

Charte d'Utilisation des Ressources Informatiques

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 1 / 17

0. DEFINITIONS	2
1. PREAMBULE	2
2. CHAMP D'APPLICATION DE LA CHARTE	2
2.1. PERSONNES CONCERNEES	3
2.2. DIFFUSION	3
2.3. MISE A JOUR	3
3. REGLES D'UTILISATION DU SYSTEME D'INFORMATION	3
3.1. DISPOSITIONS REGLEMENTAIRES	3
3.2. REGLES GENERALES	4
3.3. UTILISATION PRIVEE RESIDUELLE ET NOMMAGE DES DONNEES PRIVEES	4
3.4. DROITS D'ACCES AUX DONNEES	5
4. ATTRIBUTION ET RETRAITS DU DROIT D'ACCES AU SYSTEME D'INFORMATION	6
4.1. ATTRIBUTION.....	6
4.2. GESTION DES ABSENCES	6
4.3. GESTION DES DEPARTS.....	7
5. LA PROTECTION DU SYSTEME D'INFORMATION.....	7
5.1. PROTECTION DES RESSOURCES ET DES INFORMATIONS	7
5.2. VIRUS INFORMATIQUES ET AUTRES EVENEMENTS MALVEILLANTS	8
5.3. UTILISATION DES SUPPORTS AMOVIBLES	8
5.4. CHIFFREMENT	9
6. UTILISATION DES MOYENS DE COMMUNICATION MESSAGERIE, INTRANET, INTERNET	9
6.1. LA MESSAGERIE	9
6.2. INTRANET	9
6.3. INTERNET.....	9
7. MOBILITE ET MATERIELS MIS A DISPOSITION PAR L'ORGANISME	11
8. DONNEES NOMINATIVES	11
9. PROPRIETE INTELLECTUELLE	12
10. ANALYSE ET CONTROLE DE L'UTILISATION DES RESSOURCES DU SYSTEME D'INFORMATION	13
10.1. PRINCIPE DIRECTEUR	13
10.2. ROLE DES ADMINISTRATEURS DU SYSTEME D'INFORMATION	13
10.3. ROLE DU MANAGER DE LA SECURITE DES SYSTEMES D'INFORMATION	13
10.4. CONTROLE DE L'UTILISATION DES RESSOURCES	14
11. SAUVEGARDE ET ARCHIVAGE.....	14
11.1. DONNEES GENERALES	14
11.2. ARCHIVAGE ET DESTRUCTION	15
12. CONTROLE DE L'APPLICATION DE LA CHARTE	15
13. JOURNAUX D'EVENEMENTS.....	15
14. SANCTIONS.....	15
15. DISPOSITIONS SPECIFIQUES LIEES AUX ORGANISATIONS SYNDICALES	16
16. SUIVI DE LA MISE EN APPLICATION DE LA CHARTE.....	16
17. ENTREE EN VIGUEUR	16

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 2 / 17

0. Définitions

Par simplification, et en cohérence avec la dénomination nationale, la Charte d'Utilisation des Ressources Informatiques sera désignée dans le document sous le terme « Charte » ou « Charte informatique ».

On désignera également dans ce document sous le terme « Organisme » la Caisse Primaire d'Assurance Maladie des Bouches-du-Rhône.

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) **en accord avec les dispositions légales et réglementaires en vigueur et en application de la Politique Nationale de Sécurité des Systèmes d'Information.**

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 Cnamts 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, ...).

Cette charte s'applique aux usages du Système d'Information dans et en dehors des locaux de l'organisme (nomadisme, télétravail).

L'utilisation à des fins professionnelles de ressources informatiques ou moyens de communication, appartenant à titre privé à l'utilisateur, est interdite. Dans certains cas justifiés et maîtrisés, des dérogations peuvent être validées par la Sous-Direction des Systèmes d'Information.

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 3 / 17

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 ([agents avec un contrat de travail quel que soit sa durée, stagiaire, vacataire...](#)) 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.

[Dans certains cas](#), les tiers d'entités extérieurs 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 publication sur le portail intranet de l'organisme](#).

