



Le Ministre

Circulaire N° 032 / DIM / SG/2016. 17 MARS 2016

Mesdames et Messieurs

- Le Secrétaire Général ;
- Le Chef du Cabinet de Monsieur le Ministre ;
- l'inspecteur Général ;
- Les Directeurs de l'Administration Centrale ;
- Les Directeurs Régionaux de la Santé ;
- Le Directeur de l'Ecole Nationale de Santé Publique ;
- Les Chefs des Divisions rattachées au Secrétariat Général ;
- Les Directeurs des Instituts ;
- Les Directeurs des CAPM, CNTS et CNRP.

Object : Sécurité du Système d'information du Ministère de la Santé.

Réf: Lettre n°10 / DGSSI / DAFCE.

P.J : Charte relative à l'usage des Systèmes d'Information du Ministère de la Santé.

Par lettre sus référencée, la Direction Générale de la Sécurité des Systèmes d'Information, relevant de l'Administration de la Défense Nationale, a procédé à l'élaboration d'un ensemble de guides qui proposent des lignes directrices et des règles de bonne pratique pour la protection des systèmes d'information de l'Etat.

Ainsi, et afin de garantir une meilleure utilisation du Système d'Information au niveau de notre Département, j'ai l'honneur de vous faire parvenir, ci-joint, une charte relative à l'utilisation du Système d'Information du Ministère de la Santé.

L'objectif de cette charte se résume comme suit :

- Définir les règles régissant l'usage des systèmes d'information et les ressources technologiques y afférentes ;
- Préciser les règles de sécurité relatives au Système d'Information du Département ;
- Préciser les droits et devoirs de l'Administration et de l'utilisateur du Système d'Information.

Compte tenu de l'importance que revêt la sécurité des systèmes d'information parmi les priorités sectorielles, je vous demande de prendre toutes les mesures nécessaires pour se conformer à la stricte application de ladite charte, en lui assurant une large diffusion auprès de vos services.

Le Ministre de la Santé

Le Ministre de la Santé

El Housseine MOUADEB



Charte relative à l'usage des systèmes d'information du Ministère de la Santé

Préambule

La présente charte est portée à la connaissance de tout utilisateur des technologies de l'information et de la communication au Ministère de la Santé.
Elle définit les règles régissant l'usage des systèmes d'information et des ressources technologiques et précise les règles de sécurité relatives au système d'information que l'utilisateur et l'institution s'engagent à respecter et les engagements de l'administration envers cet utilisateur. Par la présente charte on précise, donc, les droits et devoirs de chacun.

Définitions

Le système d'information est l'ensemble des moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition de l'utilisateur. A cette partie fixe du système d'information s'ajoute une partie dynamique ou mobile, non négligeable, tels que les assistants personnels, les ordinateurs portables, les téléphones portables ... ou tout moyen servant comme outil pour accéder, à distance, au système d'information du Ministère.

Un utilisateur est toute personne, interne ou externe, ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information quel que soit son statut (fonctionnaire, prestataire de service, stagiaire, ...).

Le bon fonctionnement du système d'information suppose le respect, d'une part, des dispositions législatives et réglementaires, et, d'autre part, des normes et standards internationaux adoptés par le ministère de la Santé comme référence, qui s'imposent et notamment, la sécurité, la performance des traitements et la conservation et la protection des données personnelles.

Le responsable du traitement : désigne une personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres,



détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires, le responsable du traitement doit être indiqué dans la loi d'organisation et de fonctionnement ou dans le statut de l'entité légalement ou statutairement compétente pour traiter les données à caractère personnel en cause ;

Le responsable/personne habilité : désigne une personne responsable de l'information ou le responsable hiérarchique, ou toute autre personne désignée par l'administration comme habilitée à recevoir des demandes

Le Responsable de la sécurité des systèmes d'information (RSSI) : est chargé de la définition et de la mise en œuvre de la politique de sécurité. Il possède en outre un rôle stratégique d'information, de conseil et d'alerte sur les risques en matière de sécurité informatique.

Article 1 : Périmètre d'application de la charte

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à tous les systèmes d'information du Ministère de la Santé. Tous les utilisateurs de ces systèmes d'information sont dans l'obligation de respecter les dispositions de cette charte et des textes législatifs et réglementaires qui encadrent leur fonction ainsi que les normes et standards internationaux adoptés par le ministère de la Santé comme référence.

