Table des matières

1 PREAMBULE

1.1 Esprit

Le Système d'Information (SI) du CHU de NANTES est désormais un outil indispensable pour de nombreux professionnels. Cette tendance ne fera que s'amplifier et s'accentuer avec l'arrivée de nouvelles fonctionnalités au cœur du métier de l'hôpital (prescription connectée, plan de soins, télémédecine, etc.), entrainant des exigences croissantes en matière de sécurité et de performance du SI.

Cette performance et cette sécurité reposent sur le respect d'un certain nombre de règles et de bonnes pratiques applicables à la fois pour les utilisateurs et pour les informaticiens. De telles règles sont rendues d'autant plus nécessaires que l'évolution rapide des technologies, tant en fonctionnalité qu'en simplicité d'utilisation, et l'ouverture aux réseaux externes font apparaître de nouveaux risques.

Certains de ces risques peuvent être maîtrisés par des outils technologiques (pare-feu, anti-virus, outils de surveillance des systèmes, etc.). D'autres en revanche ne peuvent être maîtrisés sans une implication forte de chaque utilisateur. Pour cela, une prise de conscience individuelle et collective des enjeux de la sécurité du SI est indispensable, tant pour l'institution que pour l'utilisateur, notamment en ce qui concerne la responsabilité civile et pénale.

En outre, l'application de procédures de sécurité et la mise en œuvre des outils associés doit rester compatible avec les contraintes de fonctionnement opérationnel. En effet, un système sécuritaire trop contraignant pourrait in fine devenir bloquant pour la performance de fonctions métier supportées par le SI.

C'est pourquoi cette Charte se veut pragmatique et pédagogique. Elle doit susciter pour chaque utilisateur du SI des réflexes d'autorégulation favorisant une utilisation sûre et performante des services informatisés offerts aux professionnels du CHU.

La Charte Utilisateur du Système d'Information n'a pas vocation à être un guide d'utilisation des outils informatiques et renvoie pour cela le lecteur aux guides pratiques et documentations publiés sur l'Intranet.

Cette charte affiche l'engagement de la Direction Générale concernant la déontologie vis-à-vis du respect des patients, de la vie privée des utilisateurs du SI, ainsi que la construction d'une culture sécurité globale à tout l'établissement.

1.2 Objectifs essentiels

La présente charte a pour but de définir les règles de sécurité et de bon usage du Système d'Information du CHU de Nantes.

Il s'agit de fournir à tous les intervenants, y compris ceux chargés de la mise en œuvre du Système d'Information (SI), un document de référence formalisant les règles de sécurité et les comportements attendus des utilisateurs.

Il s'agit aussi de regrouper ces règles, qui existent la plupart du temps mais sont comprises dans des documents de valeur diverses et souvent distincts.

Le Système d'Information est un **outil professionnel** essentiel pour le CHU, concernant des informations de nature médicale, scientifique, de gestion du personnel ou technique et dont le bon fonctionnement est **conditionné par un usage loyal et responsable par l'ensemble des utilisateurs.**

Ces règles de bon usage relèvent avant tout du bon sens et ont pour but :

- d'assurer à chaque utilisateur un fonctionnement optimal des services informatisés nécessaires à son activité professionnelle ;
- de garantir le respect de la réglementation et de l'éthique ;
- d'être conforme à la politique de sécurité du SI ;

Cette charte s'applique à tout utilisateur interne ou externe au CHU de Nantes, qui est réputé en avoir pris connaissance et en avoir accepté les termes.

1.3 Portée

Notion d' « Utilisateur »
Est considéré comme utilisateur toute personne physique formellement autorisée à accéder au SI du CHU de Nantes, quel que soit son statut (personnel permanent ou intérimaire, stagiaire, étudiant, partenaire hébergé, prestataire externe, délégué syndical, etc.).
Un utilisateur est donc une personne, ou un groupe de personnes qui sont liés au CHU de NANTES par une relation contractuelle de type droit du travail, convention de stage, contrat relevant du code des marchés public ou de tout autre code en vigueur.
Certains utilisateurs sont, de par leur métier, amenés à travailler sur des systèmes d'information relevant des missions de recherche ou d'enseignement du CHU. La charte du SI s'applique également à ces activités, dès lors qu'elles nécessitent un accès au Système d'Information.

Notion de « Système d'information (SI) »
On entend par Système d'Information (ci-après le « SI ») l'ensemble des ressources, matérielles et logicielles, des moyens techniques, et des procédures et moyens humains et organisationnels, mis en jeu dans la création, le stockage, le traitement, l'archivage, la transmission, la diffusion et la communication des données et informations utilisées dans le fonctionnement de l'établissement quel que soit leur support (numérique, papier, oral). Cela inclut entre autres : les logiciels (applications informatiques, systèmes de messagerie électronique, outils bureautiques, systèmes d'exploitation, outils d'administration, utilitaires, bases de données…), les matériels informatiques ou bureautiques (serveurs, ordinateurs et téléphones – fixes ou portables –, PDA, imprimantes et photocopieurs, etc.), les équipements des réseaux de données (routeurs, commutateurs, autocommutateurs, fax…), les médias de stockage (disques durs, CD-ROM, clés USB, …) et les équipements de production.

Applicabilité
La présente charte s'applique au Système d'Information numérique du CHU de Nantes, soit à l'ensemble des fonctions informatisées participant à la mission de soins, d'enseignement et de recherche du CHU, qu'il s'agisse des services de soins eux-mêmes ou des services de support (administration, logistique, …).