2.3. Mise à jour

Cette charte est susceptible d'évoluer en fonction des nouveaux risques affectant les ressources informatiques et de toute nouvelle consigne réglementaire et/ou technique émise par la CNAMTS, ou par toute autorité qui s'imposerait en la matière

3. Règles d'utilisation du Système d'Information

3.1. Dispositions réglementaires

Les utilisateurs doivent respecter les dispositions légales et réglementaires en matière de Sécurité du Système d'Information dont les principales références sont mentionnées ci-dessous. Toute atteinte à ces dispositions doit être considérée comme une infraction. Elle sera assimilée à un incident de sécurité et devra être traitée comme tel. Les textes ci-après constituent une base de référence.

Textes et lois sur la protection des données à caractère personnel, en particulier :

- La Loi modifiée n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,
- La Directive européenne n°95/46/CE du 24 octobre 1995,
- La charte des droits fondamentaux de l'Union Européenne et particulièrement l'article 8 portant sur la protection des données à caractère personnel,
- La convention européenne du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (dite convention 108),
- L'article 9 du code civil sur l'atteinte à la vie privée

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 4 / 17

- L'article 226-22 du Code pénal, qui assimile la divulgation des informations portant atteinte à la vie privée à un délit. Dans ce dernier cas, l'entreprise peut être déclarée civilement responsable (cf. art. 1384 du Code Civil).

Textes sur le secret professionnel et le secret médical

- L'article 226-13 du code pénal sur le secret professionnel,
- L'article L 1110-4 du code de la Santé Publique sur le droit des malades,
- Ainsi que l'article R 4127-4 portant sur le secret médical des médecins.

Textes et lois sur les atteintes aux systèmes de traitement des données

- Les articles 323-1 à 323-7 du code pénal portant sur les atteintes aux systèmes de traitement automatisé de données,

Textes relatifs à la propriété intellectuelle, le secret des communications, de l'utilisation de la langue française et à la cryptologie :

- La loi du 10 mai 1994 (propriété intellectuelle)
- Loi 91.646 du 10 juillet 1991 (secret des correspondances émises par la voie des communications)
- Loi du 04 Août 1994 (utilisation de la langue française)
- Arrêté du 25 mai 2007 et Décret n° 2007-663 du 2 mai 2007 définissant la forme et le contenu des dossiers de déclaration et de demande d'autorisation d'opérations relatives aux moyens et aux prestations de cryptologie

Textes sur la relation entre les Administrations et les usagers

- La législation propre aux administrations concernant l'obligation de communiquer les publications et documents administratifs non confidentiels.
- Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives,
- Le Décret n° 2010-112 du 2 février 2010 et publication de l'arrêté Référentiel Général de Sécurité (RGS) le 18 mai 2010.

3.2. 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 **installation** ou 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.

3.3. Utilisation privée résiduelle et nommage des données privées

L'utilisation à titre privé **des ressources informatiques** et des moyens de communication électroniques **professionnels** (messagerie et Internet) est tolérée dans le cadre d'un usage raisonnable et à condition **que cette utilisation respecte les règles de sécurité de la présente charte** qu'elle n'affecte pas la disponibilité, l'intégrité et la confidentialité du système d'information et qu'elle ne mette pas en cause l'intérêt et la réputation de l'organisme...

	Politique de Sécurité du Système d'Information Charte d'Utilisation des Ressources Informatiques	 Page 5 / 17
--	--	---

Il est rappelé à ce titre que l'agent est tenu à une obligation de loyauté vis-à-vis de son employeur (article L.1222-1 du code du travail).

Dans tous les cas, l'utilisateur doit supprimer toute mention relative à l'employeur ou indication qui pourrait laisser croire que le message est rédigé dans le cadre de son exercice professionnel.

L'Organisme ne pourra prendre connaissance du contenu des messages privés, à la condition que ceux-ci soient clairement identifiés comme tels et sous réserve des dispositions de l'article 3.4.

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

La participation à un service de type communautaire, en particulier forums, réseaux sociaux... est interdite, sauf autorisation expresse de la Direction.

L'utilisateur peut stocker des données privées dans un répertoire situé sur le disque local du poste de travail, dénommé « **PERSONNEL – NOM-N° GRH** », 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. **Seuls les documents professionnels peuvent être copiés et hébergés sur des espaces serveurs.**

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

3.4. Droits d'accès aux données

Les dossiers, fichiers y compris sur supports amovibles (même personnels) 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 que 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.

