrictive des droits d’accès administrateurs, ainsi que des mesures techniques et organisationnelles forçant le verrouillage des terminaux

Toute exception aux mesures décrites ci-dessus est empêchée par à développer.

### Cas spécifique : télétravail

[Nom de l’institution] interdit le télétravail pour les utilisateurs du DEP au moyen d’une directive institutionnelle et/ou des contraintes techniques suivantes : à développer

OU

[Nom de l’institution] autorise le télétravail à ses utilisateurs du DEP. Cependant, les mesures de sécurité applicables sont identiques à celles applicables au sein de l’institution et sont complétées par à développer.

## Gestion des incidents de sécurité

Conformément au ch. 2.2 des CGU Mon Dossier Santé et au processus générique « Annonces obligatoires à la CR DEP NE », le processus de gestion des incidents de sécurité applicable au sein de [Nom de l’institution] est le suivant :

1. Détection d’un incident
2. Évaluation initiale de l’incident
3. Remplissage d’une fiche de non-conformité (FNC)[[1]](#footnote-1)
4. Transmission de la FNC à la CR DEP NE par e-mail (info@mondossiersante.ch)

En cas d’urgence, la CR DEP NE est immédiatement prévenue par téléphone (032 889 52 61).

Sont considérés comme des incidents tous les événements impactant la confidentialité, l’intégrité et/ou la disponibilité de l’information / des données. Voici quelques exemples devant être annoncés à la CR DEP NE :

* Utilisation non-autorisée d’un mot de passe, usurpation d’identité, abus de droits
* Utilisation irrégulière ou illégale des systèmes informatiques (spam, piratage, etc.)
* Vol / perte de matériel informatique
* Intrusion physique dans les locaux ou intrusion informatique (programme, etc.)
* Divulgation de données sensibles
* Demandes d’information abusives (origine de la demande non garantie)
* Saturation / perturbation du système informatique (attaques DDOS, etc.)
* Non-respect des directives, règlements, mesures de sécurité par un collaborateur

En cas de doute, [Nom de l’institution] contacte le service d’assistance de la CR DEP NE.

## Revue des conditions d’accès au DEP

[Nom de l’institution] s’engage à pouvoir mettre à disposition de la CR DEP NE une liste des utilisateurs du DEP en tout temps. Cela permet notamment à la CR DEP NE de :

* S’assurer que les accès au DEP sont octroyés aux bonnes personnes et que celles-ci n’abusent pas de cet accès.
* S’assurer de la concordance des utilisateurs annoncés avec les comptes présents dans la base de données
* S’assurer que toutes les annonces organisationnelles (p. ex. changement de nom) ont été faites, conformément au ch. 2.2 des CGU Mon Dossier Santé

[Nom de l’institution] accède à Mon Dossier Santé de manière intégrée à son système primaire, qui est XY.

## Assistance aux utilisateurs

[Nom de l’institution] dispose (à décrire) / ne dispose pas d’un service informatique de 1er niveau (= prestataire informatique, p. ex. informaticien mettant à jour les machines).

En cas de besoin et conformément au processus « Fonctionnement du service d’assistance (Prestataires de soins) » fourni par la CR DEP NE, les utilisateurs du DEP peuvent faire appel au service d’assistance Mon Dossier Santé.

Celui-ci est atteignable en semaine, durant les heures de bureau :

**E-mail :** info@mondossiersante.ch

**Téléphone :** +41 32 889 52 61

1. Disponible à l’adresse suivante, rubrique « Institutions de santé » : <https://www.mondossiersante.ch/telechargements/> [↑](#footnote-ref-1)