

HealthNet Luxembourg

Politique de sécurité

version 1.0

Octobre 2007

G.I.E. – HealthNet
R.C. Luxembourg N° C69
Siège Social:
Villa Louvigny – Allée Marconi
L-2120 Luxembourg



2A rue Kalchesbrück
L-1852 Luxembourg

HISTORIQUE DU DOCUMENT

Version	Initiative	Objet	Date	Auteur
1.0	GIE	Version française	03.05.07	PPI

TABLE DES MATIERES

1	OBJECTIF	4
2	CONTACTS	5
3	POLITIQUE GÉNÉRALE	6
3.1	<u>GESTION DE LA SÉCURITÉ</u>	6
3.2	<u>PROTECTION DES DONNÉES</u>	6
3.3	<u>CENSURE DES DONNÉES</u>	6
3.4	<u>CONFIDENTIALITÉ DES DONNÉES</u>	6
3.5	<u>CONTRÔLE PRIVILÉGIÉ</u>	7
3.6	<u>DROITS DE PROPRIÉTÉ INTELLECTUELLE</u>	7
3.7	<u>GARANTIE DE SÉCURITÉ/AUDIT</u>	7
3.8	<u>RESPONSABILITÉS</u>	8
4	ACCÈS INDIVIDUEL	9
4.1	<u>ACCÈS À HEALTHNET</u>	10
4.1.1	<u>ISDN</u>	10
4.1.2	<u>Secure Connect/SSL-VPN</u>	10
4.1.3	<u>VPN</u>	10
4.2	<u>CONNECTIVITÉ À L'INTERNET</u>	10
4.3	<u>COMMUNICATION SÉCURISÉE</u>	10
4.4	<u>VIRUS</u>	11
4.5	<u>SPAM</u>	11
4.6	<u>CONTRÔLE DES PRIVILÈGES</u>	11
5	ACCÈS RÉSEAU	12
5.1	<u>RESPONSABILITÉ</u>	12
5.2	<u>ACCÈS PHYSIQUE</u>	12
5.3	<u>ACCÈS À HEALTHNET</u>	12
5.3.1	<u>ISDN</u>	12
5.3.2	<u>Secure Connect / SSL-VPN</u>	12
5.3.3	<u>VPN</u>	13
5.4	<u>COMMUNICATION SÉCURISÉE</u>	13
5.5	<u>CONNECTIVITÉ À L'INTERNET</u>	13
5.6	<u>COURRIER ÉLECTRONIQUE</u>	14
5.7	<u>VIRUS</u>	14
5.8	<u>SPAM</u>	14
6	LABO	15
6.1	<u>EXIGENCES DE SÉCURITÉ</u>	15
6.1.1	<u>Exigences de sécurité de la CA</u>	15
6.1.2	<u>Exigences de sécurité des utilisateurs</u>	16
6.1.3	<u>Règles de certification</u>	16
6.1.3.1	<u>Enregistrement</u>	16
6.1.3.2	<u>Génération des clés</u>	16
6.1.3.3	<u>Mise à jour/prolongation</u>	16
6.1.3.4	<u>Suppression</u>	17
6.1.3.5	<u>Publication des clés</u>	17
7	GLOSSAIRE	18

1 Objectif

Pendant les dernières années, HealthNet Luxembourg est devenu un élément important du système des soins de santé luxembourgeois. Tous les hôpitaux, plus de 200 médecins indépendants ainsi que beaucoup de laboratoires et entreprises externes utilisent cette plateforme quotidiennement. Il est donc évident que tous les services doivent être fiables et que la confidentialité des données doit être assurée.

Par conséquent, toutes les informations doivent être protégées, proportionnellement à leur sensibilité, valeur et criticité. Des mesures de sécurité doivent être réalisées indépendamment des médias sur lesquels les informations sont stockées, respectivement transférées. Le G.I.E. – HealthNet, en coopération avec l'Entreprise des Postes et Télécommunications (EPT), doit s'assurer que les informations et les systèmes d'information sont protégés au moins de la même manière que ceux d'autres organismes gérant le même type d'information. Pour atteindre cet objectif, des revues annuelles des risques et de la sécurité relatives à HealthNet et aux systèmes d'information seront conduites.

