



Agence nationale  
des informations partagées  
dans le domaine de la santé

**POLITIQUE DE SÉCURITÉ DE L'INFORMATION**

**CHARTRE INFORMATIQUE DU RÉSEAU HEALTHNET**

---

<b>Informations générales</b>			
Numéro de séquence	013		
État	Validée	Version	1.0
Classification	Public	Responsable	DBA
Distribution	Blanc	Date de mise en vigueur	31/03/2017

## Historique du document

Version	Date	Auteur	Modifications effectuées
1.0	31/03/2017	DBA	Version Validée

## Table des matières

<b>1. Introduction .....</b>	<b>4</b>
1.1. Contexte et enjeu .....	4
1.2. Objet .....	4
1.3. Mise à jour.....	4
1.4. Domaine d'application .....	5
1.5. Définitions .....	5
1.6. Engagements .....	6
<b>2. Accès au réseau .....</b>	<b>7</b>
2.1. Conditions d'accès .....	7
2.2. Sécurisation des moyens d'authentification .....	8
<b>3. Utilisations du réseau .....</b>	<b>9</b>
3.1. Utilisation conforme .....	9
3.2. Utilisation tolérée.....	9
3.3. Utilisations prohibées .....	9
<b>4. Modalités d'utilisation des Moyens informatiques .....</b>	<b>10</b>
4.1. Le poste de travail, les équipements nomades et logiciels .....	10
4.2. Internet.....	11
<b>5. Protection des données Personnelles .....</b>	<b>11</b>
5.1. Utilisateurs réseau HealthNet .....	11
5.2. Utilisation des services du réseau HealthNet.....	13
<b>6. Contrôle du réseau HealthNet .....</b>	<b>13</b>
6.1. Mesures en place .....	13
6.2. Traitement des incidents .....	14
<b>7. Violation et sanction .....</b>	<b>14</b>
7.1. Identification de la violation et mesures de protection.....	14
7.2. Sanctions .....	15
7.3. Autres sanctions.....	15
<b>8. Fins d'accès au réseau .....</b>	<b>15</b>
<b>9. Annexes .....</b>	<b>17</b>
9.1. Références Internes .....	17
9.2. Références Légales .....	17

## **1. INTRODUCTION**

### **1.1. CONTEXTE ET ENJEU**

La mission de l'Agence eSanté est de permettre le développement de l'utilisation des nouvelles technologies de l'information dans le secteur de la santé du Luxembourg pour favoriser l'échange et le partage de données de santé de manière optimale et sécurisée.

Dans ce cadre, l'Agence eSanté utilise et met à disposition des Établissements de santé et des Professionnels de Santé un réseau informatique hautement sécurisé pour assurer la conduite de leurs activités de prestataires de soins de santé et dans le respect de la confidentialité et la protection des données.

Cependant il doit être souligné qu'une mauvaise utilisation de ce réseau et/ou des outils connectés à ce réseau peut entraîner des risques d'atteinte à la confidentialité, à l'intégrité et sécurité des informations accessible au travers de celui-ci.

Dès lors l'Agence, les Établissements de santé connectés et les Utilisateurs pourront voir leur responsabilité engagée, et/ou supporter des coûts additionnels. Il relève donc de l'intérêt et de la responsabilité de chacun d'en protéger l'utilisation, notamment eu égard aux dispositions légales en vigueur.

Aussi la présente charte doit permettre une bonne compréhension du cadre d'utilisation du réseau HealthNet dans le respect des droits des Utilisateurs ainsi que pour en assurer les besoins de sécurité.

### **1.2. OBJET**

La présente charte définit les modalités d'accès et d'utilisation du réseau HealthNet mises à disposition par l'Agence auprès des Établissements de Santé et des Professionnels de Santé pour l'exercice de leur activité professionnelle.

Elle formalise également les règles légales et de sécurité relatives à l'utilisation de ce réseau, et mentionne dans ce cadre tout dispositif de contrôle et surveillance destinés à assurer la sécurisation des infrastructures techniques du réseau.

Elle mentionne dans ce cadre aux Etablissement de Santé et aux Utilisateurs les règles d'utilisation afin de les informer des responsabilités de chacun pour assurer la bonne utilisation du réseau ainsi que des conséquences d'une mauvaise utilisation de celui-ci.

### **1.3. MISE A JOUR**

Tout changement mineur de la présente charte devra être validé préalablement par les membres du réseau HealthNet lors de la réunion opérationnelle, et ce avant toute mise en application.

