

LIVRET DE SECURITE DU SYSTEME D'INFORMATION

SOMMAIRE

Table des matières

1. LES ENJEUX DE SECURITE.....	3
2. ACCES AU POSTE INFORMATIQUE.....	3
3. ACCES AUX DONNEES.....	4
4. LES PERIPHERIQUES	4
5. LA MOBILITE ET LE TELETRAVAIL	5
6. LA PROTECTION DES LOCAUX	5
7. ACTEURS DE LA SECURITE	5
8. LE PLAN DE CONTINUITE DES ACTIVITES (PCA).....	6
9. LA CLASSIFICATION DES DOCUMENTS	6
10. CONTACTS.....	7

Introduction

L'UGECAM Aquitaine, comme toute entreprise, est confrontée à des menaces pesant sur son système d'information qui l'ont amenée à se doter d'une démarche de sécurité du système d'information.

Elle se doit de protéger les patients, les usagers, les biens, les données, les applications et le matériel, avec pour objectifs la confidentialité, la disponibilité et l'intégrité du système d'information et des données.

La sécurité du système d'information passe par l'adhésion à la démarche, la vigilance et la réactivité de chaque agent de l'Ugecam quelle que soit sa fonction :

La sécurité du système d'information, c'est l'affaire de tous !

1. LES ENJEUX DE SECURITE

Protéger les données à caractère personnel

Les textes de loi et avis des autorités de tutelle ainsi que ceux de la Commission nationale de l'informatique et des libertés (CNIL) concernant la protection des informations à caractère personnel constituent le cadre réglementaire qui s'impose à tous.

Pour chaque utilisateur, les habilitations sont justifiées par le métier, mais tous les accès fonctionnellement possibles avec une habilitation donnée ne sont pas autorisés. Le seul accès conforme à des données à caractère personnel est celui justifié par une mission. C'est cette mission qui fonde le droit d'en connaître.

Protéger le patrimoine informationnel

Au titre de ses missions de service public, l'UGECAM Aquitaine traite des informations indispensables au bon déroulement de ses processus métiers et notamment à la prise en charge et à l'accompagnement des patients, usagers et résidents.

La protection de ces données, par l'ensemble des acteurs de l'UGECAM Aquitaine, contribue à garantir l'accomplissement de l'ensemble des missions de l'Institution.

Assurer la sécurité et la continuité des soins et des prises en charge

L'UGECAM Aquitaine délivre des prestations et des services dont la continuité doit être garantie.

Les processus métiers permettant la prise en charge et l'accompagnement des patients, usagers et résidents doivent être conformes et maîtrisés. Ils doivent intégrer les procédures et outils de sécurité cohérents avec les règles de l'art ainsi que satisfaire aux obligations légales.

La mise en œuvre des plans de continuité d'activité (PCA) appuyée sur les ressources et organisations dédiées apporte une assurance raisonnable quant à la continuité des missions.

Préserver l'image de l'Assurance Maladie et de l'UGECAM

L'image de l'Institution est un bien important dont la valeur ne doit pas être entachée par les incidents ou accidents dans le traitement des informations.

2. ACCES AU POSTE INFORMATIQUE

La sécurité du système d'information passe par la sécurisation de l'environnement de travail.

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 code PIN)** qui ne doit pas être communiqué(s).

La carte agent est un élément clé du dispositif de sécurisation des accès informatiques. Les règles concernant leur usage et leur conservation doivent être scrupuleusement respectées.

✓ **En aucun cas, une carte ne peut être prêtée**, car elle est strictement personnelle.

- ✓ **En cas d'absence du bureau**, même pour une très courte durée, il faut retirer la carte du lecteur et ne pas la laisser en évidence.
- ✓ En fin de journée, **la carte doit être emportée et conservée par l'utilisateur**.
- ✓ **Le code** ne doit ni être communiqué à une tierce personne, ni être conservé à proximité de la carte.
- ✓ **En cas de perte ou de vol**, le propriétaire de la carte doit immédiatement en informer son responsable hiérarchique.
- ✓ **La carte est la propriété de l'organisme d'Assurance Maladie**. En cas de départ (retraite, mutation, ...) elle doit être restituée.

Outre la carte agent, l'**utilisation d'un mot de passe** peut s'avérer nécessaire pour accéder à certaines ressources.

- ✓ **Le mot de passe certifie votre identité**. Il est strictement confidentiel.
- ✓ **Respectez les règles** de définition et de mise à jour des mots de passe.
- ✓ **Choisissez un mot de passe facilement mémorisable**. Néanmoins, ne choisissez pas un mot de passe évident à trouver (prénom des enfants...) ou à deviner. Il doit comporter des lettres et des chiffres et ne pas correspondre à un mot que l'on peut trouver dans un dictionnaire (*voir les fiches de préconisation publiées par ailleurs*)
- ✓ **Ne notez pas votre mot de passe** : retenez-le par cœur.
- ✓ **Ne le divulguez à personne** : il est unique, personnel, inaccessibles et confidentiel
- ✓ **Utilisez des mots de passe différents** pour chaque application.
- ✓ **Différenciez vos mots de passe** professionnels et personnels.

