

# Charte informatique de l'Assurance Maladie

Charte informatique - Novembre 2019

RESTREINT

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br><b>Ssi</b><br>Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 2 sur 19</b>  |

## Table des matières

|   |           |
|---|-----------|
| <b><u>1. PREAMBULE</u></b>  | <b>4</b>  |
| <b><u>2. CHAMP D'APPLICATION DE LA CHARTE</u></b>   | <b>4</b>  |
| <b><u>2.1. PERSONNES CONCERNÉES</u></b>   | <b>5</b>  |
| <b><u>2.2. DIFFUSION</u></b>  | <b>5</b>  |
| <b><u>3. REGLES D'UTILISATION DU SYSTEME D'INFORMATION</u></b>  | <b>6</b>  |
| <b><u>3.1. REGLES GENERALES</u></b>   | <b>6</b>  |
| <b><u>3.2. UTILISATION PRIVEE RESIDUELLE ET NOMMAGE DES DONNEES PRIVEES</u></b>   | <b>6</b>  |
| <b><u>3.3. DROITS D'ACCES AUX DONNEES</u></b>   | <b>7</b>  |
| <b><u>4. ATTRIBUTION ET RETRAIT DU DROIT D'ACCES AU SYSTEME D'INFORMATION</u></b>   | <b>8</b>  |
| <b><u>4.1. ATTRIBUTION</u></b>  | <b>8</b>  |
| <b><u>4.2. GESTION DES ABSENCES</u></b>   | <b>8</b>  |
| <b><u>4.3. GESTION DES DEPARTS</u></b>  | <b>9</b>  |
| <b><u>5. LA PROTECTION DU SYSTEME D'INFORMATION</u></b>   | <b>9</b>  |
| <b><u>5.1. PROTECTION DES RESSOURCES ET DES INFORMATIONS</u></b>  | <b>9</b>  |
| <b><u>5.2. VIRUS INFORMATIQUES ET AUTRES EVENEMENTS MALVEILLANTS</u></b>  | <b>9</b>  |
| <b><u>5.3. UTILISATION DES SUPPORTS AMOVIBLES</u></b>   | <b>10</b> |
| <b><u>5.4. CHIFFREMENT</u></b>  | <b>11</b> |
| <b><u>6. UTILISATION DES MOYENS DE COMMUNICATION, OUTILS COLLABORATIFS, INTRANET, INTERNET</u></b>  | <b>12</b> |
| <b><u>6.1. LES OUTILS COLLABORATIFS (MESSAGERIE, ESPACES COLLABORATIFS, RESEAUX SOCIAUX D'ENTREPRISE, MESSAGERIE INSTANTANEE, SMARTPHONES, ...)</u></b> | <b>12</b> |
| <b><u>6.2. INTRANET</u></b>   | <b>12</b> |
| <b><u>6.3. INTERNET</u></b>   | <b>12</b> |
| <b><u>7. MOBILITE ET MATERIELS MIS A DISPOSITION PAR L'ORGANISME</u></b>  | <b>14</b> |
| <b><u>8. LES OBJETS CONNECTES</u></b>   | <b>15</b> |

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>Ssi Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 3 sur 19</b>  |