Tout changement majeur étant entendu comme changement ayant un impact sur les engagements des parties notamment en termes d'obligations de sécurité sera soumis à approbation préalable du Conseil de Gérance de l'Agence eSanté. La signature de la charte pourra être requise à nouveau, ou une communication devra être expressément réalisée pour informer les utilisateurs avant l'entrée en vigueur des modifications.

## **1.4. DOMAINE D'APPLICATION**

La charte s'applique aux Établissements de Santé, à l'Agence eSanté et à tous les utilisateurs du réseau HealthNet.

Chaque Utilisateur du réseau reçoit (envoi par email ou téléchargement) un exemplaire de la présente charte, dont il doit prendre connaissance des termes et s'engager expressément à leur respect par sa signature au sein du formulaire de demande.

## **1.5. DEFINITIONS**

### **1.5.1. Réseau HealthNet**

Le réseau HealthNet est un réseau dédié au secteur de la santé du Luxembourg permettant aux établissements de santé et aux professionnels de santé d'échanger des données médicales de manière sécurisée.

L'objectif du réseau HealthNet est de rationaliser les investissements en matière de sécurité des équipements réseau par la mise en commun d'une infrastructure commune, le partage de services et la mise en place d'un point unique de contact.

### **1.5.2. Moyens informatiques**

Les Moyens informatiques concernés sont, sans que cette liste ne puisse être considérée comme exhaustive, l'ensemble des serveurs, stations de travail, ordinateurs portables, postes de consultation connectés au réseau HealthNet, ainsi que l'ensemble du parc logiciel, des bases de données, des produits multimédias ou des périphériques affectés au fonctionnement des éléments décrits.

### **1.5.3. Maintien en Condition de Sécurité**

Le Maintien en Condition de Sécurité (MCS) représente les actions nécessaires à réaliser permettant d'atteindre les objectifs suivants :

- La maîtrise des risques de sécurité ;
- Le maintien dans le temps du niveau de conformité avec les exigences de sécurité précisées ci-après ; et
- Le transfert de responsabilité en cas d'incidents de sécurité comme explicité au sein du manuel d'utilisation du réseau HealthNet.

### **1.5.4. Établissement de Santé**

Tout établissement hospitalier tel que défini par la loi modifiée du 28 août 1998 sur les établissements hospitaliers, tout laboratoire d'analyses médicales tel que défini par la loi modifiée du 16 juillet 1984, tout autre établissement de soins agréé en application de la loi modifiée du 8 septembre 1998 réglant les relations entre l'Etat et les organismes œuvrant dans les domaines social, familial et thérapeutique, ainsi que toute pharmacie autorisée à s'établir en application des dispositions de la loi du 4 juillet 1973.

Est également repris dans cette catégorie, les centres de recherches en santé notamment le Luxembourg Institute of Health (LIH) et l'Integrated BioBank of Luxembourg (IBBL), et l'ensemble des groupements d'intérêt économique (G.I.E), les représentant.

### **1.5.5. Professionnel de Santé**

Toute personne physique dument agréementée pour exercer légalement au Luxembourg une profession de santé strictement définie au sein de la loi modifiée du 29 avril 1983 concernant l'exercice des professions de médecin, de médecin-dentiste et de médecin-vétérinaire, au sein de la loi modifiée du 26 mars 1992 sur l'exercice et la revalorisation de certaines professions de santé, ainsi qu'au sein de la loi modifiée du 31 juillet 1991 déterminant les conditions d'autorisation d'exercer la profession de pharmacien.

### **1.5.6. Agent de Santé**

Toute personne physique non-identifiée comme Professionnel de santé exerçant toutefois une activité professionnelle au sein d'Établissement de santé, de l'Agence eSanté ou organisme de sécurité sociale.

### **1.5.7. Utilisateur**

Toute personne physique identifiée comme Professionnel de Santé, Agent de Santé, Etablissement de Santé, ou technicien externe chargé de la maintenance des Moyens informatiques.

## **1.6. ENGAGEMENTS**

### **1.6.1. Engagements de l'Agence eSanté**

L'Agence eSanté veille à la disponibilité et à l'intégrité du réseau HealthNet aux fins de la bonne conduite de ses missions.