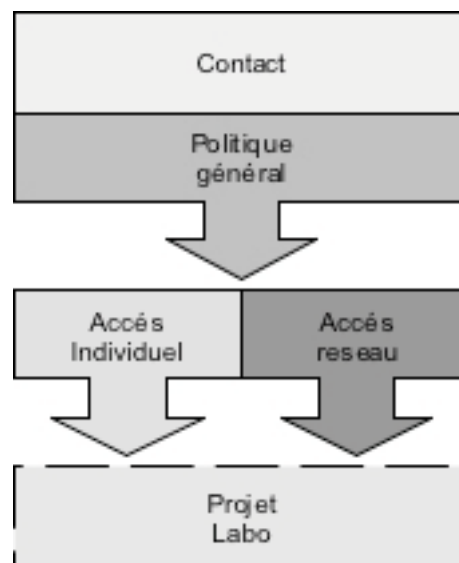
Le G.I.E. – HealthNet, en tant que propriétaire de HealthNet Luxembourg, entreprendra toutes les étapes nécessaires vers une infrastructure fiable et sécurisée. Une de ces étapes est la définition et la mise en place d'une politique de sécurité efficace. Pour cette raison, chaque participant de HealthNet Luxembourg doit accepter les directives suivantes.

Comment lire ce document

Le document est divisé en 5 parties :

- information de contact
- politique générale
- suppléments pour un accès individuel
- suppléments pour un accès réseau
- suppléments pour l'application Labo

Toute personne/organisation intéressée doit lire et comprendre la politique générale, plus l'accès individuel ou l'accès de réseau (selon la méthode d'accès). Si vous souhaitez participer au projet Labo, veuillez également lire le chapitre intitulé « projet Labo ».



L'accès individuel et l'accès réseau se différencient par la quantité d'utilisateurs qui veulent se connecter ainsi que par les conditions et besoins d'utilisation. Pour connecter un ordinateur individuel à HealthNet Luxembourg, les règles définies dans le chapitre « Accès individuel » seront appliquées et en cas de connexion de plusieurs ordinateurs (habituellement un réseau), le chapitre « Accès réseau » devra être appliqué.

2 Contacts

Contact administratif:

G.I.E.-HealthNet
R.C. Luxembourg N° C69
Siège Social:
Villa Louvigny – Allée Marconi
L-2120 Luxembourg
E-mail: info@gie.HealthNet.lu
Site Internet : www.HealthNet.lu

Contact technique:

HealthNet Helpdesk
Tél. : 4991-5080
Fax : 2660-5080
E-mail : servicedesk@HealthNet.lu (support général)
incident.servicedesk@HealthNet.lu (en cas d'incident)
change.service@HealthNet.lu (création, modification d'un service)

Projet Labo

Identité de l'Autorité de Certification

Centre de Recherche Public Henri Tudor - SANTEC
2A rue Kalchesbrück
L-1852 Luxembourg
Tél. : +352 42 59 91 – 250
Fax: +352 42 59 91 – 251

E-mail: ca@HealthNet.lu (questions sur la certification)
labo@HealthNet.lu (questions générales)

Pour plus d'information, veuillez consulter: www.HealthNet.lu/applications/lab/

3 Politique générale

3.1 Gestion de la sécurité

- Chaque utilisateur/organisation doit comprendre les politiques et les procédures de HealthNet relatives à la sécurité des données et doit fournir son consentement écrit quant à son adhérence à ces politiques et procédures.
- La politique de sécurité de HealthNet Luxembourg sera revue chaque année.
- Cette politique de sécurité peut être modifiée sans préavis. En cas de changements, une notification sera envoyée à chaque participant de HealthNet par courrier et/ou par e-mail. La nouvelle version sera appliquée dès son édition sur le site Internet de HealthNet.
- Le G.I.E.-HealthNet a le droit de refuser tout accès à l'utilisateur ou à l'organisation en cas de violations en relation avec cette politique de sécurité.
- Le G.I.E.-HealthNet décline toute responsabilité en cas de perte de données, de dommages aux données ou de dommages aux logiciels qui résulteraient de manipulations et/ou efforts des utilisateurs en vue de répondre aux objectifs fixés dans la politique de sécurité, y compris de futures modifications de ladite politique.
- Par sa signature de cette politique de sécurité, l'utilisateur ou le responsable de l'organisation accepte que ses données personnelles (nom, adresse et le cas échéant le code UCM) soient vérifiées par l'Union des Caisses de Maladie (UCM) comme preuve d'autorité.