Article 2. Engagements du Ministère de la Santé

- ❖ Le Ministère de la Santé, s'engage, à travers cette charte à mettre à la disposition des utilisateurs de son système d'information, tous les moyens nécessaires (ordinateurs, imprimantes, connexion aux serveurs, connexion Internet, partage des ressources, ...) pour accomplir ses missions, dans la limite des attributions de chaque personne et des ressources budgétaires disponibles.
- ❖ Le Ministère de la santé met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection de la vie privée des utilisateurs.
- ❖ Le Ministère de la santé facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont exclusivement à usage professionnel.
- ❖ Le Ministère de la santé est tenu de respecter la vie privée de chaque personne utilisateur de son système d'information.

Article 3. Engagement de l'utilisateur

- ❖ L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a l'obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie.
- ❖ L'utilisateur a une responsabilité particulière dans l'utilisation des ressources mises à sa disposition par le Ministère de la santé.
- ❖ En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut de fonctionnaire, de stagiaire ou de d'intervenant externe.
- ❖ L'utilisateur a l'obligation de respecter l'ensemble des dispositions de la présente charte.

Article 4. Conditions d'utilisation des systèmes d'information

- Les règles relatives à l'utilisation professionnelle ou privée des SI du Ministère
- ❖ Les ressources dédiées à la communication électronique, mises à la disposition des utilisateurs par le Ministère de la santé, (supports physique de la communication, usage des services Internet, usage du réseau, ...) sont destinés à l'activité professionnelle des utilisateurs qui est encadrée par les textes spécifiant les missions et les attributions des services du Ministère de la santé. Toutefois, ces ressources peuvent être utilisés dans le cadre d'un usage privé à condition que cet usage soit: non lucrative, raisonnable, limité et sans nuisance à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.
- ❖ Les données à caractère privé doivent être explicitement désignées par l'utilisateur comme relevant de sa vie privée (en attribuant des noms aux dossiers permettant de les reconnaître ou à travers le recours à la sécurisation par mot de passe,...). Ainsi, il appartient à l'utilisateur de mettre ces données dans un espace de stockage prévu explicitement à cet effet ou en mentionnant le caractère privé sur les fichiers. La sauvegarde et la protection régulière de ces données incomberont à l'utilisateur et non pas à l'administration.
- Les règles relatives à la continuité de service
- ❖ Pour assurer la continuité de service, l'utilisateur doit garantir l'accès à tout moment à ses données professionnelles. En cas d'absence non planifiée et pour des raisons exceptionnelles, si un utilisateur se trouve dans l'obligation de

communiquer ses codes d'accès au système d'information, il doit procéder dès que possible au changement de ces derniers ou en demander la modification à l'administrateur.

- ❖ Dans l'objectif d'assurer cette continuité, l'administration encourage les utilisateurs à utiliser une adresse mails professionnels et les espaces partagés mis à sa disposition, pour les activités liées à sa fonction, et dans la mesure du possible.

- **L'utilisation conforme aux lois en vigueur**

- *Respect de la propriété intellectuelle*

Le Ministère de la santé rappelle que l'utilisation des moyens informatiques implique le respect des droits de la propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits. En conséquence, chaque utilisateur doit :

- Utiliser les logiciels dans les conditions des licences souscrites ;
- Ne pas reproduire, copier, diffuser, modifier, adapter ou utiliser les logiciels, bases de données, pages Web, textes, images, photographies ou autres créations protégées par la loi, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits ;
- Respecter le droit des marques ;
- Ne pas procéder au téléchargement des œuvres protégées par la loi relative aux droits d'auteur.

L'utilisateur engage, donc, sa responsabilité en cas de non respect de ces dispositions ou des dispositions des textes législatifs et réglementaires en vigueur.

- *Respect des textes de loi relatifs à la protection des personnes physiques à l'égard de traitement des données à caractère personnel*

- ❖ Tout utilisateur des systèmes d'information est informé, à travers cette charte, de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément aux dispositions de la loi relative à la protection des personnes physiques à l'égard de traitement des données à caractère personnel et ses décrets d'application.
- ❖ Conformément aux dispositions de cette loi, chaque utilisateur disposera d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'information. Ce droit s'exerce auprès du responsable du traitement.