1.4 Nature et effet

Cette charte est rédigée par le Responsable Sécurité des Systèmes d'Information (RSSI), et proposée à la validation de la Direction Générale du CHU de NANTES et des instances.

La présente charte fait partie intégrante du Règlement Intérieur du CHU de NANTES conformément aux dispositions légales et règlementaires. Les dispositions qu'elle contient ont une force juridique équivalente à celles du règlement intérieur. La violation des dispositions de cette charte peut constituer une faute susceptible d'entraîner des sanctions disciplinaires et / ou engager la responsabilité civile et pénale de celui qui commet cette violation.

Dans le cas d'intervenants externes, cette Charte est annexée au contrat entre le CHU et l'organisme ou l'entreprise prestataire qui doit garantir son application auprès de ses employés en mission au CHU.

Il est important de noter que cette charte ne peut s'appliquer qu'aux individus qui sont liés au CHU de NANTES par un lien juridique tel que décrit au §1.3. Cela exclut donc de fait les individus qui n'ont aucune relation juridique avec le CHU de NANTES comme les visiteurs temporaires, les bénévoles qui ne seraient pas liés au CHU de NANTES par le biais d'une convention avec une association, etc.
Tout individu n'ayant aucun lien contractuel avec le CHU de NANTES ne dispose d'aucun droit sur le Système d'Information du CHU de NANTES et n'a pas à y avoir accès.

Elle s'applique dès son passage aux instances de l'établissement, conformément à la législation en vigueur.

1.5 Publication et affichage

La présente charte est publiée sur l'Intranet du CHU et diffusée par les canaux de communication habituels (notes de service, flash info, etc.).

De plus, elle sera annexée et/ou intégrée :
- aux contrats et marchés passés avec les prestataires du CHU.
- aux conventions passées avec les organismes de recherche et d'enseignement publics ou privés.

1.6 Corpus documentaires

L'ensemble des documents qui régissent les règles de bon usage du Système d'Information sont la Politique de Sécurité du Système d'information et ses documents associés.

1.7 Spécifications CNIL

Conformément à la loi du 6 janvier 1978 (art 32), les données des agents dans le contexte de leur activité professionnelle sont susceptibles d'être collectées pour être traitées dans le cadre des obligations de gestion de l'institution, ou afin de mettre à disposition des logiciels utilisés par les agents dans le cadre de leurs missions.
Par exemple :

- Collecte et traitement de données afin de gérer la carrière et la paye des agents ;
- Collecte et traitement de données dans le cadre de la bonne gestion des ressources de l'établissement : affectation des PC ou des véhicules à des agents ;
- Collecte et traitement de données afin de mettre à disposition des outils informatiques : logiciels métiers, logiciels bureautiques, etc. ;

Tous les traitements font l'objet de déclaration CNIL conformément à la loi du 6 janvier 1978. Le droit d'accès et de rectification peut être exercé auprès des responsables de traitement.

2 ENGAGEMENT DES UTILISATEURS

2.1 Condition d'accès au Système d'Information

L'accès au SI du CHU de NANTES obéît aux grands principes suivants.

2.1.1 >Un accès sécurisé

Principe d'identification
Tout utilisateur du Système d'Information est identifié nominativement et accède aux ressources du SI à l'aide de moyens d'accès (login / mot de passe, carte à puce, etc.) qui lui sont délivrés personnellement en tenant compte de sa fonction et de l'organisation dans laquelle il exerce au CHU. Ces cartes, codes d'accès et les mots de passe associés sont confidentiels et ne doivent pas être divulgués à un tiers sauf circonstances exceptionnelles.
Les utilisateurs du SI ne doivent en aucun cas :

- Dégrader leur carte d'établissement afin de masquer ou falsifier leur identité
- Masquer leur véritable identité lors d'un accès au SI ;
- Usurper l'identité d'un autre utilisateur
- Permettre ou faciliter l'utilisation de leur propre identité par toute autre personne
- Contourner les mécanismes de protection du SI
- Utiliser les failles d'un composant du système pour contourner les règles de sécurité du SI

La capacité d'accéder à une information, qui résulterait d'un dysfonctionnement du système d'habilitation, d'une erreur humaine ou d'une faille d'un outil informatique, ne constitue pas un droit d'accès à cette information. Tout utilisateur qui utiliserait une telle faille serait en faute et s'exposerait à des sanctions.

Le cas particulier des identifications génériques (c'est-à-dire associées non pas à un individu, mais à un service, une UF, un groupe de personne, etc.) est dérogatoire et validé par la DSN (et éventuellement le RSSI) sur justification et au cas par cas. Ces dérogations font l'objet d'une traçabilité spécifique.

Principe de traçabilité
Tout accès logique au SI est sécurisé par une étape d'identification et d'authentification de l'Utilisateur, qui doit fournir son couple d'identifiant et mot de passe ou tout moyen d'authentification mis en place dans l'organisme (ex. cartes d'établissement ou cartes de type CPS/CPE).

Ce contrôle d'accès logique permet à chaque connexion de l'Utilisateur l'attribution de droits et privilèges propres définis en considération stricte des besoins du poste qu'il occupe (ci-après le « compte Utilisateur »).

D'une manière générale, l'Utilisateur admet que toute connexion au SI permet son identification et qu'elle constitue une acceptation implicite de l'enregistrement automatique de traces de son activité.

Principe d'imputabilité
Tous les secrets et moyens d'authentification (cartes à puce, codes PIN, mots de passe, etc.) sont strictement personnels et il est interdit de les communiquer, de les prêter à un tiers ou de les partager.