En ce sens, l'Agence eSanté s'assure :

- du respect du niveau de service garanti par le prestataire en charge de la gestion opérationnelle du réseau HealthNet ;
- de la définition et de la communication des règles d'usage des Moyens informatiques connectés au réseau HealthNet et de la vérification de leur application par déclaration de l'établissement sur base d'un formulaire d'évaluation fourni par l'Agence eSanté ;
- du maintien du niveau de sécurité du réseau HealthNet par l'évolution des solutions de sécurité mises en place ; et
- du respect de la législation relative à la protection des données à caractère personnel.

### **1.6.2. Engagements des Établissements de Santé**

Les Établissements de Santé connectés au réseau HealthNet s'engagent à maintenir les Moyens informatiques connectés au réseau HealthNet en Condition de Sécurité.

En ce sens, les Établissements de Santé s'assurent :

- de la tenue d'un inventaire des Moyens informatiques connectés au réseau HealthNet qui sont sous leur responsabilité ;
- que les logiciels installés sur leurs Moyens informatiques proviennent de sources réputées et respectent les licences d'utilisation de l'éditeur;

- de la protection contre les logiciels malveillants notamment par l'application régulière des correctifs de sécurité et de l'installation d'antivirus sur les Moyens Informatiques qui sont sous leur responsabilité ;
- de l'information et de formations adaptées et suffisantes de leurs Utilisateurs pour la bonne utilisation des Moyens informatiques mis à leur disposition ;
- de la sensibilisation de leurs Utilisateurs à la sécurité de l'information ;
- de la sauvegarde de ses données et de la protection physique de ses Moyens informatiques ; et
- de l'utilisation du réseau HealthNet et ses services dans le respect de la législation applicable à l'Établissement de santé dans l'exercice de son activité, et notamment de la législation relative à la protection des données à caractère personnel.

### **1.6.3. Engagements des Utilisateurs**

L'Utilisateur est responsable de l'utilisation qu'il fait des Moyens informatiques. Dans ce cadre, il s'engage à :

- connaître, respecter et faire appliquer l'ensemble des dispositions de la présente charte ;
- respecter les bonnes pratiques généralement connues<sup>1</sup> pour l'utilisation conforme et sécurisée des Moyens informatiques, sans préjudice des instructions émises par leur Établissement de Santé ou les règles d'utilisation du service concerné ; et
- utiliser le réseau HealthNet et ses services dans le respect de la législation applicable à l'exercice de son activité, et notamment de la législation relative à la protection des données à caractère personnel.

Lorsque l'Utilisateur est le propriétaire de ses Moyens informatiques, il s'assure :

- de la protection contre les logiciels malveillants par l'application régulière des correctifs de sécurité et de l'installation d'antivirus sur ses Moyens Informatiques qui sont sous sa responsabilité ;
- que les logiciels installés sur ses Moyens informatiques proviennent de sources réputées et respectent les licences d'utilisation ; et
- de la sauvegarde de ses données et de la protection physique de ses Moyens informatiques.

## **2. ACCÈS AU RÉSEAU**

### **2.1. CONDITIONS D'ACCES**

Les demandes d'accès au réseau HealthNet se font via un formulaire de demande qui est accessible sur la page <https://www.healthnet.lu>. L'Utilisateur s'engage par la signature du formulaire de demande au respect de la présente charte. La non-acceptation de cette charte ne permettra pas la mise à disposition de l'Utilisateur d'un accès au réseau HealthNet.

L'accès au réseau HealthNet est accordé aux Professionnels de Santé et aux Agents de Santé ainsi qu'aux Etablissements de Santé. L'accès aux services fournis au

---

<sup>1</sup> <https://www.cases.lu/>

travers du réseau HealthNet par un Établissement de santé et au réseau privé d'un Établissement de santé connecté au réseau HealthNet nécessite l'accord exprès de celui-ci au sein du formulaire de demande.

Chaque accès au réseau HealthNet est nominatif et les moyens d'authentification sont personnels. L'ensemble de ces moyens d'authentification est strictement personnel et confidentiel, et ne doit servir qu'à l'usage propre de l'Utilisateur.

L'intervention d'un technicien externe sur demande d'un Établissement de santé concernant ses Moyens informatiques connectés au réseau HealthNet, est réalisée sous sa responsabilité et sa surveillance. Il appartient à l'Établissement de demander un accès pour cette intervention, et en cas d'urgence il lui appartient de prendre les mesures nécessaires pour assurer le respect par le technicien de la présente charte, de la sécurité du réseau HealthNet et des moyens de connexion pendant son intervention.