Les connexions internet établies par un salarié sur des sites internet pendant son temps de travail sont également présumées avoir un caractère professionnel.

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.

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 6 / 17

4. Attribution et retraits 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 une carte agent avec un **code confidentiel** (code PIN) et parfois des identifiants et mots de passe qui ne doivent pas être communiqués.

La carte agent doit faire l'objet d'une attention particulière dans le cadre de l'activité professionnelle. L'utilisateur doit respecter les règles de sécurité en vigueur concernant la carte agent, à savoir :

- Il doit mémoriser son code confidentiel et détruire le support sur lequel il lui a été communiqué, ou le conserver à l'abri des regards,
- Il doit garder sa carte sur lui lorsqu'il arrive sur son lieu de travail ou le quitte,
- Il doit signaler immédiatement 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.
- Il ne doit pas divulguer son code confidentiel,
- Il ne doit pas écrire son code confidentiel sur le dos de sa carte ou sur tout support accessible aux regards,
- En cas d'absence du bureau, même pour une très courte durée, il doit retirer la carte du lecteur et l'emporter avec lui,
- Il ne doit pas prêter sa carte à un autre utilisateur dans quelque circonstance que ce soit.

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.

Lorsqu'un utilisateur est en possession de plusieurs identifiants, il doit utiliser en priorité celui qui entraîne le moins de privilèges et qui correspond le mieux à la tâche réalisée.

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.

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

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 §3.4).

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 7 / 17

4.3. Gestion des départs

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

- ▶ détruire son répertoire « **PERSONNEL – NOM-N° GRH** » 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 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

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et aussi à celle de son service. L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles ou non professionnelles.

5.1. Protection des ressources et des informations

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

L'utilisateur doit veiller à ce que des informations sensibles ne soient pas affichées sur son écran, en son absence.

Il s'engage à ne pas mettre à la disposition de tiers non autorisés un accès aux systèmes ou au réseau, à travers des matériels dont il a l'usage.

L'utilisateur doit 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 de gestion des incidents de sécurité. Il doit également noter et signaler le plus rapidement possible aux équipes informatiques toute faille de sécurité observée ou soupçonnée. Néanmoins, il ne doit, en aucun cas, essayer de démontrer l'existence d'une faille soupçonnée.

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux (internes ou extérieurs à l'Organisme) que ce soit par des installations ou des manipulations anormales du matériel, ou par l'introduction de logiciels malveillants.

L'utilisation d'utilitaires permettant une élévation de privilèges est proscrite.

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, contourner ou déconnecter (partiellement ou totalement) un dispositif technique de sécurité.

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 8 / 17

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.

Si un utilisateur suspecte ou constate un dysfonctionnement de l'anti-virus sur son PMF, il doit cesser toute activité sur le poste et avertir [la Sous-Direction des Systèmes d'Information au travers du circuit en vigueur de demandes d'interventions](#).

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 PMF de l'Assurance Maladie est interdite.

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

- ▶ le support 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 MSSSI),
- ▶ le support est apporté par un représentant d'un autre organisme de l'Assurance maladie ou un tiers habilité et doit être utilisé par nécessité de service.

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.
- Sauvegarder les documents nécessaires dans un espace sécurisé après chaque utilisation.
- Effacer les données et déconnecter le support du PMF.

Toute connexion de supports amovibles extérieurs, à l'organisme, est interdite sur le poste de travail. Toutefois, si la connexion est indispensable pour des raisons de service, il convient de prendre les précautions complémentaires suivantes :

- Ne jamais utiliser de support amovible dont l'origine ne peut être garantie.
- Ne pas double-cliquer sur les documents, mais les ouvrir à partir des logiciels de son PMF (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 PMF.

Dans tous les cas il convient d'être prudent et vigilant, de signaler tout incident ou anomalie et ne pas hésiter à se rapprocher de [la Sous-Direction des Systèmes d'Information](#) de l'organisme pour connaître la conduite à tenir.

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 9 / 17

5.4. Chiffrement

La transmission en interne ou en externe de données sensibles (données classées « secret » et « confidentiel ») doit impérativement répondre aux préconisations de la LR-DDO-214/2013 portant sur la « Classification des informations ».