La devise du bon mot de passe est :

« Le retenir, c'est facile, le deviner c'est difficile »

3. ACCES AUX DONNEES

Vous manipulez des informations de différents niveaux de sensibilité.

Le secret professionnel couvre les faits et informations qui sont connus des agents des organismes en raison de leur fonction. L'obligation de respect du secret professionnel s'applique en tout lieu et en tout temps (ex : au sein de l'UGECAM Aquitaine comme à l'extérieur, pendant la durée du contrat de travail et après la fin de celui-ci).

Les données personnelles et médicales sont des données sensibles. Seules certains agents bénéficiant d'une habilitation particulière y ont accès, et elles ne peuvent être communiquées à des tiers que sous certaines conditions.

- ✓ **N'accédez qu'aux informations utiles à votre activité professionnelle**. Le seul accès conforme à des données à caractère personnel est celui justifié par une mission.
- ✓ **Ne laissez pas** sans surveillance les matériels, les documents, les supports ayant un caractère professionnel.
- ✓ **Les discussions** relatives à la situation d'un patient ou d'un usager doivent être menées **en toute confidentialité**.
- ✓ **Soyez vigilant** quant à l'identité de vos correspondants.

4. LES PERIPHERIQUES

L'utilisation des disques durs externes, des clés USB et autres périphériques nomades s'est largement répandue, ouvrant ainsi de nouvelles failles de sécurité (virus, perte ou vol de données...).

- ✓ **N'utilisez** que le matériel mis à votre disposition dans le cadre professionnel.
- ✓ **Ne vous servez pas** d'une clé USB offerte par un intervenant extérieur à l'UGECAM Aquitaine.
- ✓ **Protégez** votre clé à l'aide des solutions proposées par les experts locaux.
- ✓ **La clé USB est un outil de transport** mais pas de stockage.
- ✓ **Supprimez** régulièrement le contenu de votre clé USB.

- ✓ **Ne prêtez** votre clé professionnelle qu'après suppression des données.
- ✓ **Adoptez** le même niveau de vigilance pour tout autre support amovible.
- ✓ **Signalez** immédiatement tout vol ou perte.

5. LA MOBILITE ET LE TELETRAVAIL

Que cela soit dans le cadre de déplacements professionnels, en télétravail ou à distance sur un autre site, les règles de bon usage des outils informatiques et les principes de sécurité et de confidentialité doivent continuer à s'appliquer.

- ✓ **Adoptez** les mêmes gestes de sécurité qu'au bureau.
- ✓ **Ne laissez pas** sans surveillance les matériels, les documents, les supports ayant un caractère professionnel.
- ✓ **Respectez** la charte informatique, la confidentialité et le secret professionnel.
- ✓ **Protégez** le matériel mis à votre disposition.

6. LA PROTECTION DES LOCAUX

La protection des locaux ainsi que de leur contenu contre les menaces (dommages matériels, intrusions de personnes non habilitées, vols, dégradations...) passe par le strict respect des consignes d'accès et de circulation.

- ✓ **Respectez** les procédures d'accueil du personnel et des visiteurs.
- ✓ **Ne laissez pas** entrer des personnes inconnues dans les locaux de l'organisme. Assurez-vous des raisons de leur présence et réorientez-les vers les points d'accueil ou les circulations dédiées,
- ✓ **Fermez** fenêtres et bureaux lorsque vous partez.
- ✓ **Le soir, éteignez** votre poste et tout appareil électrique.
- ✓ **Aucun dispositif de sécurité ne doit être désactivé** ou contourné (les portes coupe-feu, alarmes intrusions, détecteurs de fumée, issues de secours...). Signalez sans délai tout dysfonctionnement.
- ✓ **Vous devez signaler** à votre responsable la perte ou le vol des clés ou cartes d'accès aux locaux.
- ✓ **De manière générale signaler toute situation inhabituelle ou paraissant anormale.**

7. ACTEURS DE LA SECURITE

De la messagerie à Internet en passant par les applications du poste de travail, la sécurité du système d'information dépend de la vigilance et du comportement de chacun.