Il en résulte que chaque Utilisateur est tenu pour responsable des opérations effectuées à partir de son compte Utilisateur ou grâce à sa carte d'établissement, dont l'utilisation est réputée, a priori, être de son fait. Il s'agit notamment des opérations d'authentification (par exemple connexion à un progiciel) et de signature (lorsqu'un dispositif de signature numérique type carte CPE/CPS est mis en œuvre).

2.1.2 Un usage loyal et professionnel

Les moyens mis à la disposition de l'Utilisateur par l'établissement doivent être mis en œuvre dans une finalité professionnelle et leur utilisation doit rester conforme aux besoins du service et aux intérêts de l'établissement.

L'usage de l'outil informatique doit donc être **licite et conforme** au cadre légal et réglementaire existant et à la déontologie.
Les règles énoncées ci-après n'ont aucun caractère exhaustif. La réglementation et la jurisprudence évoluent assez régulièrement dans ce domaine, et il est vivement conseillé de se rapprocher de sa direction en cas de doute sur le caractère licite d'un usage particulier.

Dans tous les cas, l'usage de l'outil informatique doit être conforme aux règles professionnelles, aux procédures et référentiel internes ainsi qu'aux obligations contractuelles des utilisateurs.

2.1.3 Une classification de l'information

Tout utilisateur peut être amené à avoir connaissance ou à manipuler des informations plus ou moins sensibles sur le plan de la confidentialité. Il est de son devoir de ne pas diffuser à l'extérieur du CHU les informations qui pourraient nuire au fonctionnement ou à l'image de l'institution ou porter préjudice à une personne, qu'elle soit employée par le CHU ou patient de l'Hôpital. Les informations internes au CHU sont accessibles aux professionnels dans la mesure où elles sont nécessaires à l'exercice de leur fonction.

De manière générale, les informations peuvent être classées en trois catégories de criticité croissante :

- Les informations de niveau **« Public »** qui peuvent être diffusées librement à l'intérieur et à l'extérieur du CHU. Il s'agit, par exemple, de toute information utile à l'usager dans sa relation avec le CHU (numéros de téléphone des secrétariats des services de soins, adresse du site Web du CHU, …)
- Les informations de niveau **«Interne CHU»**. Ces informations sont accessibles sans restriction à tout personnel du CHU pour qu'il en fasse usage dans le cadre de sa fonction et dans le respect des procédures internes et du règlement intérieur. Ce type d'information ne doit cependant pas être diffusé à l'extérieur du CHU car pouvant perturber le fonctionnement des services (par exemple, les numéros de téléphone directs des personnels du CHU, médecins, directeurs, ou de locaux tels que les blocs opératoires, etc.)
- Les informations de niveau **« Accès restreint».** Ces informations présentent un niveau de criticité élevé au regard d'un des critères suivants :
    - Informations nominatives, médicales ou administratives, concernant un patient
    - Informations concernant le personnel du CHU
    - Informations sensibles au regard des critères de sécurité (disponibilité, intégrité, confidentialité)
    - Informations de production personnelle (bureautique)
    - Informations relatives à la vie privée
    - Informations de management ou d'organisation du CHU (politique, stratégie)
    - Informations relatives à la sécurité et aux contre-mesures associées
    - Informations possédant une valeur financière ou scientifique (travaux de recherche)

Les informations de type « Accès restreint » doivent être manipulées et / ou transmises dans le respect de la réglementation en vigueur : Code de la Santé Public, décret confidentialité, etc.

La classification d'une information est directement applicable au média informatique qui sert à la traiter, à la stocker ou à la communiquer. C'est la classification la plus élevée des informations contenues dans le média qui s'applique à celui-ci dans sa totalité.

2.2 Règles générales de sécurité et de bon usage

Généralités

Chaque utilisateur s'engage à :

- respecter les règles de gestion relatives à la classification et la protection des informations et documents ; différentes instances internes au CHU de NANTES traitent des questions de confidentialité de données et des politiques d'habilitation associées ;
- s'assurer que ses données sont régulièrement sauvegardées, conformément aux recommandations prévues et aux solutions mises à disposition, et tout en évitant les stockages redondants ou inutiles ; la DSN peut être contactée en cas de question sur ce sujet ;
- ne pas installer des matériels ou logiciels autres que ceux validés par le CHU de NANTES ;
- sous peine de constituer un acte relevant de la contrefaçon, ne pas dupliquer ou utiliser les logiciels mis à leur disposition, en dehors des limites des droits d'utilisation acquis par l'organisme ;
- ne pas effectuer des installations et/ou des connexions non autorisées, en particulier établir une connexion physique et/ou logique alors qu'une connexion au réseau de l'établissement est en cours (modems, LAN, …) ;
- ne pas volontairement modifier ou supprimer les outils de sécurité mis en place pour la protection du Système d'Information ; en particulier,
    - changer la configuration du logiciel anti-virus installé sur son ordinateur professionnel par le service informatique ;

- modifier la configuration des postes et autres moyens mis à sa disposition (messagerie, réseau, Internet,…) sur des paramètres ayant trait à la sécurité du poste de travail et son environnement ;
- effectuer des opérations qui pourraient causer, de manière directe ou indirecte, une atteinte à l'intégrité, la disponibilité et la confidentialité des moyens informatiques et des informations dont l'établissement est propriétaire.