L'utilisation d'outils de chiffrement est encadrée par la [Sous-Direction des Systèmes d'Information](#) et le MSSI de l'organisme.

6. Utilisation des moyens de communication messagerie, Intranet, Internet

6.1. La messagerie

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.

[De plus, le reroutage systématique des messages vers une boîte aux lettres privée est interdit sauf sur dérogation autorisée par la Sous-Direction des Systèmes d'Information.](#)

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 (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 :

- ▶ Les informations en ligne doivent être utilisées à des fins professionnelles et ne pas être divulguées ni diffusées à des tiers non autorisés,
- ▶ L'enregistrement pour modification et diffusion interne ou externe de documents ou d'informations présents dans l'Intranet est interdit sans autorisation de la Direction,
- ▶ Les contributions à caractère diffamatoire, discriminatoire ou incorrect sont interdites.
- ▶ [Toute création de site ou utilisation de technologies permettant des accès à distance sur des postes et la publication de documents sur un site autorisé par le biais des ressources informatiques doivent être soumises à l'accord écrit d'un délégué de la Sous-Direction des Systèmes d'Information.](#)

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 [informatique](#).

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

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 10 / 17

Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle. [L'accès d'Internet ne peut être utilisé pour fournir des services à des utilisateurs extérieurs.](#)

La [Sous](#)-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,
- ▶ 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),
- ▶ [le raccordement du poste de travail à des bornes sans-fil publiques d'accès à Internet](#)
- ▶ 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 @xxx-organisme.cnamts.fr (exemple: eric.dupont@cpam-paris.cnamts.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.

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, pour un motif personnel, est tolérée dans la mesure où celle-ci est exceptionnelle et raisonnable et lorsque le contenu n'est contraire à aucune des prescriptions de cette charte.

La participation des utilisateurs à un service de type communautaire, forums, réseaux sociaux..., est interdite à partir du poste de travail, sauf autorisation expresse de la Direction.

Les connexions Internet font l'objet de supervisions, de vérifications et d'audits réguliers selon des directives définies au niveau national. Les identifiants et les adresses de connexion sont ainsi enregistrés.

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 11 / 17

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 ou non conforme aux règles fixées par 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. [L'utilisateur doit déconnecter les sessions de nomadisme quand son travail sur le poste nomade est terminé ou qu'il ne nécessite plus d'accès aux ressources partagées.](#)

[L'utilisateur nomade doit contacter immédiatement la Sous-Direction des Systèmes d'Information afin de déclarer la perte ou le vol de ses matériels ou moyens d'authentification.](#)

8. Données nominatives

La présence de données nominatives au sein du système d'information, en particulier celles d'assurés, de professionnels de santé et d'employeurs n'est possible et autorisée qu'en respect de formalités préalables et d'obligations pour le responsable du traitement.

Ainsi, les utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de traitement automatisé ou non, de données à caractère personnel.

[Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers contenant des données à caractère personnel, il devra auparavant en avoir fait la demande auprès du Correspondant Informatique et Libertés de l'organisme et en avoir reçu l'autorisation. Il est rappelé que cette autorisation n'est valable que pour le traitement défini dans la demande. Tout nouveau traitement doit faire l'objet d'une nouvelle déclaration.](#)

Définition d'une donnée à caractère personnel :

Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement par référence à un numéro d'identification (par exemple le n° de sécurité sociale) ou par référence à un ou plusieurs éléments qui lui sont propres (par exemple les initiales du nom et du prénom) ou par recoupement d'informations du type : date de naissance, commune de résidence, éléments biométriques, etc.

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 12 / 17

Définition de la donnée de santé à caractère personnel

Donnée à caractère personnel relative à la santé d'une personne physique.

Dans le domaine sanitaire, une donnée de santé à caractère personnel se définit comme une donnée susceptible de révéler l'état pathologique de la personne. Cette indication doit toutefois être aujourd'hui appréciée au regard de la définition d'une donnée de santé issue de la proposition de règlement du parlement européen et du conseil du 5 janvier 2012 sur la protection des données : « toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne ».

Elle traduit un concept plus large de la donnée de santé, qui aujourd'hui ne peut se limiter à la seule indication d'une maladie tant la prise en charge sanitaire d'une personne emporte également la connaissance de sa situation familiale ou sociale et fait intervenir des acteurs multiples professionnels de santé et personnels sociaux.