3.2 Protection des données

- Le G.I.E.-HealthNet et/ou ses sous-traitants auront le droit de surveiller toutes les activités système et le trafic de réseau (e-mail compris) d'un utilisateur pour imposer les dispositions de cette politique. Ceci peut inclure des données personnelles en cas de soupçon justifié d'une utilisation frauduleuse de l'infrastructure de HealthNet.

3.3 Censure des données

- HealthNet se réserve le droit d'enlever des ordinateurs, respectivement du réseau, Healthnet toute donnée estimée illégale ou inadéquate.

3.4 Confidentialité des données

- Les données personnelles stockées dans un système de courrier électronique, les dossiers personnels, etc. peuvent être examinées seulement en cas d'obligation légale ou de permission explicite de l'utilisateur.

- Le tirage ou l'impression de copies supplémentaires contenant de l'information secrète, confidentielle ou privée ne doit pas être effectuée sans autorisation préalable du propriétaire de l'information.
- Des informations confidentielles doivent uniquement être révélées en cas d'autorisation légale ou après obtention de la permission explicite du propriétaire de l'information. L'accord accordé à un individu d'accéder à des informations secrètes, n'implique pas la permission de les révéler à des tiers.
- Les utilisateurs n'ont pas le droit de naviguer dans les systèmes informatiques ou les réseaux de HealthNet. Par exemple, la recherche par curiosité de dossiers ou programmes intéressants dans les fichiers des autres utilisateurs est interdite. Les mesures prises pour localiser légitimement l'information nécessaire à l'exécution de son travail ne sont pas considérées comme recherche abusive.
- En cas d'utilisation d'un système d'encryption, les clés employées doivent être générées par des moyens dans la pratique non-reproductibles par un adversaire et produisant des clés difficiles à deviner.
- Toutes les clés de chiffage ont une vie **maximale** de 5 ans et doivent être changées à ou avant la date d'échéance indiquée.

3.5 Contrôle privilégié

- Toute information d'un compte d'utilisateur (y compris des fichiers du home directory) peut être effacée après une période minimale de trois (3) mois après le départ définitif de l'utilisateur.
- Les utilisateurs ne sont pas autorisés à utiliser un compte e-mail d'autrui pour l'envoi ou la réception de messages. En cas de nécessité de suivre le courrier d'un utilisateur absent, il faudra utiliser d'autres moyens comme le forward de messages.

3.6 Droits de propriété intellectuelle

- Le G.I.E.-HealthNet adhère strictement au respect des contrats de licence des fournisseurs de logiciels et des copyrights. En cas de réalisation de copies non autorisées, les utilisateurs d'Internet ou d'autres systèmes informatiques doivent en assumer la responsabilité personnellement.

3.7 Garantie de sécurité/audit

- Le G.I.E.-HealthNet peut désigner des administrateurs de réseau chargés de tester les contrôles d'accès ou autorisés à examiner le réseau sur d'autres vulnérabilités. Les utilisateurs ne sont pas autorisés à effectuer des recherches de vulnérabilité et/ou 'à essayer d'obtenir accès manuellement ou en utilisant des programmes installés.

- HealthNet utilise des contrôles d'accès et d'autres mesures de sécurité afin de protéger la confidentialité, l'intégrité et la disponibilité des données gérées par les ordinateurs et les systèmes de communication. En accord avec ces objectifs, le G.I.E.-HealthNet et/ou ses sous-traitants sont autorisés à prendre toute mesure nécessaire à la gestion et à la protection de ses systèmes d'information.
- En cas de détection de vulnérabilités, les utilisateurs ne sont pas autorisés à profiter de celles-ci manuellement ou en utilisant des programmes installés.
- Le G.I.E.-HealthNet et les administrateurs qui ont été désignés auront accès aux outils de contrôle de la sécurité informatique. Aucun autre utilisateur ne doit avoir accès à ces outils.
- Sans autorisation préalable du G.I.E. – HealthNet, les utilisateurs/entreprises ne sont pas autorisés à établir des connexions vers Internet ou des réseaux externes, qui pourraient permettre ou faciliter un accès non-autorisé aux systèmes et informations d'HealthNet à des utilisateurs étrangers à HealthNet.
- En général, tous les internautes doivent être conscients que les firewalls, systèmes anti-intrusion (Intrusion Detection Systems, IDS) et d'autres logiciels de sécurité génèrent un rapport détaillé contenant toute demande de service entrant et sortant.