## **2.2. SECURISATION DES MOYENS D'AUTHENTIFICATION**

Chaque Utilisateur se voit attribuer un moyen d'authentification pour se connecter directement au réseau HealthNet (token, carte magnétique, clefs de chiffrement ...).

Il est demandé aux Utilisateurs pour empêcher tout accès frauduleux au réseau HealthNet de :

- conserver confidentiels tous codes, mots de passe, cartes magnétiques, clefs ou tout autre dispositif de moyens de connexion qui leur sont confiés à titre strictement personnel ;
- veiller à la confidentialité du compte utilisateur qui leur est attribué à titre strictement personnel, ainsi que des informations auxquelles ils accèdent par l'intermédiaire de ce compte ;
- verrouiller leur ordinateur lorsqu'il quitte son poste de travail, verrouiller son matériel mobile (téléphone, tablette) par code ou pattern ou moyens biométriques;
- se déconnecter immédiatement après la fin de leur période de travail au sein de chaque application, compte utilisateur ou session ou lorsqu'ils s'absentent ;
- informer immédiatement le responsable informatique de son Etablissement ou le Service Desk du HealthNet de toute tentative d'accès frauduleux ou de tout dysfonctionnement qui leur paraîtrait suspect ;
- conserver de manière à empêcher toute perte, casse ou vol, tout moyen de connexion et dans ce cadre éviter tout transport de matériel lorsque cela n'est pas requis ;
- utiliser un mot de passe fort comportant au moins 8 signes dont une minuscule, une majuscule, un chiffre et un caractère de ponctuation ; et
- changer à intervalle régulier son mot de passe d'accès lorsque le changement n'est pas imposé techniquement.

Toute utilisation des moyens d'authentification de l'Utilisateur est présumée être de son fait. Le non-respect de la présente charte sera de la responsabilité de l'Utilisateur.



Il sera donné la possibilité à l'Utilisateur de pouvoir démontrer que l'utilisation des moyens d'authentification n'est pas de sa personne, étant entendu que toute faute constatée pourra être sanctionnée selon l'article 7.

### **3. UTILISATIONS DU RÉSEAU**

#### **3.1. UTILISATION CONFORME**

Le réseau HealthNet est mis à disposition des Établissements de santé et des Utilisateurs par l'Agence eSanté pour les seuls besoins de l'exercice de leur activité professionnelle, incluant notamment l'échange de données de santé.

L'utilisation du réseau HealthNet est présumée conforme lorsqu'elle est réalisée dans le respect des dispositions légales applicables à leur activité, de la présente charte et des politiques de sécurité applicables dans son Établissement de santé ainsi que le cas échéant des instructions techniques et spécifiques associées à chaque Moyen informatique concerné.

#### **3.2. UTILISATION TOLEREE**

Le réseau HealthNet peut être utilisé à des fins privées par les Utilisateurs dans les limites du raisonnable, dès lors que son utilisation ne vient pas en violation de la présente charte ainsi que des règles de sécurité et de confidentialité qui lui sont applicables, et que cela n'entrave pas le bon fonctionnement du réseau HealthNet et des Moyens informatiques qui y sont connectés.

Le non-respect du cadre de l'utilisation tolérée mentionné ci-dessus, et notamment toute utilisation au-delà du raisonnable, sera qualifié d'utilisation prohibée.

Il est précisé également que cette tolérance pourra être remise en cause à tout moment par l'Agence eSanté aux fins d'assurer la confidentialité, intégrité et sécurité des informations, ainsi qu'atteindre le niveau de sécurité exigé pour le système d'information connecté au réseau. La décision prendra effet après notification préalable aux Utilisateurs, sauf en cas d'incident majeur de sécurité où elle sera d'application immédiate.

#### **3.3. UTILISATIONS PROHIBEES**

Est prohibée toute utilisation du réseau HealthNet qui ne répondrait pas à la qualité d'utilisation conforme ou tolérée, telle que définie ci-dessus. L'identification d'une utilisation prohibée par un Utilisateur entraînera application des sanctions tel que disposé à l'article 7.