- *Respect de la vie privée*

- ❖ Le droit à la vie privée, le droit à l'image et le droit de représentation implique qu'aucune image ou information relative à la vie privée d'autrui ne doit être mise en ligne sans un consentement de la personne intéressée ou sauf dans les cas prévus par un texte législatif ou réglementaire.

- *Respect de secret professionnel*

- ❖ Les ressources documentaires électroniques produites par les fonctionnaires du ministère sont également soumises à des conditions d'utilisation très strictes qui seront établies par le Ministère de la santé dans des guides spécifiques. En effet, cet usage n'est autorisé que dans le cas d'un usage raisonnable et limitatif autorisé, d'usage personnel autorisé et strictement non commercial (interdiction de distribuer des copies papier ou de diffuser des versions numériques à toute personne extérieure au ministère, même à titre gratuit).

- *Responsabilité en matière de transmission d'informations*

Dans l'objectif d'assurer une utilisation rationnelle des systèmes d'information du ministère, l'utilisateur devra, principalement, veiller à :

- ❖ Ne pas diffuser, en utilisant les ressources informatiques mises à sa disposition, des messages diffamatoires ou injurieux (ces faits sont répréhensibles quel que soit leur mode de diffusion, public ou privé) ;
- ❖ Ne pas exploiter les ressources informatiques mises à sa disposition pour diffuser certaines formes d'apologie (crime, racisme, négationnisme, crimes de guerre, ...)
- ❖ A ne pas utiliser les ressources informatiques mises à sa disposition pour toute forme de provocation et de haine raciale ;
- ❖ A ne pas diffuser des informations confidentielles sans autorisation préalable d'une personne habilitée.

Article 5. La sécurité des systèmes d'information

- *Règles de sécurité applicables*

Le Ministère de la santé met en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition de l'ensemble des utilisateurs.

En particulier tout utilisateur du système d'information du Ministère de la santé doit être référencé dans les bases de référence du ministère et avoir obtenu une autorisation d'accès aux systèmes d'information, c'est à dire les codes d'accès "authentifiant et mot de passe", qui lui sont personnels et confidentiels.

L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité permettant de protéger les données et les outils auxquels il a accès de toute utilisation malveillante ou abusive. Cette mesure ne confère pas pour autant un caractère personnel à ces données ou outils. Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité des systèmes d'information impose à l'utilisateur de :

- ❖ respecter les consignes de sécurité, notamment :
 - Ne pas accéder aux données d'un autre utilisateur sans l'autorisation de celui-ci ;
 - Ne pas modifier ou détruire des informations ne lui appartenant pas ;
 - Respecter les règles relatives à la gestion des mots de passe et choisir des mots de passe difficiles à deviner, les changer périodiquement et ne pas les communiquer à des tiers,
 - L'utilisateur ne doit pas désactiver le logiciel anti-virus ;
 - Ne pas laisser à disposition des supports informatiques (clé USB, CD..) contenant des données confidentielles dans un bureau ouvert ;
 - Le propriétaire des PC portables du Ministère de la Santé s'engage, quel que soit l'endroit où il se trouve, à sécuriser son matériel et l'accès aux données qu'il contient
 - Doit rester vigilant lors de l'utilisation des ressources informatiques du Ministère en dehors de ses locaux ;
 - Ne jamais ouvrir un message contenant un texte ou un fichier suspect
 - Éteindre le poste à travers le bouton « démarrer-arrêter » et non par interrupteur pour terminer proprement ses sessions.
- ❖ garder strictement confidentiels son (ou ses) mot(s) de passe et ne pas le(s) dévoiler à un tiers ;
- ❖ respecter la gestion des accès, en particulier ne pas utiliser les noms et mots de passe d'un autre utilisateur, ni chercher à les connaître en utilisant des logiciels ou d'autres moyens technologique dédiés à cette fin;
- ❖ protéger son certificat électronique (s'il en dispose) par un mot de passe sûr gardé secret.

Comme la signature manuscrite, le certificat électronique est strictement personnel et l'utilisateur s'engage à n'autoriser personne à en faire usage à sa place.

Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouve dans l'obligation de communiquer son mot de passe, il ne doit le faire qu'avec l'accord de son supérieur hiérarchique et il devrait procéder, dès que possible, au changement de ce dernier ou en demander la modification à l'administrateur. Le bénéficiaire de la communication du mot de passe ne peut le communiquer à son tour à un tiers, ni l'utiliser en dehors de la circonstance exceptionnelle qui lui a fait bénéficier de ce mot de passe.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions :

- *de la part du Ministère de la santé:*
- ❖ veiller à ce que les ressources sensibles, qui sont sous son contrôle, ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation

de la continuité du service mises en place par la Charte des utilisateurs concernant l'usage du système d'information du Ministère de la Santé;

- ❖ limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;
- ❖ ne pas autoriser les redirections de messagerie pour les adresses de fonctions dans la mesure où le système d'information est accessible (après authentification) tant du réseau du ministère que de l'extérieur.

o de la part de l'utilisateur :

- ❖ s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information et aux communications entre tiers pour lesquelles il n'a pas reçu d'habilitation explicite
- ❖ ne pas utiliser les services qui lui sont offerts pour proposer ou rendre accessibles à des tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- ❖ ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par le Ministère de la santé. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Elles peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation de l'activité professionnelle qui l'a justifiée ;
- ❖ ne pas installer, télécharger ou utiliser sur le matériel connecté au réseau du Ministère de la santé, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de la Division de l'Informatique et des Méthodes;
- ❖ ne pas déposer des données sur un serveur interne ou ouvert au grand public ou sur le poste de travail d'un autre utilisateur sans y être autorisé par les responsables habilités ;
- ❖ ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels. Tout travail, risquant de conduire à la violation de cette règle, ne pourra être accompli qu'avec l'autorisation des responsables de la sécurité du système d'information du ministère et dans le strict respect des règles qui auront alors été définies ;
- ❖ se conformer aux dispositifs mis en place par le ministère pour lutter contre les virus et les attaques par programmes informatiques,
- ❖ assurer la protection de ses informations et plus particulièrement celles considérées comme sensibles, en utilisant différents moyens de sauvegarde individuels ou mis à sa disposition. En particulier, l'utilisateur ne doit pas transporter sans protection (telle qu'un chiffrement) des données sensibles sur des supports non fiables tels que ordinateurs portables, clés USB, disques externes, etc.
- ❖ ne pas quitter son poste de travail ni ceux en libre service en laissant des ressources ou services accessibles.

• Devoirs de signalement et d'information

L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, etc. Il signale également aux Responsables de la sécurité des systèmes d'information (RSSI) au niveau de la Division de l'informatique et des Méthodes toute possibilité d'accès à une ressource qui ne corresponde pas à son habilitation.

- Mesures de contrôle de la sécurité

L'utilisateur est informé :

- ❖ que pour effectuer la maintenance corrective, curative ou évolutive, le Ministère de la santé se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- ❖ qu'une maintenance à distance est précédée d'une information de l'utilisateur ;
- ❖ que toute information bloquante ou présentant une difficulté technique d'acheminement à son destinataire, peut être isolée, le cas échéant supprimée.

Le Ministère de la santé informe l'utilisateur que le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.

Les personnels en charge des opérations de contrôle sont soumis au secret professionnel. Ils ne peuvent donc pas divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction dès lors que :

- ❖ ces informations sont couvertes par le secret des correspondances ou, qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur ;
- ❖ elles ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité ;

- Informatisation du Système d'information

Tout développement informatique concerne le système d'information, en interne ou dans le cadre d'un infogérance globale ou partielle, doit s'effectuer en concertation avec la Division de l'Informatique et des Méthodes.

Toute acquisition de logiciel ou progiciel doit s'effectuer en concertation avec la Division de l'Informatique et des Méthodes.

Article 6. Communications électroniques

- Les services de la messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail et de mutualisation de l'information au sein du Ministère de la Santé.

La messagerie est un outil de travail ouvert à des usages professionnels; elle peut constituer le support d'une communication privée telle que définie par la loi. A cette fin, le ministère recommande l'utilisation d'adresses de messagerie privée.