9. 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.

Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle. Ces dernières ne peuvent être effectuées que par un délégataire de la Sous-Direction des Systèmes d'Information.

Par ailleurs, l'utilisateur n'est pas autorisé à installer, copier ou utiliser sur son poste de travail de logiciels gratuits, à caractère ludique ou dont le droit d'usage est acquis à titre privé, ni contourner les restrictions d'utilisation d'un logiciel.

Il est rappelé que les logiciels commerciaux disponibles pour les utilisateurs de l'Organisme font l'objet de licences par lesquelles des droits d'usage sont concédés et font l'objet de contrats conclus par celui-ci. Il est de la responsabilité de l'utilisateur de respecter les termes de ces licences sous peine de faute professionnelle.

De même, l'utilisateur ne doit pas se servir d'images, textes, musiques, photographies, vidéos, codes sources hors domaine public dont il n'est pas l'auteur, sans s'exposer aux sanctions légales prévues pour le délit de contrefaçon.

Pour les agents assurant une fonction de développement informatique, il est rappelé que les logiciels créés dans le cadre du contrat de travail demeurent la propriété de l'organisme.

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 13 / 17

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

10.1. 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.

10.2. Rôle des administrateurs du système d'information

Les administrateurs sont nommément désignés et assurent le bon fonctionnement des moyens informatiques de l'organisme. **Ils sont des acteurs essentiels pour la préservation de la sécurité du système d'information.**

Les administrateurs d'un système d'information sont tenus à des obligations particulières de loyauté, de transparence et de confidentialité :

- Loyauté : L'administrateur étant investi de larges pouvoirs de surveillance sur les données qui circulent sur les systèmes d'information de l'organisme, le respect de règles d'éthique est attendu de sa part.
- Transparence : L'administrateur doit exercer ses missions dans le cadre du règlement intérieur et de la charte informatique.
- Confidentialité : L'administrateur est tenu à une obligation particulière de confidentialité, tenant notamment au secret professionnel. Il ne doit pas divulguer les informations auxquelles il aurait pu avoir accès lors de l'exercice de ses fonctions, a fortiori lorsqu'elles sont couvertes par le droit à la vie privée ou le secret des correspondances, à moins qu'une disposition législative ne l'impose (ex. en cas de découverte de contenus illicites)

Dans le cadre de leurs fonctions, ils peuvent prendre des mesures conservatoires, telles que l'arrêt d'une exécution, la suppression des droits d'accès et de mots de passe, voire la fermeture du réseau au monde extérieur, afin de pallier un incident éventuel de fonctionnement et/ou de sécurité.

Leurs activités peuvent rendre nécessaire un examen des fichiers, courriers ou journaux d'événements (connexions, accès distants, etc...), afin de diagnostiquer et corriger tout dysfonctionnement d'un logiciel, ou après tout incident technique qui pourrait mettre en cause le bon fonctionnement de la sécurité du système.

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.

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

10.3. Rôle du Manager de la Sécurité des Systèmes d'information

Le Manager de la Sécurité des Systèmes d'Information (MSSI) ou ses délégataires, coordonne et fédère les différents acteurs concourant à la sécurité de l'organisme. Dans ce cadre, il est chargé du suivi de la charte et de son respect.

Il travaille en collaboration avec les différents administrateurs exploitant les équipements de l'organisme et leur assure une fonction de conseil. **Il prend en charge également plusieurs contrôles de l'utilisation des ressources du Système d'Information.**

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 14 / 17

Le MSSi ou ses délégataires, doit être informé par les utilisateurs et les administrateurs des besoins locaux perçus en matière de sécurité et de toute modification impactant la sécurité, que celle-ci touche les équipements, serveurs ou réseaux de l'Organisme.

10.4. Contrôle de l'utilisation des ressources

Pour des nécessités de maintenance, de gestion technique et de sécurité, l'administrateur peut analyser et contrôler l'utilisation des ressources informatiques matérielles ou logicielles ainsi que les échanges via le réseau ou les services d'accès.

En conséquence, l'utilisateur ne doit pas procéder volontairement au cryptage de son poste de travail sans autorisation, faisant ainsi obstacle au contrôle de l'administrateur.