|  |                  |
|--|------------------|
| <b><u>9. DONNEES PERSONNELLES</u></b>  | <b><u>15</u></b> |
| <b><u>10. PROPRIETE INTELLECTUELLE</u></b>   | <b><u>16</u></b> |
| <b><u>11. ANALYSE ET CONTROLE DE L'UTILISATION DES RESSOURCES DU SYSTEME D'INFORMATION</u></b> | <b><u>16</u></b> |
| <b><u>11.1. PRINCIPE DIRECTEUR</u></b>   | <b><u>16</u></b> |
| <b><u>11.2. ACTIONS DES ADMINISTRATEURS DU SYSTEME D'INFORMATION</u></b>                       | <b><u>16</u></b> |
| <b><u>12. SAUVEGARDE ET ARCHIVAGE</u></b>  | <b><u>16</u></b> |
| <b><u>12.1. DONNEES GENERALES</u></b>  | <b><u>16</u></b> |
| <b><u>12.2. DONNEES TECHNIQUES</u></b>   | <b><u>17</u></b> |
| <b><u>12.3. ARCHIVAGE ET DESTRUCTION</u></b>   | <b><u>17</u></b> |
| <b><u>13. CONTROLE DE L'APPLICATION DE LA CHARTE</u></b>                                       | <b><u>17</u></b> |
| <b><u>14. JOURNAUX D'EVENTEMENTS</u></b>   | <b><u>18</u></b> |
| <b><u>15. SANCTIONS</u></b>  | <b><u>18</u></b> |
| <b><u>16. DISPOSITIONS SPECIFIQUES LIEES AUX ORGANISATIONS SYNDICALES</u></b>                  | <b><u>18</u></b> |
| <b><u>17. SUIVI DE LA MISE EN APPLICATION DE LA CHARTRE</u></b>                                | <b><u>18</u></b> |
| <b><u>18. ENTREE EN VIGUEUR</u></b>  | <b><u>18</u></b> |

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>SSI Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 4 sur 19</b>  |

## 1. Préambule

L'organisme met à la disposition des utilisateurs, dans le cadre de leur activité professionnelle, des ressources informatiques et de communication électronique, dont l'usage est source de responsabilité.

Il est important de rappeler que le statut des personnels de l'organisme ne protège en aucune manière l'utilisateur d'une mise en cause de sa responsabilité civile ou pénale en cas d'utilisation illicite de ces moyens.

Compte tenu de la présomption de caractère professionnel des données présentes sur le poste de travail, la présente charte vise à informer et sensibiliser chaque salarié de l'Assurance Maladie sur ses droits et obligations dans l'usage des Technologies et l'Information et la Communication (TIC).

L'usage correct des ressources informatiques et de communication électronique permet de garantir l'intégrité et la disponibilité du système d'information pour une utilisation conforme à son objet.

Il participe au respect du secret professionnel (et/ou médical) et de la confidentialité des données. Enfin, il permet de préserver l'image de marque de l'organisme en évitant de porter atteinte à sa réputation.

## 2. Champ d'application de la charte

La présente charte s'applique à l'outil professionnel que constitue le Système d'Information de l'organisme et à l'infrastructure associée. L'organisme est responsable de toutes les ressources mises à disposition des utilisateurs :

- les équipements informatiques (stations de travail, ordinateurs portables, serveurs, équipements réseaux,...),
- les logiciels et leurs mises à jour conformes aux préconisations CNAM et répondant aux exigences de sécurité,
- les moyens de communication (téléphone, smartphone, messageries électronique et instantanée, Internet, Visio conférence, accès à distance tel que le télétravail, ...),
- les fichiers, informations, données...,
- les périphériques externes (Imprimantes, Scanner, Fax, les supports de stockage type clés USB, ...).

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>SSI Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 5 sur 19</b>  |

L'organisme doit en encadrer l'usage, notamment en cas de travail en dehors des locaux (télétravail, nomadisme) en restreignant ou interdisant l'accès aux données sensibles.

Cette charte veille au respect des règles du Système d'Information et des dispositions relatives à la protection des données dans et en dehors des locaux de l'organisme.

Toute ressource ou moyen de communication connecté au réseau de l'Assurance Maladie utilisé à des fins professionnelles mais appartenant aux utilisateurs est interdit, sauf dérogation expresse de la Direction après réalisation d'une analyse de risque.

## 2.1. Personnes concernées

Les obligations décrites dans la présente charte s'appliquent de droit aux utilisateurs de l'Assurance Maladie et assimilés mais aussi, à titre exceptionnel, aux tiers accédants qui doivent utiliser le système d'information mis à leur disposition.