Également est prohibée toute utilisation du réseau HealthNet qui violerait toute disposition légale et réglementaire en vigueur, incluant notamment :

- le téléchargement, la consultation, la reproduction et la diffusion de tout contenu de nature à porter atteinte aux bonnes mœurs, à la dignité, à l'honneur, ou à la vie privée des personnes (incluant notamment contenu obscène, pornographique, portant apologie de la violence, du terrorisme ...), ainsi que tout contenu portant atteinte aux droits de propriété intellectuelle et actifs intellectuels de tiers ;

- l'envoi en masse de mails non sollicités, de messages publicitaires qui n'ont pas de liens avec l'activité professionnelle de l'Utilisateur ;
- la pénétration non autorisée et le maintien dans un Moyen informatique, l'utilisation ou la tentative d'utiliser le compte d'un tiers, ainsi que toute manœuvre qui viserait à accéder aux moyens informatiques sous une fausse identité ou en masquant l'identité véritable de l'utilisateur ; et
- le traitement de données à caractère personnel en violation de la loi modifiée du 2 août 2002 relative à la protection des données, et notamment contrairement aux finalités des traitements notifiés ou autorisés, et contrairement aux instructions du responsable de traitement (cf. article 6 ci-après).

## **4. MODALITÉS D'UTILISATION DES MOYENS INFORMATIQUES**

### **4.1. LE POSTE DE TRAVAIL, LES EQUIPEMENTS NOMADES ET LOGICIELS**

Les Utilisateurs sont tenus de respecter tout Moyen informatique et logiciel qui leur sont attribués aux fins de réalisation de leur fonction. Dans ce cadre ils s'engagent à :

- prendre les mesures nécessaires pour empêcher tout vol, perte, ou dégradation, notamment les conserver sur soi en déplacement, ou les laisser à l'abri des regards ; et
- ne pas transporter les équipements nomades avec eux lorsque cela n'est pas nécessaire pour la bonne réalisation de leur fonction et mission.

Les Utilisateurs reconnaissent qu'ils ne sont pas autorisés, sauf mention contraire présente au sein d'une procédure, guide d'utilisation ou instruction écrite, à :

- modifier les paramétrages des Moyens informatiques qui leur sont attribués et des environnements applicatifs, matériels et périphériques auxquels ils ont un droit d'accès (ex par suppression ou ajout de composants logiciels ou matériels), les Utilisateurs eSanté peuvent toutefois personnaliser leur configuration d'utilisation d'un logiciel lorsque ce dernier le permet ;
- télécharger, installer, copier, modifier dont l'utilisation n'a pas été approuvée par son établissement ;
- supprimer ou désinstaller des logiciels sans autorisation de l'établissement ;
- récupérer des fichiers auprès de sources inadéquates qui présentent le risque d'introduire des virus, des logiciels piratés ou sans licence (jeux, économiseurs d'écran, exécutables) ;
- utiliser ou essayer d'utiliser des comptes, ou téléphones mis à disposition d'autres Utilisateurs ;
- d'utiliser des moyens permettant de masquer sa véritable identité ; et
- relier un équipement informatique non connu dans l'établissement et/ou dont l'intégrité ou le niveau de sécurité n'est pas adéquat.

Les Utilisateurs qui constatent une perte, dégradation ou un dysfonctionnement d'un de leur équipement doivent, dans les plus brefs délais, informer leur Service Informatique.

## 4.2. INTERNET

L'utilisation des réseaux internet par les Utilisateurs via le réseau HealthNet est présumée être réalisée dans le cadre professionnel pour la réalisation de son activité professionnelle.

Dans ce cadre :

- seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle et tout accès à des sites à des fins privées est toléré dans le cadre des articles 3.2. et 3.3 ci-dessus ;
- l'Utilisateur est responsable de la navigation qu'il effectue sur internet, consultation et/ou de toute publication d'information et s'interdit dans ce cadre tout accès et/ou publication de contenu pouvant porter atteinte à son Établissement de santé, au réseau HealthNet, à l'Agence eSanté et à des tiers en application des articles 1.6 et 3.3 ci-dessus.

L'Utilisateur est informé que tout accès à internet depuis le réseau HealthNet est fait par l'intermédiaire d'un proxy et que, dans ce cadre, un blocage technique pour l'accès aux sites dont le contenu est connu<sup>2</sup> comme pouvant porter atteinte à la sécurité du réseau HealthNet et des Moyens informatiques.

L'Utilisateur est invité à alerter le ServiceDesk si l'accès à un site présentant un contenu dangereux<sup>3</sup> n'est pas bloqué. Également l'Utilisateur est invité à demander auprès du ServiceDesk l'autorisation d'accès à un site bloqué par défaut, selon la règle ci-dessus, sur présentation de justification permettant de qualifier le site concerné de sûr.