L'usage de la messagerie professionnelle est soumis aux règles suivantes :

- L'utilisation des services de la messagerie doit être rationnelle et loyale. L'utilisateur doit éviter le risque de saturation des boîtes aux lettres en évitant de joindre des documents trop volumineux et utilisant les outils de compression.
- Le Ministère peut interrompre l'accès à la messagerie en cas d'utilisation non conforme.
- Le Ministère se réserve le droit d'accéder à des informations nécessaires à l'administration du système de messagerie et peut entreprendre les mesures d'urgence nécessaires au bon fonctionnement du service.
- L'utilisateur ne doit pas utiliser les données de l'annuaire de la messagerie sauf pour des besoins professionnels.
- L'utilisateur ne doit pas communiquer son adresse e-mail sur des sites web sauf pour des besoins professionnels.
- en cas d'absence d'un utilisateur, les demandes de changement de ses codes d'accès se font après accord des supérieurs hiérarchiques de l'intéressé

❖ Adresses électroniques

L'adresse électronique nominative est attribuée à un utilisateur qui la gère sous sa responsabilité.

L'utilisation d'une adresse électronique, fonctionnelle ou organisationnelle, est fortement conseillée pour un utilisateur ou un groupe d'utilisateurs.

❖ Contenu des messages électroniques

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place et qui seront portées à la connaissance des utilisateurs. Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé. Dans ce cas et afin de lui conserver son caractère privé, l'utilisateur doit le déposer dans un dossier identifiable comme « personnel ».

❖ Emission et réception des messages

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

❖ Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par dispositions de la loi relative à l'échange électronique de données juridiques.

L'utilisateur doit en conséquence être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

❖ *Stockage et archivage des messages*

Chaque utilisateur doit organiser et mettre en oeuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou utiles en tant qu'éléments de preuve.

À ce titre, il doit notamment se conformer aux règles définies dans la présente charte et tout autre document élaboré par les services concernés pour encadrer les échanges entre les utilisateurs.

• *Les services de l'Internet*

Il est rappelé que l'Internet est soumis à l'ensemble des règles imposées par les textes législatifs et réglementaires en vigueur sur le territoire national.

❖ *La publication sur les sites Internet et Intranet du Ministère de la Santé.*

Toute publication de pages d'informations ou de documents sur les sites Internet ou Intranet du Ministère doit être validée par la Division de Communication ou un responsable de publication nommément désigné.

Aucune publication de pages d'information (ou documents) à caractère privé sur les ressources du système d'information du Ministère n'est autorisée, sauf disposition particulière précisée dans une documentation établie par le ministère.

❖ *La sécurité*

Le Ministère de la Santé se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par le Ministère. Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans la documentation établie par le service ou le responsable concerné.

L'utilisateur doit être informé des risques et limites inhérents à l'utilisation d'Internet par messagerie ou par le biais d'actions de formations ou de campagnes de sensibilisation.

❖ *Les téléchargements*

Tout téléchargement de fichiers, notamment de sons ou d'images, sur le réseau Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis par la loi relative aux droits d'auteurs et droits voisins.

Le Ministère de la Santé se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus, code malicieux, programmes espions ...).

À l'inverse, l'utilisation du réseau pour l'offre d'un service disponible depuis l'Internet doit être rationnelle de manière à éviter toute consommation abusive ;

notamment toute mise en service d'un serveur doit être déclarée, ne serait ce que pour en autoriser l'accès depuis l'extérieur du réseau du Ministère. L'offre de sons, d'images, de vidéos, de logiciels et tous autres documents doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis par la loi relative aux droits d'auteurs et droits voisins et être en rapport avec les missions du Ministère.

❖ *La traçabilité*

Le Ministère de la Santé se garde le droit de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées. Ainsi que des outils de traçabilité sur tous les systèmes d'information.

❖ *L'hébergement des sites ou applications web*

Tout hébergement de site ou application web, en intra ou extra du Ministère, doit s'effectuer en concertation avec la Division de l'Informatique et des Méthodes.

Article 7. Les limitations des usages

En cas de non respect des règles définies dans la présente charte, les responsables informatiques du ministre pourront, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extraprofessionnelles, est passible de sanctions.

Article 8. Entrée en vigueur de la charte

La présente charte entrera en vigueur dès sa diffusion et sa notification à l'ensemble du personnel du Ministère de la Santé. En plus de respect des dispositions de cette charte, l'utilisateur des systèmes d'information du Ministère doit également veiller sur le respect des textes législatifs et réglementaires en vigueur en la matière.