- **Les utilisateurs** : Agents de l'assurance maladie amenés à créer, consulter, modifier et/ou mettre en œuvre les ressources informatiques et de communication électronique.
- **Les personnels assimilés** : personnes en situation de mise à disposition ou détachement dans l'Assurance Maladie.
- **Les administrateurs** : Agents de l'assurance Maladie pour lesquels il convient de se référer aux conditions d'utilisation des droits administrateur imposés par le Système d'information de l'Assurance Maladie.

A titre exceptionnel, les tiers d'entités extérieures à l'organisme (prestataires notamment) qui peuvent avoir accès aux ressources informatiques et de communication électronique ou traiter des informations extraites du système d'information.

## 2.2. Diffusion

La diffusion de la charte sera réalisée par voie de note de service après modification du Règlement Intérieur pour ce qui concerne les organismes du réseau.

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 6 sur 19</b>  |

### 3. Règles d'utilisation du système d'information

#### 3.1. Règles générales

Les ressources informatiques et moyens de communication électronique mis à disposition des utilisateurs doivent être utilisés dans la stricte application de la charte. Toute modification de la ressource ou d'un élément du SI ne peut être réalisée que par du personnel habilité.

Les utilisateurs du SI doivent être vigilants par rapport à la sécurisation des équipements qui leur sont confiés. L'utilisation des ressources informatiques et des moyens de communication électronique est limitée à un usage professionnel.

#### 3.2. Utilisation privée résiduelle et nommage des données privées

L'utilisation des moyens de communication électroniques (messagerie et Internet) à titre privé est tolérée dans le cadre d'un usage raisonnable.

L'utilisateur doit supprimer toute mention relative à l'employeur (signature de mail...) ou indication qui pourrait laisser croire que le message est rédigé dans le cadre de son exercice professionnel au nom de son employeur. De même il doit s'abstenir de tout commentaire de nature à porter atteinte à la vie privée ou à la réputation d'une personne physique ou morale, y compris de l'employeur.

Un employé a le droit, même au travail, au respect de sa vie privée et au secret de ses correspondances privées.

Un employeur ne peut pas librement consulter les courriels personnels de ses employés, même s'il a interdit d'utiliser les outils de l'entreprise à des fins personnelles.

Les messages personnels doivent être identifiés comme tels, par exemple :

- en précisant dans leur objet « Personnel » ou « Privé »,
- en les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

Les courriers ne seront pas considérés comme personnels du simple fait de leur classement dans le répertoire « mes documents » ou dans un dossier identifié par les initiales de l'employé.

L'Organisme se réserve la possibilité de se retourner contre l'utilisateur si sa responsabilité venait à être engagée.

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>SSI Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 7 sur 19</b>  |

Sauf autorisation expresse de la direction, la participation au nom de l'employeur à un service de type communautaire, en particulier forums, réseaux sociaux... est interdite.

L'utilisateur peut stocker des données privées dans un répertoire nommé « PERSONNEL » ou « PRIVE » en veillant toutefois à ce que la taille du dossier reste dans les limites d'une volumétrie raisonnable et qu'il ne comporte pas de données professionnelles.

En cas d'abus, l'organisme se réserve le droit de prendre toute sanction appropriée.

### 3.3. Droits d'accès aux données

Les dossiers, fichiers y compris sur supports amovibles (même personnels qui par ailleurs ne sont pas autorisés) créés par un salarié grâce à l'ordinateur mis à sa disposition par son employeur pour l'exécution de son contrat de travail sont présumés avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors de sa présence, sauf si le salarié les a identifiés comme étant personnels.

L'employeur n'est autorisé à accéder aux fichiers personnels de ses salariés qu'en sa présence ou par une décision de justice ou par une autorité habilitée (police, gendarmerie, douanes, Cnil, Direction générale de la concurrence, de la consommation et de la répression des fraudes, etc.) ou en présence d'un risque avéré en termes notamment de sécurité, de continuité de service, d'un risque grave de voir sa responsabilité engagée, ou en cas de suspicion d'acte malveillant pouvant impacter le SI. Les modalités et les circonstances d'accès ainsi que les données accédées sont notifiées par écrit au salarié.