## 5. PROTECTION DES DONNÉES PERSONNELLES

### 5.1. UTILISATEURS RESEAU HEALTHNET

L'Agence eSanté, en qualité de responsable du traitement, collecte et traite les données à caractère personnel des Utilisateurs du réseau HealthNet aux fins d'administrer, gérer le réseau HealthNet incluant l'identification et la gestion des utilisateurs du réseau HealthNet, conformément à la loi modifiée du 2 août 2002 relative à la protection des données.

Les données sont collectées auprès des Utilisateurs par l'intermédiaire du formulaire de demande de connexion au réseau HealthNet (voir Annexe). Après signature de ce dernier par la personne concernée et concernant les données d'identification demandées au sein du formulaire, celles relatives à leur profession et lieu d'exercice, ainsi que les données d'identification électroniques associées aux moyens de connexion attribués.

Les données sont traitées par l'Agence aux fins, d'administrer et gérer le réseau HealthNet incluant notamment :

---

<sup>2</sup> Identification des sites qualifiés au sein de bases de données externes (veille et monitoring en matière de sécurité de l'information) de dangereux car source de spams, ransomware, attaques en déni de service, transmission virus et malware ...

<sup>3</sup> Id.

- attribuer, modifier ou supprimer les droits d'accès au réseau HealthNet, incluant la gestion des moyens de connexion,
- attribuer, modifier ou supprimer les droits d'accès au(x) service(s) demandé(s) par l'Utilisateur,
- journaliser les traces techniques des accès au réseau HealthNet et ses services.

L'Agence eSanté utilisera également les données anonymisées pour la réalisation de statistiques aux fins de suivi de l'utilisation et de la performance du réseau HealthNet.

Les données sont traitées au sein du réseau HealthNet, dont la gestion opérationnelle a été sous-traitée auprès de la société POST établie au Luxembourg. Les données sont hébergées au sein d'un datacentre Tier 3 au G-D du Luxembourg. POST est engagée auprès de l'Agence eSanté au respect de la confidentialité de toutes données et informations qu'elle serait amenée à traiter dans le cadre de sa mission.

Conformément à la finalité du traitement, les données traitées sont accessibles exclusivement :

- par le personnel de l'Agence eSanté et de son sous-traitant POST en charge de l'administration et la gestion du réseau HealthNet,
- par les responsables de la sécurité informatique des établissements de santé, uniquement sur demande de leur part dans le cadre de la gestion des utilisateurs des services sous leur responsabilité, ainsi que l'inventaire des connexions utilisateurs de leur système au réseau HealthNet.

Les données collectées, requises pour assurer la mise en place des services demandés et la facturation de ces services, sont transmises auprès de POST exclusivement pour les finalités mentionnées, à l'exclusion de toute autre utilisation.

L'Agence eSanté s'engage à ne procéder à aucune communication ni transfert des données traitées d'une part en dehors de l'Union Européenne et d'autre part auprès d'un destinataire tiers non mentionné ci-dessus sans consentement de l'utilisateur. En cas de changement de lieu d'hébergement des données, une information sera communiquée à l'Utilisateur.

Les données collectées sont conservées tant que le compte est actif, et 6 mois au terme de sa désactivation (cf. art 8 de la présente charte) pour assurer la gestion et administration du réseau HealthNet. Il est précisé à ce titre :

Les traces techniques, de types logs des Utilisateurs sont conservées pendant une durée maximale de 6 mois.

L'Agence eSanté prend, conformément à la loi modifiée du 2 août 2002 modifiée, les mesures nécessaires pour assurer la sécurité et confidentialité des données traitées, et notamment :

- empêcher toute divulgation non autorisée des données,
- assurer la disponibilité des données et leur intégrité, notamment par un système de sauvegardes,
- traiter tout incident pour limiter et si possible éviter les impacts sur les données et l'utilisateur.