Pour s'assurer que les utilisateurs puissent être tenus responsables de leurs actions dans le réseau HealthNet, le G.I.E. – HealthNet et/ou ses sous-traitants utiliseront un ou plusieurs systèmes d'enregistrement de données pendant un laps de temps raisonnable. Ces enregistrements sont soumis aux lois sur la confidentialité et le stockage des données.

3.8 Responsabilités

- Les ordinateurs et les systèmes de communication HealthNet sont strictement destinés à l'usage professionnel.
- Les abonnés aux services de communication de HealthNet ne sont pas autorisés à utiliser ces ressources pour des sollicitations commerciales, la vente de produits ou tout autre engagement dans des activités commerciales autres que celles expressément autorisées par le G.I.E. – HealthNet.
- Tout soupçon d'incidents concernant la sécurité des informations doit être reporté le plus rapidement possible par les voies prévues (*voir chapitre 2 – Contacts*).
- La responsabilité de la sécurité quotidienne des informations fait partie des devoirs de chaque utilisateur. La responsabilité explicite de la sécurité informatique n'est pas exclusivement attribuée aux employés de HealthNet.
- Les utilisateurs doivent informer immédiatement le G.I.E. – HealthNet et/ou ses sous-traitants de toute circonstance pouvant mener à des interruptions d'activité.

- Les utilisateurs sont responsables pour toute activité effectuée avec leur user-IDs personnels. Les user-IDs doivent être utilisés exclusivement par les personnes/groupes à qui ils ont été attribués. Les utilisateurs ne sont pas autorisés à permettre à des tiers d'exécuter des activités avec leur user-IDs. De même, les utilisateurs ne doivent pas non plus utiliser des user-IDs appartenant à d'autres personnes (excepté les user-IDs anonymes comme « guest »).
- Quelque soient les circonstances, les mots de passe ne doivent jamais être partagés ou communiqués à des personnes autres que l'utilisateur autorisé. Les personnes/groupes à qui un nom d'utilisateur et un mot de passe ont été attribués seront tenus responsables vis-à-vis du G.I.E. – HealthNet et des utilisateurs du réseau, pour toute action effectuée par une personne non-autorisée sauf s'ils peuvent prouver qu'ils n'étaient pas en mesure d'empêcher cet usage abusif et qu'il s'est produit sans leur faute. Si les utilisateurs doivent partager des données informatiques internes, ils devraient utiliser le courrier électronique, des répertoires publics sur des serveurs du réseau local ou d'autres mécanismes.
- Tout changement d'adresse d'un utilisateur/groupe doit être communiqué immédiatement. Si des essais de contact échouent, le compte de l'utilisateur/de l'organisation sera suspendu au bout de 3 mois et effacé après 6 mois.
- Les utilisateurs/sociétés concernés seront préalablement informés des interventions de maintenance ayant des répercussions sur l'utilisation de HealthNet.

4 Accès individuel

Les règles du présent chapitre sont applicables pour chaque utilisateur connecté individuellement à HealthNet Luxembourg via un PC ou un notebook.

4.1 Accès à HealthNet

HealthNet Luxembourg supporte plusieurs possibilités sécurisées d'accès au réseau :

- ISDN
- Secure Connect
- SSL-VPN

4.1.1 ISDN

- Le mot de passe initial provenant d'un administrateur sécurité sera valide pendant la période d'existence du compte. Des modifications de mots de passe peuvent avoir lieu, mais seulement via l'administrateur sécurité.

4.1.2 Secure Connect/SSL-VPN

- De nouvelles connexions à distance seront créées par défaut avec les solutions « Secure Connect » ou « SSL-VPN » de l'EPT (*Entreprise des Postes et Télécommunications*). Ces solutions ont l'avantage d'être entièrement intégrées dans HealthNet, fournissant ainsi la meilleure sécurité et la meilleure maintenance possibles pour les participants de HealthNet.

4.1.3 VPN

- Les connexions VPN SecuRemote existantes seront terminées et ne seront installés uniquement que dans des cas exceptionnels, qui devront être motivés par écrit par la personne et/ou la société demandant la connexion VPN.