Concernant les documents papier, les utilisateurs sont invités à prendre les précautions suivantes :
- impression sécurisée par utilisation de code PIN ;
- prendre garde aux oublis de documents dans les imprimantes et les photocopieurs multifonction ;
- rangement sous clé des documents sensibles ;
- broyage des documents sensible avant de les jeter ;

Les utilisateurs doivent également prendre garde au comportement à l'extérieur du CHU de NANTES, et notamment :
- Ne pas diffuser de données pouvant nuire à l'image de l'établissement ;
- Devoir de réserve lors d'échanges oraux dans les lieux publics ou avec des personnes non habilitées ;
- Utilisation d'appareils nomades dans les lieux publics (wifi non protégé, « shoulder-surfing », etc.) ;
- Protection des biens de l'établissement en dehors des locaux (postes portables, smartphones, carte d'établissement, carte matricielle, USB, papier, etc.) ;
- Accès à distance depuis des postes non maîtrisés (session laissée ouverte, copie de données, postes « à risques » type cybercafé, etc.).

Les utilisateurs doivent également remonter sans délai :
- - les événements ou incidents de sécurité suspectés ou avérés
- - les anomalies et failles de sécurité
- - les vols/pertes de matériel ou d'informations du CHU
- - les violations des règles de sécurité définies.
- - etc.

Par exemple sont interdits :
- le fait d'utiliser des outils mettant sciemment en cause l'intégrité du SI ou de propager des virus informatiques, notamment en introduisant sur le SI des CD Rom, DVD Rom, clé USB ou tout autre support de stockage externes détenus à titre personnel,
- le fait d'utiliser des outils d'analyse de type balayage (« scan ») ou repérage (« sniff ») ou tout autre moyen de surveillance et d'écoute du trafic réseau ;
- le fait de contourner ou tenter de contourner des moyens ou procédures de sécurité (ex. utilisation d' « anonymisers »).

Protection des codes d'accès
Les codes d'accès et les mots de passe garantissent la confidentialité des informations. Ils signent les accès de l'utilisateur et constituent des éléments clés de la traçabilité des accès aux informations et aux ressources du SI.
Chaque utilisateur est responsable de la confidentialité de ses codes d'accès, il lui incombe d'appliquer les bonnes pratiques suivantes :
- choisir un mot de passe non trivial, de longueur suffisante (8 caractères au minimum), en incluant des caractères non-alphabétiques tels que #, &, _, etc.
- changer régulièrement son mot de passe et chaque fois qu'il y a doute sur sa confidentialité
- ne jamais communiquer son mot de passe à un tiers sauf circonstance exceptionnelle (urgence vitale par exemple) et dans ce dernier cas, le changer dès le retour à une situation normale ;
- protéger ses cartes et éventuels moyens d'authentification forte (token, carte matricielle ou « bataille navale »).
- ne pas masquer ou tenter de masquer sa véritable identité ;
- ne pas accéder ou tenter d'accéder au compte d'un autre Utilisateur sans l'autorisation de celui-ci ;
- ne pas conserver une copie de ses secrets d'authentification, sur papier ou sous format électronique, qui ne serait pas protégé comme une donnée classifiée ;
- ne pas quitter son poste de travail en laissant accessible une session réseau ou applicative ouverte, laquelle doit être au minimum protégée par un écran de veille avec mot de passe ;

Confidentialité de l'information
Chaque utilisateur s'engage à :
- ne pas diffuser des informations, à fortiori sensibles, sur les lignes ou réseaux non sécurisés tels que le fax et le téléphone en externe, la messagerie électronique ou Internet ;
- ne pas permettre la divulgation à des tiers non autorisés de données à caractère personnel ou confidentiel présentes sur le Système d'Information ; cette règle doit être scrupuleusement respectée lors de l'utilisation de support de stockage externe type clé ou disque dur USB, DVD, etc. ;

- ne pas diffuser en dehors du CHU de NANTES des informations confidentielles, à fortiori nominatives ou médicales ;
- lorsqu'il est responsable d'un traitement de données nominatives au sens de la loi informatique et liberté, procéder à la déclaration CNIL de tout fichier ou application contenant des données à caractère personnel;
- respecter la limite de ses habilitations, droits d'accès et/ou privilèges, en fonction de chaque application ;
- dans le cadre du chiffrement de données professionnelles :
    - utiliser les outils et clés de chiffrement fournis par les équipes informatiques et sécurité du site,
    - chiffrer également au moyen de la clé fournie par l'établissement.
- Ne pas limiter par un mot de passe l'accès à des fichiers ou mettre en œuvre tout autre moyen (chiffrement des données par exemple) susceptible d'entraver la continuité du service ou les opérations de maintenance ou de contrôle ;

Concernant la confidentialité des informations, nous attirons fortement l'attention sur les règles spécifiques qui régissent les informations de nature médicale. Les utilisateurs sont invités à prendre connaissance de la charte de l'information médicale de l'établissement et de la réglementation sur ce sujet ou à se rapprocher de leur direction en cas de doute sur ce sujet.

Il est strictement prohibé d'utiliser les répertoires communs (accessibles à tous les utilisateurs) des serveurs bureautiques du CHU de NANTES afin de créer, de stocker, d'échanger ou de publier des fichiers comprenant des données nominatives qu'il s'agisse de données concernant les patients, le personnel ou toute personne physique. Cette règle s'applique à tous les types de fichiers (Word, Excel, Access, Power Point, PDF, Images, …).

2.3 Règles spécifiques

2.3.1 Usage des espaces de fichiers commun

Par défaut, les fichiers et répertoires stockées sur les espaces communs (serveurs de fichiers, espace dans l'explorateur identifiés par des lecteurs au-delà de la lettre « E ») sont réputés professionnels.