Dans le respect de la loi modifiée du 2 août 2002, l'Utilisateur peut exercer ses droits auprès de l'Agence eSanté, comme suit :

- droit de consultation et d'accès : par demande auprès du chargé de protection des données désigné par l'Agence par email à l'adresse [privacy@esante.lu](mailto:privacy@esante.lu),
- droit de rectification : par transmission d'un formulaire de demande incluant les nouvelles données auprès du ServiceDesk, et escalade par email à l'adresse [privacy@esante.lu](mailto:privacy@esante.lu),
- droit d'opposition : en demandant la résiliation de son compte par l'utilisation du formulaire de demande, le traitement des données étant requis pour se connecter et utiliser le réseau HealthNet,
- toute information complémentaire concernant le traitement des données peut être demandée auprès du chargé de protection des données désigné par l'Agence par email à l'adresse [privacy@esante.lu](mailto:privacy@esante.lu).

Un accusé de bonne réception de la demande sera émis, et toutes les données échangées dans ce cadre seront protégées au titre de la correspondance privée.

## 5.2. UTILISATION DES SERVICES DU RESEAU HEALTHNET

Dans le cadre de l'utilisation du réseau HealthNet, l'Utilisateur peut être amené à échanger, partager ou traiter des données à caractère personnel. Il appartient à chaque Utilisateur de s'assurer qu'il agit dans ce cadre en conformité des finalités du service qu'il utilise ainsi que dans le respect des droits de la personne concernée.

L'Agence eSanté n'est responsable que des traitements réalisés dans le cadre des services listés au sein du manuel.

Les autres services accessibles au sein du réseau HealthNet sont sous la responsabilité des Établissements de santé qui les exploitent.

A ce titre chaque Établissement de santé concerné se doit :

- d'informer les Utilisateurs et personnes concernées des finalités et modalités du traitement de données réalisé, ainsi que des conditions d'exercice de leurs droits ; et
- de prendre les actions requises pour le respect des droits des personnes physiques à la protection de leurs données et de leur vie privée conformément à la loi modifiée du 2 août 2002 relative à la protection des données.

L'Agence pourra demander l'arrêt du service en cas de non-respect avéré par l'Établissement de santé de la loi susmentionnée.

## 6. CONTRÔLE DU RÉSEAU HEALTHNET

### 6.1. MESURES EN PLACE

L'Agence eSanté, exploitant du réseau HealthNet, a mis en place différents systèmes de sécurité, tels que pare-feu, filtre d'email entrant, proxy, sans que cette liste ne soit exhaustive.

Il est précisé que les mesures mises en place ne collectent et analysent que les informations systèmes, de réseau et d'application à l'exclusion de toute collecte et analyse de contenu de documents et/ou messages.

Les informations collectées sont centralisées afin de permettre l'émission d'alertes, selon des indicateurs et seuils configurés, ainsi que de tableaux de bords et de rapports auprès des personnes en charge de la sécurité du réseau HealthNet.

## 6.2. TRAITEMENT DES INCIDENTS

Lors de la réception d'une notification de sécurité par le Service Desk, les personnes en charge de la sécurité et de la gestion du réseau HealthNet, de l'Agence eSanté et de POST conjointement :

- prennent directement les actions requises pour traiter la notification, lorsque le traitement ne requiert pas d'intervention sur le Moyen informatique de l'Utilisateur ;
- prennent contact avec l'Établissement ou l'Utilisateur (cf. manuel d'utilisation) pour l'informer de la nécessité des actions à réaliser pour le traitement de la notification reçue ; et
- informent l'Utilisateur de tout changement d'instructions, règles d'accès et/ou utilisation aux fins de traitement de la notification de sécurité.

Toutefois en cas d'urgence l'Agence eSanté, le cas échéant avec la coopération de l'Établissement de santé, peut de manière temporaire pour protéger le réseau HealthNet et les Moyens informatiques qui y sont connectés, après notification aux personnes sus mentionnées :

- déconnecter un Utilisateur, avec ou sans préavis selon la gravité de la situation;
- isoler ou neutraliser provisoirement tout Moyen informatique qui manifestement mettrait en péril la sécurité du réseau HealthNet.

En cas de besoin, l'Agence eSanté pourra recourir aux services de CERTs publics ou privés pour l'assister dans le traitement d'incidents.

## 7. VIOLATION ET SANCTION

### 7.1. IDENTIFICATION DE LA VIOLATION ET MESURES DE PROTECTION

A réception d'une notification ou alerte de sécurité, l'Agence eSanté prend les mesures et actions nécessaires pour traiter l'incident identifié et assurer la sécurité du réseau HealthNet. L'Agence eSanté dans ce cadre pourra procéder à des investigations techniques pour déterminer notamment la source et l'impact de l'incident

Il pourra être demandé la coopération de l'Établissement de santé concerné.