Par défaut, les fichiers ont un caractère professionnel et l'employeur peut y accéder librement. Lorsque les fichiers sont identifiés comme « personnels » ou « privés », l'employeur peut y accéder :

- en présence de l'employé ou après l'avoir informé,
- en cas de risque ou évènement particulier, qu'il appartient aux juridictions d'apprecier.

Les courriels adressés ou reçus par le salarié à l'aide de l'outil informatique mis à sa disposition par l'employeur pour les besoins de son travail sont présumés avoir un caractère professionnel en sorte que l'employeur est en droit de les ouvrir hors la présence de l'intéressé sauf s'ils sont identifiés comme personnels.

Les conditions d'accès par l'employeur à la messagerie électronique professionnelle des agents sont précisées dans la Charte de messagerie.

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>SSI Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 8 sur 19</b>  |

## 4. Attribution et retrait du droit d'accès au système d'information

### 4.1. Attribution

Chaque utilisateur reçoit un droit d'accès individuel, personnel et confidentiel qui se matérialise par un ou plusieurs moyen(s) d'authentification (identifiant, mot de passe, carte avec ou sans code PIN) qui ne doit(vent) pas être communiqué(s).

La carte agent doit faire l'objet d'une attention particulière dans le cadre de l'activité professionnelle.

A ce titre, elle ne doit donc pas être prêtée à un tiers, même appartenant au personnel de l'organisme, et elle doit être systématiquement enlevée du lecteur en cas d'absence, même momentanée.

L'utilisateur s'engage à respecter la politique de gestion des mots de passe (changement régulier, complexité...) énoncée au niveau national.

Celui-ci devra donc signaler à son responsable la perte ou le vol de sa carte de même que tout événement faisant suspecter un usage frauduleux, afin de dégager sa responsabilité.

La protection de ces moyens est placée sous la responsabilité de l'utilisateur, qui reconnaît que l'usage de son droit d'accès peut engager sa responsabilité.

L'identifiant est strictement confidentiel. Cela emporte pour conséquence que l'accès aux ressources informatiques et de communication électronique via cet identifiant est réputé avoir été réalisé par le titulaire, qui devra donc assumer la responsabilité d'usage non conforme, sauf à démontrer avoir demandé, préalablement, une suspension ou une suppression de son droit d'accès.

L'utilisateur ne doit accéder qu'aux seules informations nécessaires à son activité professionnelle au titre du «besoin d'en connaître».

Il est interdit d'user, par quelque moyen que ce soit, de l'identité et du droit d'accès d'un autre utilisateur.

### 4.2. Gestion des absences

En cas d'absence prolongée, l'organisme « suspend » le droit d'usage et/ou d'accès d'un utilisateur. Pour des raisons de service, la Direction de l'organisme se réserve le droit d'accéder directement aux fichiers et/ou messages professionnels (cf. Modalités d'accès aux données au §3.3).

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>SSI Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | Page <b>9</b> sur <b>19</b>   |

## 4.3. Gestion des départs

Au moment de son départ de l'organisme, il appartient à l'utilisateur de :

- détruire son répertoire « PERSONNEL » et tous les messages de nature privée,
- restituer l'ensemble des informations professionnelles, des moyens d'accès informatiques et de communications électroniques, y compris les matériels nomades, selon la procédure nationale de sortie du personnel.

A son départ, l'utilisateur perd tout droit d'accès au système d'information.

## 5. La protection du système d'information

### 5.1. Protection des ressources et des informations

L'utilisateur doit systématiquement verrouiller son poste de travail en cas d'absence, même momentanée.

Les utilisateurs doivent signaler tout incident de sécurité, toute suspicion de compromission d'une information, toute tentative d'intrusion extérieure sur le SI, de falsification, d'usurpation de droit ou de présence de virus selon les modalités décrites dans la procédure nationale de gestion des incidents de sécurité.

L'utilisateur ne doit pas, sauf autorisation préalable de la Direction de l'organisme :

- communiquer à des tiers toute information du système d'information,
- modifier les configurations informatiques,
- déroger aux consignes d'utilisation des outils informatiques,
- désactiver ou contourner le dispositif technique de sécurité.