L'utilisateur s'engage à ne pas :

- chiffrer par ses propres moyens des données, même personnelles ; l'usage de progiciel de cryptage à ces fins est strictement interdit en dehors de ceux fournis par l'institution ;
- stocker des données personnelles sur les espaces réservés aux données professionnelles ;
- stocker des données professionnelles sur les espaces réservés aux données personnelles ;

2.3.2 Usage de la messagerie

L'utilisateur s'engage à :

- Assumer la responsabilité du contenu et de la forme de tout message qu'il émet avec son adresse de messagerie établissement. Il ne doit pas se faire passer pour une autre personne en utilisant son adresse ;
- En cas de réception d'un message ne lui étant pas destiné il est demandé à l'utilisateur de le supprimer et d'avertir l'émetteur. Dans la mesure du possible il doit également éviter d'en prendre connaissance.
- se conformer aux règles de gestion relatives à la classification et la protection des informations et documents. A cet égard, l'utilisateur s'engage, en fonction de la nature et de la sensibilité des informations qu'il transmet, à utiliser les outils mis à sa disposition (ex. logiciel de chiffrement des données) ;
- prévenir toute confusion ou erreur sur l'origine ou la destination des messages et en particulier, prévenir toute diffusion de données ou informations issues du SI à des destinataires non autorisés, ainsi que toute diffusion de données à caractère personnel à destination de tiers non autorisés. Pour éviter ce genre d'erreur il convient entre autre d'être vigilant aux homonymes.
- prévenir tout engorgement du système de messagerie électronique et, à cet effet détruire ou archiver régulièrement ses messages ;
- prévenir l'envoi et/ou, en cas de réception, l'ouverture de fichiers dits « exécutables » (programmes, logiciels ou applications, …) en raison de la menace sérieuse qu'ils constituent pour la sécurité et l'intégrité du réseau de l'établissement (ex. risque majeur d'infection par un virus, risque d'intrusion par un tiers malveillant) ;
- respecter les limitations de la taille des pièces jointes, de la nature des fichiers, du nombre des destinataires le cas échéant ;

- le transfert automatisé des messages de la messagerie professionnelle vers une messagerie personnelle est interdit ;

L'utilisateur s'engage à ne pas :

- utiliser des messageries instantanées de type MSN Messenger, Skype ou AIM ;
- utiliser, *aux fins d'envoi de courriers à caractère privé*, les listes de diffusion (*mailing lists*), ainsi que les boîtes aux lettres collectives ou génériques, créées dans le cadre des activités de l'organisme ;
- chiffrer les messages sortants, et tous les messages ou archives de messagerie, signalés comme « PERSONNEL », tant dans leur contenu qu'en ce qui concerne les fichiers (image, texte, …) qui y sont attachés ;
- participer à des « chaînes de solidarité » (appelés aussi « *spam* sociaux ») ;
- diffuser des alertes virus ou autres messages de sécurité ; sur ce point, il est vivement conseillé à tout utilisateur ayant connaissance d'une alerte de sécurité de la communiquer directement à la DSN ou au RSSI, qui prendra les mesures conservatoires adéquates ;
- utiliser depuis le CHU de NANTES des relais de messagerie de type webmail ;

Responsabilité des utilisateurs

L'**hameçonnage** (ou ***phishing***, et parfois **filoutage**), est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. L'hameçonnage peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques.

Le CHU de NANTES dispose de moyens techniques permettant de filtrer les vecteurs habituels de communication du hameçonnage (filtres anti pourriels, filtre web, etc.). Cependant, aucun filtre n'est parfaitement efficace et il est impossible au CHU de NANTES de garantir qu'aucun site web, message électronique ou autre moyen de transmission ne puisse pénétrer le réseau interne du CHU de NANTES.

Tout utilisateur est notamment informé du danger du hameçonnage. En particulier, tout utilisateur est informé du fait que toute transmission de renseignements personnels ou confidentiel (mot de passe, numéro de carte de crédit, etc.) par tout moyen de communication (messagerie, site web, téléphone, etc.), engage l'utilisateur et lui seul et dégage toute responsabilité du CHU de NANTES sur les conséquences de cet acte.

2.3.3 Services Internet (Web, ftp, …)

L'utilisateur s'engage à :

- ne pas modifier la configuration du logiciel de navigation (comme Internet Explorer). Tout besoin de déroger à cette règle est soumis à autorisation de la part de la DSN ou du RSSI ; de manière générale, l'accès à l'Internet ne doit être réalisé qu'à partir des équipements fournis par l'établissement ;
- ne pas participer ni publier d'informations sur des forums de discussion, des blogs externes ou des réseaux sociaux de type Facebook dans le cadre de l'activité professionnelle, sauf le cas des personnes ayant mandat de l'organisme ;
- ne pas installer une ressource web partagée (site web, serveur FTP, etc.) sur son poste de travail ;
- ne pas mener d'activités liées la création et l'administration de sites Web, *blogs* privés ou de réseaux sociaux de type Facebook, à l'aide des moyens professionnels mis à la disposition de l'Utilisateur
- Ne pas utiliser les réseaux P2P ni télécharger ou consulter des fichiers image/audio/vidéo sans lien avec l'activité professionnelle ou en violation de droits de tiers (notamment contrefaçon) ;

L'utilisateur s'engage à :

- respecter les mesures de filtrage au moyen de listes de sites autorisés ou à l'inverse interdits ;

2.3.4 Matériels et logiciels tiers

Les règles d'installation et / ou de connexion de matériels et logiciels tiers, c'est-à-dire non fournis de base par la DSN, sont décrites dans un document spécifique de Politique Technique de Sécurité, accessible sur simple demande à la DSN.