Lorsque le traitement de l'incident requiert une investigation de l'activité de l'Utilisateur ou des Utilisateurs concernés au sein du réseau HealthNet, l'Utilisateur(s) concerné(s), le cas échéant avec la coopération de l'Établissement de santé, sera(ont) informé(s) préalablement à la réalisation de l'investigation.

Lorsqu'il est constaté, soit de manière évidente, soit au terme d'une investigation une violation de la présente charte n'ayant causé aucun dommage auprès du réseau HealthNet, il est rappelé auprès de l'Utilisation les bonnes pratiques, règles et instructions d'utilisation du réseau HealthNet, et de la présente charte informatique.

Il est précisé cependant que l'article 7.3 ci-après pourrait venir s'appliquer en présence de violations répétées qualifiées de mineures, ou n'ayant pas entraîné de dommage.



## **7.2. SANCTIONS**

Lorsqu'il est constaté, soit de manière évidente, soit au terme d'une investigation une violation de la présente charte par l'Utilisateur, ayant entraîné un dommage auprès du réseau HealthNet ou de tiers, ou une violation correspondant à une faute professionnelle ou négligence caractérisée de l'Utilisateur, l'Établissement de santé ou l'Agence eSanté pourra résilier l'accès de cet Utilisateur au réseau.

## **7.3. AUTRES SANCTIONS**

L'Utilisateur pourra voir sa responsabilité civile ou pénale engagée pour toute violation de dispositions légales lors de l'utilisation du réseau HealthNet, outre la résiliation de l'accès au réseau HealthNet.

L'Agence eSanté pourra selon le cas engager la responsabilité civile et/ou pénale de l'Établissement de santé pour le compte duquel l'Utilisateur est intervenu.

Il est précisé que l'Agence eSanté suivra les étapes d'information et notification auprès de l'Utilisateur comme mentionnée précédemment avant l'engagement de toute action à l'encontre de l'Utilisateur et/ou de l'Établissement de santé pour le compte duquel il intervient.

## **8. FINS D'ACCÈS AU RÉSEAU**

L'accès réseau HealthNet prend fin lors de la résiliation des accès au réseau HealthNet via le formulaire disponible sur le site [www.healthnet.lu](http://www.healthnet.lu). La résiliation requiert la restitution par l'Utilisateur du moyen d'authentification au réseau (token, carte magnétique, clefs de chiffrement ...).

L'absence de renouvellement du moyen d'authentification de l'Utilisateur au réseau HealthNet, par l'absence de paiement de l'Utilisateur ou de l'établissement, vaut résiliation de l'accès.

**Pour l'Utilisateur**, je soussigné(e), \_\_\_\_\_, déclare

- avoir lu, accepter et m'engager au respect de la Charte Informatique HealthNet régissant les modalités d'accès et l'utilisation du réseau HealthNet (voir <http://www.healthnet.lu>),
- avoir lu et compris que mes données à caractère personnel sont traitées par l'Agence eSanté aux fins d'attribution et gestion de l'accès au réseau HealthNet et à ses services, selon les modalités décrites au sein de la Charte informatique HealthNet et conformément à la loi modifiée du 02/08/2002.

Signature de l'Utilisateur :

Lieu et date :

## Ou

**Pour l'institution**, la présente signature vaut acceptation et engagement de respect sans réserve de la Charte informatique HealthNet régissant les modalités d'accès et l'utilisation du réseau HealthNet

Signataire (nom, qualité):

Signature :

Lieu et date

Cachet :

*En présence d'Utilisateur non inclus au sein de l'effectif d'un Établissement de Santé, la présente charte doit être également visée par un représentant habilité de la personne morale pour le compte de qui l'Utilisateur intervient.*



## 9. ANNEXES

### 9.1. REFERENCES INTERNES

Accessibles sur : <https://www.healthnet.lu>

### 9.2. REFERENCES LEGALES

- Loi modifiée du 2 août 2002 relative à la protection des données  
<https://cnpd.public.lu/fr/legislation/droit-lux/index.html>
- Articles 509-1 à 509-7 du code pénal « de certaines infractions en matière informatique »  
[http://www.legilux.public.lu/leg/textescoordonnes/codes/code\\_penal/](http://www.legilux.public.lu/leg/textescoordonnes/codes/code_penal/)
- Loi de 19 juin 2013 relative à l'identification des personnes physiques.