### 5.2. Virus informatiques et autres événements malveillants

Le poste de travail est équipé d'un logiciel antivirus et d'autres dispositifs de lutte contre la malveillance dont le paramétrage ne doit pas être modifié. De plus, son fonctionnement ne doit pas être entravé ou arrêté. L'utilisation des applications communicantes (navigateur Internet et messagerie en particulier) et des supports de stockage externes peut provoquer la transmission et l'installation, de programmes ou de fichiers, qui altèrent ou suppriment les données et logiciels du poste.

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 10 sur 19</b>   |

Si un utilisateur suspecte ou constate un dysfonctionnement de l'anti-virus sur son poste de travail, il doit cesser toute activité sur le poste et avertir le service informatique et le MSSI/RSSI de son organisme.

### 5.3. Utilisation des supports amovibles

Il existe de nombreux supports informatiques amovibles capables de se connecter aux ordinateurs : clés USB, CD-ROM, baladeurs numériques, mémoires flash, appareils photos, assistants personnels numériques, clés U3, téléphones, smart phones, tablettes...

Ces supports présentent un risque pour le système d'information car ils peuvent contenir des logiciels malveillants (virus, logiciels espions, logiciels de prise de contrôle à distance).

Par conséquent, la connexion de supports amovibles personnels à un poste de travail de l'Assurance Maladie est interdite.

Toutefois, l'utilisation de supports amovibles professionnels est tolérée sous certaines conditions :

- le support, de préférence sécurisé est fourni par l'organisme (ou par les circuits de la Diffusion Nationale), ou son utilisation a obtenu l'accord de la fonction sécurité de l'organisme (RSSI ou MSSI),
- le support apporté par un tiers doit être utilisé de façon exceptionnelle et avec la plus grande vigilance (un avis du MSSI / RSSI est recommandé).

#### Recommandations d'utilisation de supports amovibles :

- Faire un examen systématique à l'antivirus lors de l'utilisation d'un support amovible.
- Procéder au chiffrement des données sensibles au regard de la classification.
- Sauvegarder les documents nécessaires dans un espace sécurisé après chaque utilisation.
- Effacer les données et déconnecter le support du poste de travail, le support amovible ne doit servir qu'au transport des données.

Toute connexion de supports amovibles extérieurs à l'organisme sur le poste de travail est interdite.

Toutefois, si la connexion est indispensable pour des raisons de service, il convient de prendre les précautions complémentaires suivantes :

|   |   |  |
|---|---|--|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>SSI Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 11 sur 19</b>  |

- Ne jamais utiliser de support amovible dont l'origine ne peut être garanti.
- Ne pas double-cliquer sur les documents, mais les ouvrir à partir des logiciels de son poste de travail (par exemple : exécuter Word puis menu fichier/ouvrir un fichier Word sur la clé),
- Ne pas exécuter de logiciels situés sur le support (.exe, .jar, .bat etc.), et de manière générale ne pas double-cliquer sur des fichiers inconnus ni les importer sur le poste de travail.

Dans tous les cas il convient d'être prudent et vigilant, de signaler tout incident ou anomalie et de ne pas hésiter à se rapprocher du service informatique, ou du MSSI /RSSI de l'organisme pour connaître la conduite à tenir.

## 5.4. Chiffrement

La transmission en interne ou en externe de données sensibles (données classées « secret » et « confidentiel ») doit impérativement répondre aux préconisations des documents de référence portant sur la « Classification des informations ».

L'utilisation d'outils de chiffrement est encadrée par le service informatique et le MSSI de l'organisme dans le respect des préconisations de la CNAM.

Tout autre moyen de chiffrement est interdit, même s'il se trouve en libre accès sur internet.

Toutes précisions sur ces sujets peuvent être demandées au MSSI /RSSI.

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>SSI Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 12 sur 19</b>   |

## 6. Utilisation des moyens de communication, outils collaboratifs, intranet, internet

### 6.1. Les outils collaboratifs (messagerie, espaces collaboratifs, réseaux sociaux d'entreprise, messagerie instantanée, smartphones, ...)