2.4 Usage de matériels personnels dans le cadre de l'activité professionnelle (BYOD)

Cette partie a pour objectif de cadrer l'usage du BYOD conformément à l'ISO/CEI 27002:2013, clause 6.2.1

2.4.1 Définition

Le BYOD (Bring Your Own Device) s'entend de la capacité d'un établissement à accepter que ses agents utilisent du matériel informatique personnel (smartphones, PC, tablettes, etc.) pour travailler.

2.4.2 Segmentation de l'offre de services

La DSN segmente l'offre de service BYOD en plusieurs catégories ou bouquets.

BYOD B1 : il s'agit de la possibilité donnée aux agents de synchroniser leurs smartphones personnels avec la messagerie interne de l'établissement : messagerie, calendrier, contacts.

BYOD B2 : il s'agit de la possibilité donnée aux agents dans les locaux de l'établissement de connecter un matériel personnel (PC, MAC, smartphone, tablette, etc.) sur un réseau Wifi interne à l'établissement et dédié aux agents, ce réseau Wifi donnant accès à un bouquet de service applicatif métier restreint : Intranet, messagerie, VIDAL électronique, etc. Ce bouquet de service a vocation à s'étendre à l'avenir.

BYOD B3 : il s'agit de a possibilité donnée aux agents d'accéder à un autre bouquet de service applicatif métier plus étendu à partir d'un équipement (MAC, PC, smartphone, tablette, etc.) connecté à l'Internet.

Chacune de ces catégories a vocation à évoluer, et la DSN pourra rajouter d'autres catégories à son offre à l'avenir.

2.4.3 Condition d'accès au service

L'utilisation du BYOD par les agents de l'établissement relève de leur libre choix. Cette utilisation ne peut donner droit à aucune compensation (heures supplémentaires, remboursement de matériel, etc.).

Certains de ces services peuvent être de plus restreints à certaines populations : cadres, médecins, etc.

L'utilisation des services BYOD par l'agent vaut acceptation des règles de la présente charte.

2.4.4 Assistance technique

Une procédure de connexion et un mode opératoire sont fournis aux utilisateurs.

Il n'y a aucune assistance technique de la DSN dans l'accès à ces services.

2.4.5 Sécurisation des accès

L'utilisation de ces services engage la responsabilité personnelle de l'agent, qui doit prendre toutes les précautions pour assurer la confidentialité des données auxquelles il accède. Notamment, en cas de perte ou de vol de son équipement, il appartient à l'agent de prévenir la DSN sans délai pour supprimer l'accès technique à partir de l'équipement.

L'agent doit notamment mettre en place un contrôle d'accès sur son équipement : code PIN, mot de passe, etc. Ce contrôle d'accès vient s'ajouter au contrôle d'accès technique mis en place par la DSN pour l'accès au service : certificat, mot de passe, etc.

2.4.6 Prérogatives de l'établissement

Si la DSN doit procéder à un effacement à distance, l'établissement ne pourra pas être tenu pour responsable des éventuelles données personnelles qui auraient été effacées en même temps dans la procédure technique.

La DSN est autorisée à contrôler le respect des procédures de sécurité par l'agent (sécurisation du terminal, terminal protégé conte les malwares, etc.) et se réserve le droit de supprimer l'accès à tout moment.

2.4.7 Disponibilité du service

Le service est en principe accessible en 24-7-365.

Cependant, il n'y a aucun engagement de la part de l'établissement en termes de disponibilité d'accès des services BYOD. La panne d'un service BYOD ne dégage pas l'agent de ses obligations professionnelles.

Il peut notamment être interrompu à tout moment, tout ou partie, pour des questions de sécurité.

2.4.8 Fin de service

En cas de départ de l'agent de l'établissement, l'accès au service est supprimé sans préavis.

3 CADRAGE DES OPERATIONS DE CONTROLE

3.1 Généralités

Conformément à la législation et à la jurisprudence, les données hébergées dans le système d'information sont supposées être des données à caractère professionnel.

Toute opération de contrôle doit cependant respecter les principes suivants, garants de l'équité et du respect de la vie privée résiduelle sur le lieu de travail :
- un contrôle loyal : la démarche de contrôle doit être **impartiale** c'est-à-dire que l'administrateur doit agir dans le seul cadre de ses fonctions et que son action répond à une nécessité justifiée par des impératifs de bon fonctionnement et de sécurité ;
-un contrôle transparent : sa démarche s'inscrit dans une logique de transparence vis à vis des Utilisateurs qui doivent être préalablement informés par l'organisme de la mise en place d'un dispositif de contrôle (pas de surveillance à l'insu des Utilisateurs).
- un contrôle proportionnel : les contrôles opérés doivent être conformes aux finalités déclarées pour chaque dispositif de surveillance ;
- un contrôle adéquat : faisant écho au principe de nécessité, les moyens de contrôle mis en œuvre par l'administrateur sont ceux strictement nécessaires à sa mission, sans aller au-delà (ex. pas de contrôle du contenu même des messages si le contrôle du volume des pièces jointes ou des extensions de fichiers joints permet de vérifier l'utilisation optimale du réseau).