4.2 Connectivité à l'Internet

- Les services supportés par la passerelle à Internet seront définis par un comité chargé de vérifier la nécessité de permettre les services selon les besoins relatifs à l'activité des demandeurs.
- Le G.I.E.-HealthNet se réserve le droit de bloquer l'accès à tout site ou service considéré inadéquat.
- Afin d'éviter les « back-doors », les utilisateurs n'ont pas le droit de connecter des postes de travail à d'autres réseaux en même temps qu'à HealthNet.
- Les sites Internet non autorisés par le G.I.E.-Healthnet n'ont pas le droit de commercialiser des produits ou des services propres à HealthNet.

4.3 Communication sécurisée

- Tout ordinateur de HealthNet pouvant communiquer avec un réseau d'une tierce partie (lignes dial-up, réseaux à valeur ajoutée, l'Internet, etc.) doit être protégé par un système de contrôle des accès et des privilèges approuvé par G.I.E.-HealthNet et/ou ses sous-traitants.

- Sauf approbation préalable de G.I.E.-HealthNet, les utilisateurs ne sont pas autorisés à établir de connexions Internet ou réseau additionnelles qui pourraient permettre à des utilisateurs externes d'accéder aux systèmes informatiques de HealthNet.
- Afin de pouvoir accéder au réseau informatique HealthNet, toute tierce partie devra sécuriser ses propres systèmes connectés en respectant les exigences HealthNet. Le G.I.E.-HealthNet et/ou ses sous-traitants se réservent le droit d'auditer les mesures de sécurité appliquées sur ces systèmes connectés sans avertissement préalable. Le G.I.E.- HealthNet et/ou ses sous-traitants se réservent également le droit de fermer immédiatement des connexions réseau avec tout système tiers ne respectant pas de telles exigences.

4.4 Virus

- Afin d'empêcher la diffusion de virus, de vers informatiques (Worms) et de chevaux de Troie (Trojan Horses) à travers ses réseaux, tous les e-mail entrants seront scannés à la recherche de virus éventuels et marqués le cas échéant.
- En cas de réception de fichiers électroniques (logiciels, programmes, bases de données, documents issus d'un traitement de texte ou d'un tableur, etc.) de toute source externe, il sera obligatoire d'effectuer des contrôles anti-virus avant toute utilisation sur les systèmes informatiques de HealthNet. En cas de détection d'un virus, le personnel de HealthNet doit en être informé immédiatement (voir liste des contacts au chapitre 2) et tout travail qui pourrait endommager HealthNet Luxembourg devra être évité.
- Les utilisateurs ne doivent pas intentionnellement écrire, générer, compiler, copier, propager, exécuter ou essayer d'introduire des codes informatiques qui pourraient proliférer, endommager ou empêcher d'une autre façon la performance de toute mémoire d'ordinateur, système de fichiers ou logiciel. Ces logiciels sont connus sont le nom de virus, de vers informatiques (Worms) et de chevaux de Troie (Trojan Horses), etc.

4.5 SPAM

- HealthNet Luxembourg met à disposition des outils afin de réduire la quantité de mails SPAM et de mails non-sollicités. Par conséquent, deux moyens différents de traitement des SPAM sont proposés :
 - Marquage du mail
 - Pas de détection des SPAM

Tout participant peut choisir une solution.

4.6 Contrôle des privilèges

- Le G.I.E. HealthNet se réserve le droit d'annuler à tout moment les privilèges accordés à tout utilisateur en cas d'utilisation frauduleuse d'un nom d'utilisateur qui pourrait gêner le fonctionnement normal et approprié des systèmes HealthNet et affecter de manière négative l'utilisation des autres utilisateurs, ou en cas d'utilisation ayant pour but des dommages ou des attaques.

5 Accès réseau

Les règles du présent chapitre sont applicables par chaque utilisateur connecté à HealthNet Luxembourg via un réseau informatique personnel.

5.1 Responsabilité

- L'organisation/l'entreprise est tenue responsable des actions de ses utilisateurs et doit garantir l'adhérence à la présente politique de sécurité.
- Afin de pouvoir accéder au réseau informatique HealthNet, chaque tierce partie doit respecter les obligations détaillées dans la politique de sécurité HealthNet. Le G.I.E.-HealthNet et/ou ses sous-traitants se réservent le droit d'auditer les mesures de sécurité appliquées sur ces systèmes connectés sans avertissement préalable. Le G.I.E.-HealthNet et/ou ses sous-traitants se réservent également le droit de fermer immédiatement des connexions réseau avec tout système tiers ne respectant pas de telles exigences.