Elle fait l'objet d'une charte spécifique qui définit les droits et obligations que l'organisme et l'utilisateur s'engagent à respecter, notamment les conditions de contrôles portant sur l'utilisation de la messagerie électronique ainsi que le cadre légal dans lequel s'inscrit son usage.

Elle précise les sanctions prévues en cas de non-respect des règles établies.

Elle est complétée d'un guide de bonnes pratiques auquel chaque utilisateur doit se référer.

### 6.2. Intranet

L'organisme met à la disposition de chaque agent un site Intranet avec les informations et services nécessaires à l'exercice de son activité (règlement intérieur, réglementation liée aux règlements des prestations, circulaires, modes opératoires, processus qualité, information assurés, SSI,...) et à la vie dans l'entreprise (projet d'entreprise, actualités, vacances de poste, réservation de salles en ligne...). Il s'agit d'un outil d'information et de travail.

Les responsabilités et les engagements de chaque agent avec l'Intranet sont les suivants :

- Seuls les documents classifiés « publics » peuvent être diffusés en externe.
- Les contributions à caractère diffamatoire, discriminatoire ou incorrect sont interdites.

### 6.3. Internet

L'Internet est un espace à risques dans lequel sont présentes de nombreuses sources de menaces pouvant porter atteinte à l'organisme mais également à la vie privée de l'utilisateur. La loi précise que « *la sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives* ».

L'obligation de protection de ses personnels pesant sur l'organisme justifie les règles de conduite et les interdictions édictées par la charte d'utilisation du système d'information.

L'accès à Internet est soumis à autorisation pour l'ensemble des utilisateurs.

Charte informatique - Novembre 2019

RESTREINT

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | Page 13 sur 19  |

La Direction du Système d'Information, s'autorise le droit d'opérer tout filtrage nécessaire pour protéger le système d'information, garantir la disponibilité du réseau informatique et respecter la législation en vigueur.

De par le droit du travail, l'utilisateur ne doit pas accomplir d'opérations susceptibles de représenter un manquement aux obligations professionnelles ou à la préservation des ressources informatiques mises à sa disposition comme :

- la consultation, l'importation, la diffusion et l'exploitation d'informations de nature à porter atteinte individuellement ou collectivement au respect de la personne humaine et de sa dignité, ainsi qu'à la protection des mineurs,
- le téléchargement, l'installation/exécution de scripts, de logiciels ou de programmes informatiques sans autorisation préalable de la Direction,
- la consultation, le téléchargement, la diffusion ou l'impression de données dont les volumes et/ou les fréquences d'usage risquent de mettre en danger l'intégrité et/ou la disponibilité du réseau,
- le téléchargement, la consultation ou la copie à partir d'un site illicite (sites à caractère pornographique, pédophile, négationniste, extrémiste, raciste, xénophobe, violent ou contraire aux bonnes mœurs ou à l'ordre public...) qui revêt le caractère d'une infraction pénale,
- la communication d'informations appartenant au patrimoine informationnel de l'Assurance Maladie sans autorisation préalable,
- le raccordement au poste de travail d'un matériel externe non professionnel ayant sa propre connectique à l'Internet (risque de rebond),
- la communication de l'adresse de messagerie professionnelle en dehors des sites Internet de confiance. Il est rappelé que les utilisateurs et les services des organismes de l'Assurance Maladie utilisent une adresse de type @assurance-maladie.fr (exemple: eric.dupont@assurance-maladie.fr), qui est une signature institutionnelle susceptible, dans les rapports avec les tiers, d'engager la responsabilité civile et pénale des organismes et de leurs représentants.

La reproduction d'objets issus de sites Internet, (textes, images, sons) n'est possible que dans la mesure où ils sont libres de droits et diffusés avec l'autorisation de leurs auteurs, et avec indication de leur source, conformément aux lois en vigueur.