Toute action de l'utilisateur sur le système d'information est susceptible d'être tracée, et en particulier :
La connexion / déconnexion au système d'information (login) ;
La navigation Internet (web) ;
L'usage de la messagerie ;
Tout logiciel à caractère technique, bureautique ou métier ;
L'usage des serveurs de fichiers ;
L'usage de la téléphonie ;
Etc. ;

3.2 Spécificité des contrôles des connexions à l'Internet

La connexion à l'Internet est protégée par un dispositif de sécurité imposant l'identification nominative de l'utilisateur (Proxy). Ce dispositif sert également à interdire l'accès aux sites dont le contenu présente un caractère illégal, non conforme aux bonnes mœurs ou simplement sans rapport avec l'activité professionnelle des personnels du CHU. L'établissement se réserve, de plus, le droit de bloquer les accès à des sites jugés sans rapport avec l'activité professionnelle.

Les connexions et les accès aux sites WEB sont tracés dans des fichiers journaux. L'exploitation de ces traces est réalisée conformément aux dispositions décrites ci-après.

3.3 Spécificité des contrôles d'usage de la messagerie

Pour des raisons de qualité de service, la DSN réalise des sauvegardes régulières des boîtes à lettres électroniques. De plus, compte tenu de la valeur légale des courriels professionnels, la DSN peut être amenée à archiver ces boîtes à lettres sans limite de durée.

Compte tenu de la tolérance accordée pour un usage privé de la messagerie, ces sauvegardes et archives peuvent contenir des messages privés. En effet, pour des raisons pratiques et pour garantir le respect de la vie privée, le DSN ne peut effectuer de filtrage de ces courriels privés lors des opérations de sauvegarde et d'archivage (dans le respect du secret des correspondances).

En cas de dysfonctionnement ou d'alerte de sécurité, les administrateurs système de la DSN pourront être amenés à accéder aux courriels archivés qu'ils soient professionnels ou privés. Dans ce dernier cas, cet accès se fera dans le respect des dispositions légales de protection de la vie privée.

3.4 Exploitation des fichiers de journalisation et de traces

La Charte de Sécurité et de bon Usage du Système d'Information est un élément clé de la politique de sécurité du SI du CHU. Cette politique prévoit, conformément au modèle normalisé ISO 27000, de réaliser des campagnes d'audit. Chaque campagne d'audit comporte un volet sur le respect de la Charte.

Les actions de contrôle sont réalisées dans le respect des obligations légales de l'employeur relatives à la cyber surveillance et la législation de la CNIL. Notamment, les contrôles sont réalisés par le recueil de données en masse pour une exploitation statistique ou par échantillonnage aléatoire sans cibler a priori un individu ou un groupe d'individus. En revanche, les mesures correctives pourront s'appliquer de façon ciblée si l'analyse statistique met en évidence des comportements hors norme ou non conformes. De même des analyses ciblées peuvent être réalisées en cas de suspicion de la violation de la confidentialité des informations ou des règles d'usage du système d'information.

La DSN procède à une exploitation statistique de fichiers de journalisation et de trace sous forme anonyme, à des fins opérationnelles (performance, continuité de service, sécurité). Cette exploitation consiste notamment à établir des statistiques relatives aux connexions, échanges de données et consommation de ressources informatiques (par exemple les espaces disques). Elle vise également à garantir la traçabilité des accès aux données sensibles du Système d'Information.

3.5 Périodicité

Les campagnes d'audit peuvent être déclenchées de façon aléatoire ou à la demande de la direction du CHU. Concernant la confidentialité du dossier patient, le CIMPD a décidé de déléguer à la DSN la réalisation d'un audit périodique de confidentialité.

3.6 Procédures applicables

Tout accès à des données de trace doit respecter les grands principes décrits au 3.1 ci-dessus.

La DSN et le PIMESP peuvent procéder à des audits à caractère nominatif sur les traces enregistrées suite à un dysfonctionnement, une alerte de sécurité ou une présomption d'utilisation des ressources informatiques non conforme à la présente Charte. Dans le cas où l'investigation nécessaire concerne des données relatives à des patients, l'exploitation des traces est réalisée par le PIMESP.

Cet accès ne peut se faire que sur l'ordre explicite et écrit du RSSI. Dans certains cas sensibles, l'accord du Directeur des Ressources Humaines, voire du Directeur Général, peut être demandé.

3.7 Réquisitions judiciaires

L'accès aux données de trace peut également être fait sur la demande des autorités judiciaires.

3.8 Accès à des données identifiées comme privées

En plus des dispositions décrites au 3.6 et 3.7, au cas où le CHU de NANTES aurait besoin d'accéder à des données identifiées comme privé (par exemple pour une question de continuité de service ou pour une urgence vitale), cet accès se ferait dans le respect de la réglementation en vigueur, à savoir :

- Soit présence de l'Utilisateur
- Ou bien, en son absence, •« celui-ci dûment appelé et invité à être présent» conformément aux dispositions règlementaires en vigueur et aux préconisations de la CNIL ;

3.9 Accès aux mots de passe

En plus des dispositions décrites ci-dessus, au cas où le CHU de NANTES aurait besoin de d'accéder aux données d'un agent pour des questions de continuité de service ou pour une urgence vitale.

Soit l'agent est présent, et il lui est demandé de communiquer son mot de passe à une tierce personne en prévision d'une absence (congés, maladie, maternité, déplacement professionnel, etc.) : l'agent est tenu de communiquer ce mot de passe à une personne et une seule, la direction d'appartenance de cet agent devant mettre en place un dispositif de décharge de l'agent concernant sa responsabilité dans l'usage de son mot de passe en son absence.