5.2 Accès physique

- L'EPT assure l'accès physique aux serveurs de HealthNet. En dehors des administrateurs désignés, uniquement des personnes sélectionnées par le G.I.E. – HealthNet (par exemple des administrateurs des serveurs hébergés) sont autorisées à accéder à la salle serveur. Après obtention du droit d'accès, un administrateur responsable accompagnera le visiteur pendant le temps de la visite.

5.3 Accès à HealthNet

HealthNet Luxembourg supporte plusieurs solutions d'accès sécurisées :

- Ligne louée
- IP-VPN
- ISDN
- Secure Connect
- SSL-VPN
- Lan-to-Lan VPN

5.3.1 ISDN

- Le mot de passe initial provenant d'un administrateur sécurité sera valide pendant la période d'existence du compte. Des modifications de mots de passe peuvent avoir lieu, mais seulement via l'administrateur sécurité.

5.3.2 Secure Connect / SSL-VPN

- De nouvelles connexions à distance seront créées par défaut avec les solutions « Secure Connect » ou « SSL-VPN » de l'EPT (*Entreprise des Postes et Télécommunications*). Ces solutions ont l'avantage d'être entièrement intégrées dans

HealthNet, fournissant ainsi la meilleure sécurité et la meilleure maintenance possibles pour les participants de HealthNet.

5.3.3 VPN

- Les connexions VPN SecuRemote existantes seront terminées et ne seront installées uniquement que dans des cas exceptionnels, qui devront être motivés par écrit par la personne et/ou la société demandant la connexion VPN.
- Des connexions VPN Lan-à-Lan peuvent être établies mais uniquement pour des raisons de maintenance ou d'autres raisons justifiées.

5.4 Communication sécurisée

- Tout ordinateur de HealthNet pouvant communiquer avec un réseau d'une tierce partie (lignes dial-up, réseaux à valeur ajoutée, l'Internet, etc.) doit être protégé par un système de contrôle des accès et des privilèges approuvé par G.I.E.-HealthNet et/ou ses sous-traitants.
- Afin de pouvoir accéder au réseau informatique HealthNet, toute tierce partie devra sécuriser ses propres systèmes connectés en respectant les exigences HealthNet. Le G.I.E.-HealthNet et/ou ses sous-traitants se réservent le droit d'auditer les mesures de sécurité appliquées sur ces systèmes connectés sans avertissement préalable. Le G.I.E.-HealthNet et/ou ses sous-traitants se réservent également le droit de fermer immédiatement des connexions réseau avec tout système tiers ne respectant pas de telles exigences.
- Sauf approbation préalable de G.I.E.-HealthNet, les utilisateurs ne sont pas autorisés à établir de connexions Internet ou réseau additionnelles qui pourraient permettre à des utilisateurs externes d'accéder aux systèmes informatiques de HealthNet.

5.5 Connectivité à l'Internet

- Les services supportés par la passerelle à Internet seront définis par un comité chargé de vérifier si ces services sont justifiés et que toutes les conditions nécessaires sont réunies (contrat, licence ...).
- Le G.I.E.-HealthNet se réserve le droit de bloquer l'accès à tout site ou service considéré inadéquat.
- Les utilisateurs n'ont pas le droit de connecter des modems dial-up à des postes de travail connectés simultanément au réseau local (LAN) ou à un autre réseau de transmission interne.
- Les utilisateurs ne sont pas autorisés à utiliser le compte e-mail assigné à quelqu'un d'autre pour l'envoi ou la réception de messages. En cas de nécessité de suivre le courrier d'un utilisateur absent, il faudra utiliser d'autres moyens comme le forward de messages.
- Bien que G.I.E.-HealthNet et/ou ses sous-traitants encouragent des sauvegardes périodiques des fichiers électroniques, toute correspondance interne devenue obsolète doit être supprimée. Les messages électroniques concernant des activités en cours, ou en voie de devenir pertinentes pour les activités en cours, devraient être sauvegardés comme fichiers séparés et conservés aussi longtemps que nécessaire.

- Tout usage personnel de courrier électronique ne devra ni engendrer des sollicitations, ni être associé à des activités commerciales extérieures en vue d'un profit et ne devra pas entraver les activités de HealthNet.
- Les sites Internet non autorisés par le G.I.E.-Healthnet n'ont pas le droit de commercialiser des produits ou des services propres à HealthNet.