En cas de détection d'une situation non conforme à cette charte, ou d'actions d'un utilisateur agissant en violation des règles de déontologie, des règles de sécurité et/ou de législation en vigueur, l'administrateur en informera immédiatement le Manager de la Sécurité des Systèmes d'Information ou ses délégataires.

Dans le cadre du recueil d'éléments complémentaires pour analyser une situation non conforme, et après l'accord du Directeur des Systèmes d'Information, l'administrateur pourra être autorisé à accéder aux fichiers présumés professionnels hors de la présence de l'utilisateur, sauf ceux avec une mention indiquant le caractère personnel.

Les états fournis par le logiciel d'inventaire et de gestion de parc sont également périodiquement exploités pour détecter les éventuels matériels ou/et logiciels non autorisés.

Les traces générées au niveau applicatif et au niveau de l'infrastructure technique contenant des données à caractère personnel ne font pas l'objet d'une exploitation systématique. Elles ne sont utilisées qu'en cas d'incidents d'exploitation majeur, d'incidents de sécurité, de suspicion de fraudes ou pour lever un doute sur la justification d'un accès.

Par ailleurs, à des fins statistiques, de qualité de service et de sécurité, les fichiers historiques résultant du trafic sur les sites Intranet ou Internet, pourront être sujets à des vérifications par l'organisme portant exclusivement sur :

- les durées de connexions (de façon globale / par service)
- les sites les plus visités (de façon globale / par service)

De même, des contrôles périodiques pourront être réalisés dans les domaines suivants :

- Utilisation des cartes d'accès en l'absence de son attributaire.
- Connexions au réseau local pour détecter celles réalisées en dehors des heures de travail, ou bien celles pour lesquelles l'accès a été infructueux.

11. Sauvegarde et archivage

11.1. Données générales

L'utilisateur doit stocker ses fichiers et données électroniques dans des espaces serveurs définis par la Sous-Direction des Systèmes d'Information.

La sauvegarde des données locales résidentes sur le disque dur du poste de travail et revêtant un caractère indispensable à l'activité professionnelle est à la charge de l'utilisateur. Les moyens d'archivage locaux peuvent être mis à disposition à cette fin.

Pour leur assurer une protection adaptée, les documents les plus confidentiels doivent être placés de manière exclusive et définitive sur des espaces serveurs.

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 15 / 17

Les informations médicales à caractère personnel doivent être impérativement déposées sur un serveur dédié. Elles ne doivent donc, en aucun cas, être conservées sur le poste de travail.

La sauvegarde des données déposées sur les serveurs est à la charge de [la Sous-Direction des Systèmes d'Information](#).

11.2. Archivage et destruction

L'archivage des données est effectué conformément à la réglementation applicable ainsi qu'aux préconisations de la LR-DDO-214/2013 concernant la « classification des informations ».

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

12. 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.

13. Journaux d'événements

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, [préconisée par la CNIL](#), 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.

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

[L'exploitation des traces produites sur le système d'information de l'organisme est décrite dans le chapitre 10.](#)

14. 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.

[Par ailleurs, les abus, dérives ou infractions, sanctionnés par la loi, peuvent engager la responsabilité civile et pénale de l'utilisateur, mais aussi de l'organisme. Si la responsabilité de l'organisme était recherchée à côté de celle de l'utilisateur, l'organisme se réserve le droit d'exercer un recours contre l'intéressé.](#)

	Politique de Sécurité du Système d'Information	
	Charte d'Utilisation des Ressources Informatiques	Page 16 / 17

15. Dispositions spécifiques liées aux organisations syndicales

Les dispositions de la présente charte s'appliquent aux membres des instances représentatives du personnel, des organisations syndicales et par les associations de gestion des œuvres sociales lorsqu'ils réalisent leurs activités professionnelles pour le compte de l'organisme.

Dans le cadre des activités liées à leurs mandats de représentation ou/et syndicaux, les règles d'utilisation des ressources informatiques relèvent d'accords spécifiques.

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

16. 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](#).

17. 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.

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, [au travers de sa publication sur le portail intranet de l'organisme](#), 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 dotés d'un accès au Système d'information et qui s'engageront à la respecter.



**l'Assurance
Maladie**
Agir ensemble, protéger chacun

Haute-Corse