Soit l'agent est absent, et la DSN pourra réinitialiser ce mot de passe et communiquer l'accès à une personne et une seule désignée par la hiérarchie de l'agent, le même dispositif de traçage devant être mis en place conjointement par la DSN et la direction d'appartenance de l'agent.

4 VIE PRIVEE

4.1 Généralités

Un usage personnel des moyens informatiques mis à la disposition de l'utilisateur est exceptionnellement admis pour répondre à des situations d'urgence ou dans le cas des nécessités habituelles de la vie courante et familiale. En aucun cas, l'utilisation des ressources du SI à des fins privées ne doit mettre en péril le bon fonctionnement, la performance ou la sécurité du Système d'Information.

L'usage privé du SI doit rester conforme aux dispositions légales, règlementaires et professionnelles ainsi qu'à la déontologie. En cas de non-respect de ce principe, le CHU se réserve le droit de prendre des sanctions, voire d'alerter les autorités compétentes.

4.2 Rôle et limite du champ d'action des administrateurs système

Les « administrateurs » peuvent être amenés dans le cadre des opérations d'exploitation courante à accéder par erreur et en toute bonne foi à des informations d'ordre privé. Ils doivent dès qu'ils s'aperçoivent du caractère privé de ces informations cesser immédiatement leur consultation et ne pas les divulguer. Dans le cas où cet accès serait dû à la mauvaise utilisation des ressources informatiques par le propriétaire des informations (par exemple stockage d'informations privées dans un espace public) l'administrateur avertit l'utilisateur pour lui permettre de prendre les mesures adéquates.

En cas de dysfonctionnement grave du Système d'Information imputable à l'utilisation des ressources du SI à des fins privées, la DSN peut être amenée à supprimer des données ou des programmes d'usage privé sans préavis et sans recours possible de la part de l'utilisateur.

4.3 Encadrement de l'espace informatique privé sur le lieu de travail

Les fichiers et répertoires
Le stockage de données privées est strictement limité à l'espace disque local à l'ordinateur de l'utilisateur.
L'attention est attirée sur le fait que cet espace privé n'est pas sauvegardé ni sécurisé : il appartient à l'utilisateur de s'assurer lui-même de la sauvegarde de ses données privées en dehors du système d'information de l'établissement.
Tous les fichiers et répertoires stockés sur les espaces partagés (serveurs de fichiers, serveur de données, etc.) sont supposés professionnels.

De manière générale, le stockage ou la sauvegarde des données privées est
- *préconisé* sur support amovible privé ;
- *toléré* sur le disque dur du poste de travail, dans un dossier nommé « PRIVE » sur le disque dur ;
- *prohibé* sur des ressources partagées ;

Les messages
Par défaut, tout message émis à partir ou reçu dans la boîte aux lettres d'un utilisateur est supposé professionnel.
Pour être considéré comme privé, un message devra avoir
- soit été déplacé dans un dossier de la messagerie intitulé « PRIVE ».
- soit inclure, dans son titre, le mot « PRIVE » libellé tel quel ;

Le strict non-respect de cette règle entraîne la présupposition du caractère professionnel du message.

Navigation Internet
Par défaut, l'usage de l'outil internet est réputé professionnel.

5 SANCTIONS

La responsabilité du CHU peut être engagée du fait de l'action des utilisateurs, et en particulier en cas d'un usage non conforme aux lois et règlements.

Tout utilisateur peut être tenu pour responsable juridiquement de l'usage qu'il fait du Système d'Information. Sa responsabilité peut notamment être engagée sur le plan pénal, civil et professionnel.

Lorsque sa responsabilité pénale est reconnue, l'utilisateur s'expose notamment à des peines d'emprisonnement et d'amende.

Lorsque sa responsabilité civile est reconnue, l'utilisateur s'expose à des demandes de dommages-intérêts de la part de la victime.

La responsabilité civile de l'utilisateur peut être engagée en cas de manquement aux dispositions de la présente charte susceptible de constituer une faute et de causer un préjudice aux personnes et/ou aux biens, matériel et/ou immatériel.

Par ailleurs, l'administration ne sera pas tenue d'assurer la protection fonctionnelle de l'agent telle que prévue à l'article 11 de la loi du 13 juillet 1983 portant droits et obligations des fonctionnaires en cas de faute personnelle détachable du service.

Lorsque sa responsabilité professionnelle est reconnue, l'utilisateur s'expose à des sanctions disciplinaires.

La responsabilité professionnelle de l'utilisateur peut être engagée en cas de manquement aux dispositions de la présente charte susceptible de constituer une faute professionnelle telle qu'elle est définie par :

- les Codes de déontologie et les dispositions règlementaires applicables aux professionnels de santé concernés
- le statut de la fonction publique et en particulier les droits et obligations des personnels de la fonction publique hospitalière
- le règlement intérieur du CHU de NANTES
- la charte de l'Information médicale du CHU de NANTES
- les notes de service

Par ailleurs, en cas de non-respect de la présente Charte, le CHU de Nantes peut appliquer des mesures de restriction d'utilisation du SI, à titre provisoire ou définitif et se réserve le droit de déconnecter un utilisateur sans préavis, ou de neutraliser tout fichier manifestement illégal.

Les utilisateurs du Système d'information sont donc tenus de faire un usage licite et conforme aux lois et règlements du Système d'Information. Le non-respect de ces règles expose l'agent à des sanctions administratives ainsi qu'à des poursuites civiles ou pénales.