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>SSI Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 14 sur 19</b>   |

En effet, en vertu des règles du Code de la propriété intellectuelle, l'auteur d'une œuvre de l'esprit originale jouit, sur cette œuvre, du seul fait de sa création, "d'un droit de propriété incorporel et exclusif opposable à tous".

La consultation de sites Internet, pour un motif personnel, est tolérée dans la mesure où celle-ci est exceptionnelle (sauf autorisation expresse et préalable de la Direction) et raisonnable et lorsque le contenu n'est contraire à aucune des prescriptions de cette charte.

Les connexions Internet font l'objet de surveillances, de vérifications et d'audits réguliers selon des directives définies au niveau national.

Les identifiants et les adresses de connexion sont ainsi enregistrés.

L'historique constitué permet de retracer le trafic Internet et peut être exploité par la Direction à des fins de statistiques, de qualité de service et de sécurité, pour vérifier :

- les durées de connexions,
- et les sites les plus visités.

Les traces seront conservées pendant une durée maximale de 6 mois, sauf si des dispositions légales ou réglementaires venaient à imposer des délais de conservation différents.

En cas d'utilisation illicite, non conforme aux règles fixées dans la présente charte ou non autorisée par la Direction de l'organisme, l'utilisateur s'expose à des poursuites disciplinaires, civiles et/ou pénales.

## 7. Mobilité et matériels mis à disposition par l'organisme

Tout utilisateur qui dispose de matériels nomades est informé des consignes de sécurité particulières lors de la mise à disposition de la ressource.

Seuls les matériels nomades autorisés peuvent être connectés au réseau de l'Assurance Maladie. L'attention de l'utilisateur est attirée sur le fait que l'utilisation de ces matériels nomades à l'extérieur de l'organisme engage sa responsabilité.

L'utilisation des matériels nomades impose donc à chacun un niveau de surveillance et de confidentialité renforcé.

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>SSI Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 15 sur 19</b>   |

## 8. Les objets connectés

Les objets connectés (montre, enceintes Bluetooth ...) présentent un risque pour le système d'information (virus, logiciels espions...). Ces objets connectés étant par nature peu protégés, ils permettent un accès au matériel auquel il est connecté.

Par conséquent, la connexion de ces supports personnels à un poste de travail de l'Assurance Maladie est interdite.

Toute Dérogation doit faire l'objet d'une autorisation expresse de la CNAM ou de la Direction de l'organisme.

## 9. Données personnelles

De par leur métier, les salariés et éventuels sous-traitants ont accès à des données personnelles et de santé.

Le respect du secret professionnel et du droit d'en connaître (accéder aux données strictement nécessaires à la mission confiée) s'applique, et plus généralement toutes les dispositions relatives à la protection des données.

### Définition d'une donnée à caractère personnel :

Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

### Définition de données de santé :

Toutes données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.

Les données médico-administratives sont désormais considérées comme données de santé.

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>SSI Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 16 sur 19</b>   |

## 10. Propriété intellectuelle

L'utilisation du système d'information de l'organisme implique le respect des droits de propriété intellectuelle et notamment de la réglementation relative à la propriété littéraire et artistique.

## 11. Analyse et contrôle de l'utilisation des ressources du système d'information

### 11.1. Principe directeur

L'organisme doit s'assurer du bon fonctionnement du système d'information et empêcher son utilisation dans un cadre non conforme aux règles définies dans la présente Charte.

### 11.2. Actions des administrateurs du système d'information

Les administrateurs sont nommément désignés et assurent le bon fonctionnement des moyens informatiques de l'organisme.

Les administrateurs sont tenus au secret professionnel concernant toute information confidentielle qu'ils pourraient être amenés à consulter et tout particulièrement celles couvertes par le secret de la correspondance privée.

Ils ne contournent pas les procédures de sécurité établies, et en particulier ne désactivent pas de leur propre initiative les mécanismes de traçabilité, et ne portent pas atteinte à l'intégrité des fichiers de journalisation.

Aucune exploitation à des fins autres que celles découlant de leur mission ne saurait être opérée et tolérée.