5.6 Courrier électronique

- Afin de standardiser et de sécuriser le système de courrier électronique toute correspondance électronique vers l'extérieur doit passer soit par un serveur de mail EPT dédié, soit par un serveur de l'organisation qui doit être déclaré à l'EPT.

5.7 Virus

- Un logiciel anti-virus doit être installé et configuré sur toute passerelle de courrier électronique HealthNet afin d'assurer un contrôle permanent des virus.
- Un logiciel anti-virus doit être installé et configuré sur tout poste de travail.
- Afin d'empêcher la diffusion de virus, de vers informatiques (Worms) et de chevaux de Troie (Trojan Horses) à travers ses réseaux, tous les e-mail entrants seront scannés à la recherche de virus et marqués le cas échéant.
- En cas de réception de fichiers électroniques (logiciels, programmes, bases de données, documents issus d'un traitement de texte ou d'un tableur, etc.) de toute source externe, il sera obligatoire d'effectuer des contrôles anti-virus avant toute utilisation sur les systèmes informatiques de HealthNet. En cas de détection d'un virus, le personnel de HealthNet doit en être informé immédiatement (voir liste des contacts au chapitre 2) et toute utilisation de ce poste de travail doit être stoppée tant que le virus n'a pas été éradiqué.
- Les utilisateurs ne doivent pas intentionnellement écrire, générer, compiler, copier, propager, exécuter ou essayer d'introduire des codes informatiques qui pourraient proliférer, endommager ou empêcher d'une autre façon la performance de toute mémoire d'ordinateur, système de fichiers ou logiciel. Ces logiciels sont connus sont le nom de virus, de vers informatiques (Worms) et de chevaux de Troie (Trojan Horses) etc.

5.8 SPAM

- HealthNet Luxembourg met à disposition des outils afin de réduire la quantité de mails SPAM et de mails non-sollicités. Par conséquent, deux moyens différents de traitement des SPAM sont proposés :
 - Marquage du mail
 - Pas de détection des SPAM

Tout participant peut choisir une solution.

6 Labo

Le projet Labo a démarré le 1^{er} janvier 2003 avec comme but de fournir une infrastructure dans laquelle les laboratoires au Luxembourg et les médecins pourraient échanger des données de manière sécurisée via HealthNet. Une partie des activités dans ce projet du département Santec du Centre de Recherche Henri Tudor concerne la gestion d'une Autorité de Certification (Certification Authority, CA).

6.1 Exigences de sécurité

Pour participer à une infrastructure de clés publiques, chaque utilisateur doit remplir différentes conditions concernant la sécurité du matériel et du logiciel utilisés. Les exigences concernant la CA sont évidemment plus élevées, étant donné que l'usage abusif d'une clé de la CA compromettrait la fiabilité de toutes les clés subordonnées.

6.1.1 Exigences de sécurité de la CA

La CA doit remplir les critères suivants :

- Les services de la CA dépendent d'une machine sécurisée de façon appropriée. L'accès non autorisé au serveur CA doit être évité. En particulier, il faut veiller à ce que l'ordinateur n'ait pas d'accès au réseau et soit protégé physiquement.
- Les clés personnelles de la CA (utilisées comme signatures) doivent être protégées et ne pas être divulguées. Cette responsabilité est confiée aux administrateurs de la CA. Ainsi, afin de protéger les clés, ils doivent utiliser des procédures adéquates et des dispositifs périphériques. L'accès à ces clés doit être protégé par des mots de passe ayant au moins 8 caractères et connus uniquement par les administrateurs. En plus, les clés ne doivent pas être conservées en texte clair quelque part ou transmises par un réseau non sécurisé.
- Les clés des utilisateurs peuvent être signées ou certifiées uniquement avec la clé privée utilisée pour la signature de la CA. Ces clés ne doivent pas être utilisées pour la communication standard.
- Les paires de clés asymétriques de la CA doivent avoir une longueur minimale de 2048 Bit ; une longueur supérieure est recommandée.
- Si la CA crée des paires de clés asymétriques pour un utilisateur, la CA doit le faire à l'aide d'une machine spécialisée et sécurisée. Après le transfert de la clé à l'utilisateur, la CA ne doit en aucun cas conserver les clés privées (ou des parties) après la transmission de celles-ci.
- Toutes les données provenant de la certification doivent être traitées confidentiellement.