- ✓ **Ne changez pas** les configurations des postes de travail et n'installez aucun logiciel sans l'accord du service informatique.
- ✓ **Limitez** votre utilisation d'Internet à un usage strictement professionnel.
- ✓ **Naviguez** prudemment et ne confiez pas de données professionnelles sur internet (forums, blogs, réseaux sociaux...).
- ✓ **N'ouvrez pas** et ne faites pas suivre les messages de type chaîne ou spam.
- ✓ **Soyez** prudents avec les pièces jointes.
- ✓ **Ne désinstallez pas**, ne désactivez pas les logiciels de sécurité.
- ✓ **Ne téléchargez pas** de logiciels.
- ✓ **Veillez** aux conditions d'utilisations de vos outils nomades (téléphone, ordinateur, clé USB, clé3G...) en dehors de l'environnement professionnel.
- ✓ **Signalez** tout incident pouvant nuire à la sécurité du système d'information par mail à : mssi.ug-aquitaine@ugecam.assurance-maladie.fr

8. LE PLAN DE CONTINUITE DES ACTIVITES (PCA)

Le PCA est à la fois une organisation et un ensemble de procédures permettant de gérer des situations extrêmes (incendie, inondation, coupure réseau ou électrique, pandémie.... En cas de sinistre majeur, le PCA permet en premier lieu de mettre en sécurité les personnes, puis de maintenir les activités essentielles pour préserver la mission de service public.

Sa finalité est de reprendre l'ensemble des activités de l'organisme selon les priorités définies dans les délais les plus courts et en respectant les exigences de sécurité du système d'information.

QUELS SONT LES REFLEXES A ADOPTER EN CAS DE CRISE ?

- ✓ Signaler sans attendre tout problème susceptible d'impacter l'organisme (dégât des eaux, incendie, pli suspect, etc.) et en alerter le RPCA ou le RPCA adjoint. En fonction de la gravité, alertez les services de secours en composant le 18.
- ✓ Rejoindre le point de rassemblement le plus proche et respecter les consignes de sécurité (évacuation, etc..).
- ✓ Se tenir informé de la situation (changement de site de travail, fermeture de l'organisme, etc...) auprès de son responsable
- ✓ Ne pas communiquer sur l'incident. La communication est placée sous la responsabilité de la Direction et des instances de tutelle, car elle peut nuire à mon image ou à celle de l'institution, aux éventuelles enquêtes administratives ou judiciaires..

COMMENT PARTICIPER À LA RÉUSSITE DU PCA ?

- ✓ en contribuant à l'exercice PCA annuel de façon active (si mon service est concerné).
- ✓ en communiquant et en mettant à jour mes coordonnées personnelles Ces données ne seront utilisées qu'en situation de crise réelle, soit pour vous informer des suites à donner, soit pour vous solliciter en tant que renfort.
- ✓ en étant mobilisé lors d'une crise. Selon le type de sinistre, je peux être amené à travailler sur autre site ou sur une nouvelle tâche.

9. LA CLASSIFICATION DES DOCUMENTS

Il existe ainsi 4 niveaux de classification :

- ✓ **Secret** : ce sont les informations dont l'accès est réservé au plus petit nombre possible d'agents habilités. Les informations qui relèvent de cette classe sont celles, nominatives ou non, dont la divulgation serait reprochée à l'UGECAM Aquitaine au point de remettre en cause la conduite de ses missions.
Il s'agit principalement de renseignements d'ordre médical et/ou comportemental, concernant une personne identifiée (par exemple par son NIR) et d'éléments relatifs à la stratégie d'entreprise (projets de réorganisation). Ces données étant particulièrement sensibles, elles doivent faire l'objet d'une vigilance extrême de la part des utilisateurs du système d'information **et font l'objet d'un encadrement et d'un suivi au niveau national.**
- ✓ **Confidentiel** : les informations dont la divulgation porterait préjudice aux missions de l'UGECAM Aquitaine sans remettre en cause leur conduite.
Ce sont notamment les données à caractère personnel touchant à la vie privée et/ ou professionnelle hors informations médicales.
- ✓ **Restreint** : toutes les informations nécessaires aux missions de l'UGECAM Aquitaine qui ne justifient pas un classement plus élevé.
C'est le marquage le plus fréquemment utilisé (instructions administratives type notes de service ou notes d'organisation, statistiques, comptes rendus, informations mises en ligne sur l'intranet, etc.).
- ✓ **Public** : ce sont les informations qui ont vocation à une publication externe, vers les clients, fournisseurs, partenaires.

Il est recommandé de mentionner la classification en bas de page.

10. CONTACTS

En cas de doute sur la conduite à tenir concernant la sécurité du système d'information, vous pouvez contacter, le Manager de la sécurité du système d'information :

mssi.ug-aquitaine@ugecam.assurance-maladie.fr

Pour les demandes de dépannage de votre poste informatique ou de vos périphériques, contactez le service informatique :

assistance.informatique@ugecam.assurance-maladie.fr

Pour toutes questions relatives à la Commission nationale informatiques et libertés, vous pouvez contacter le délégué à la protection des données :

dpo.ug-aquitaine@ugecam.assurance-maladie.fr