## 12. Sauvegarde et archivage

### 12.1. Données générales

L'utilisateur doit stocker ses fichiers et données électroniques dans des espaces définis par le service informatique.

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | Page 17 sur 19  |

La sauvegarde des données locales résidantes sur le disque dur du poste de travail est à la charge de l'utilisateur. Des moyens d'archivage locaux peuvent être mis à disposition à cette fin par l'organisme.

La sauvegarde des données déposées sur les serveurs est à la charge du service informatique. Les données à caractère personnel ne doivent pas être conservées sur le poste de travail.

Un stockage sur un serveur partagé interne est à privilégier.

Des dispositions spécifiques au service médical sont à appliquer (serveur sécurisé dédié).

## 12.2. Données techniques

Les données de connexion (statistiques, Internet, serveurs, applications, etc.) sont conservées pendant 6 mois.

## 12.3. Archivage et destruction

L'archivage des données est effectué conformément à la réglementation applicable ainsi qu'aux préconisations de la « classification des informations ».

Les données sont détruites lorsque le besoin de conservation de l'information n'est plus exprimé.

## 13. Contrôle de l'application de la charte

L'organisme doit pour des nécessités de maintenance et de sécurité, procéder périodiquement, par les moyens les plus appropriés, à des audits de contrôle de la bonne application de la présente charte, dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.

Les audits peuvent viser le contrôle de tout ou partie de la présente charte.

Dans le cas d'identification d'axes d'amélioration, des plans d'actions correctifs doivent être mis en place.

|   |   |   |
|---|---|---|
|  | <b>Politique de Sécurité du Système d'Information</b> | <br>Ssi Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 18 sur 19</b>   |

## 14. Journaux d'évènements

Tout accès et utilisation du système d'information génère automatiquement une trace collectée dans des journaux d'événements qui sont confidentiels et accessibles uniquement aux personnels habilités ainsi qu'à la Direction de l'organisme.

Cette collecte participe à la garantie d'un bon fonctionnement et d'une utilisation normale des ressources du système d'information et le cas échéant permet l'identification d'usages illégitimes.

## 15. Sanctions

Les sanctions prévues à la convention collective ou à toute autre disposition conventionnelle ou réglementaire existante dans l'organisme sont applicables en cas de non-respect de la présente charte.

## 16. Dispositions spécifiques liées aux organisations syndicales

La mise à disposition des organisations syndicales qui le souhaitent d'un espace dédié relève de la négociation locale.

## 17. Suivi de la mise en application de la Charte

La Direction se charge du respect de la Charte et de son suivi.

Toute difficulté d'application de la Charte doit être signalée au MSSI/RSSI.

Toute question spécifique relative aux données personnelles peut être soumise au Délégué à la Protection des Données (D.P.O.) de l'organisme.

## 18. Entrée en vigueur

Cette charte fait l'objet d'une publication auprès de l'Inspection du Travail.

Elle entre en vigueur un mois après l'accomplissement des formalités de communication à l'Inspection du travail, de dépôt et de publicité telles que prévues à l'article L 1321 4 du code du travail.

|   |   |   |
|---|---|---|
| <br>l'Assurance<br>Maladie<br>Caisse Nationale | <b>Politique de Sécurité du Système d'Information</b> |  Ssi<br>Sécurité du système d'information |
|   | <b>Charte informatique</b>                            | <b>Page 19 sur 19</b>   |

Toute modification ultérieure, adjonction ou retrait de clause de la présente charte sera soumis à la même procédure, conformément aux prescriptions de l'article L 1321-4 du code du travail, étant entendu que toute clause de la charte qui deviendrait contraire aux dispositions légales, réglementaires ou conventionnelles applicables à l'organisme du fait de l'évolution de ces dernières, serait nulle de plein droit.

Chaque personnel de l'Assurance Maladie et assimilé en est destinataire et doit s'engager à en prendre connaissance et à en respecter les termes.

De même, la charte devra être diffusée aux tiers qui se verront doté d'un accès au Système d'information et qui s'engageront à la respecter.