6.1.2 Exigences de sécurité des utilisateurs

- La clé privée de l'utilisateur doit être sécurisée de manière appropriée et ne doit pas être divulguée ; l'utilisateur en est tenu responsable.
- Si l'utilisateur n'utilise pas de systèmes périphériques (p.ex. CD) pour la sauvegarde de sa clé privée, il doit protéger la clé à l'aide d'un mot de passe (longueur 8 caractères minimum). Ni les médias ni le mot de passe ne doivent être transmis à des tiers et les clés ne doivent pas être conservées en texte clair ou transmises par un réseau non sécurisé.
- La longueur de la paire de clés asymétriques doit être au moins de 1024 Bit. L'utilisation de clés de longueur supérieure est recommandée et dépend des disponibilités techniques.
- Le directory de l'application dans lequel les clés sont sauvegardées doit être sécurisé par l'utilisateur de manière appropriée. Ceci peut être réalisé en attribuant des droits spécifiques à ce directory (en cas de support par le système d'exploitation). La sauvegarde des clés sur un support externe est vivement recommandée.

6.1.3 Règles de certification

Ce chapitre décrit les directives et procédures techniques et d'organisation qui doivent être respectées par la CA et l'utilisateur avant la certification.

6.1.3.1 Enregistrement

- Afin de vérifier l'identité de chaque utilisateur et de lui attribuer un certificat unique, tout utilisateur doit envoyer **une copie de sa carte d'identité avec la demande d'ouverture de compte**. L'utilisateur doit indiquer le code UCM et son adresse officielle. En acceptant la politique de sécurité, l'utilisateur autorise le G.I.E.–HealthNet et /ou ses sous-traitants à contre-vérifier les données avec les données officielles détenues par l'UCM ou une autre administration compétente. Les données doivent être confirmées officiellement avant toute émission d'un certificat. Si l'identité et le numéro UCM sont corrects, l'utilisateur recevra sa paire de clés.

6.1.3.2 Génération des clés

- En général, la CA crée et certifie les paires de clés asymétriques. Après avoir effectué le transfert des clés, la CA supprimera obligatoirement la clé privée. Ce processus doit être enregistré.

6.1.3.3 Mise à jour/prolongation

- Les utilisateurs du projet LABO doivent mettre à jour leurs certificats régulièrement (voir sous 3.4). Afin d'assurer la sécurité, la validité maximale du certificat est fixée à **deux ans**. Le remplacement d'un certificat (par exemple en cas d'expiration ou de

perte du certificat) sera traité comme la création d'un nouveau certificat. Le propriétaire sera informé environ 6 semaines avant la date d'expiration.

6.1.3.4 Suppression

- Suite à la demande d'un utilisateur, après la perte des clés, à la fin de la validité ou si l'utilisateur ne remplit pas les conditions de certification, les clés seront annulées et marquées comme révoquées, afin d'éviter une utilisation ultérieure. La CA est également autorisée à annuler des certifications à sa discrétion. En cas d'utilisation frauduleuse ou de perte de sa clé privée, tout utilisateur doit informer l'autorité émettrice immédiatement et arranger la révocation de son certificat.

6.1.3.5 Publication des clés

- Après l'activation, la clé publique de chaque participant sera publiée sur le LABO FTP.

7 Glossaire

Tiers (tierce partie)

Toute organisation/ tout utilisateur qui ne participe pas directement à HealthNet Luxembourg, mais qui travaille au nom d'un hôpital par exemple (par exemple, accomplissant des services de maintenance).

Certificat

Dans ce contexte : une paire de clés, utilisée pour chiffrer et /ou signer des données de HealthNet.

Autorité de certification (CA)

Un partenaire de confiance qui émet des certificats digitaux pour l'utilisation dans HealthNet. En ce moment, c'est le CRP Henri Tudor qui est en charge de cette tâche.

Réseau/organisation externe

Un réseau informatique et la possibilité de connexion à HealthNet Luxembourg.

Direction HealthNet

G.I.E.-HealthNet

Accès individuel

Un ordinateur individuel connecté à HealthNet Luxembourg

Système de détection anti-intrusion (IDS, Intrusion Detection System)

Un logiciel capable de détecter des manipulations indésirables sur des systèmes informatiques.

Accès réseau

Un réseau informatique qui se connecte à HealthNet Luxembourg.

Système de contrôle des accès et des privilèges

Par exemple un firewall

Sous-traitant

Toute société travaillant au nom du G.I.E.-HealthNet