REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

MINISTERE DE LA SANTE PUBLIQUE

SECRETARIAT GENERAL

CELLULE INFORMATIQUE

REPUBLIC OF CAMEROON
Peace – Work – Fatherland

MINISTRY OF PUBLIC HEALTH

GENERAL SECRETARY

COMPUTER UNIT

APPLICATION INFORMATIQUE DE GESTION HOSPITALIERE

MARCHE N°0096/M/MINSANTE/CIPM/2022 PASSE PAR LA SOCIETE KIAMA SA SUIVANT L'APPEL D'OFFRE NATIONAL OUVERT N°084/D13-648/AONOU/MINSANTE/CIPM/2021 DU 15 NOVEMBRE 2021 RELATIF A L'ACQUISITION D'UNE APPLICATION INFORMATIQUE DE GESTION HOSPITALIERE

CHARTE D'UTILISATION

Décembre 2022

KIAMA

SOMMAIRE

CHARTE D'UTILISATION

1. OBJET DU DOCUMENT

La présente Charte a pour objet de décrire les règles d'accès et d'utilisation l'application de gestion hospitalière de l'Hôpital et rappelle à ses utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du site.

Elle pose des règles permettant d'assurer la sécurité et la performance de l'application de gestion hospitalière de l'établissement, de préserver la confidentialité des données dans le respect de la réglementation en vigueur et des droits et libertés reconnus aux utilisateurs, conformément à la politique de sécurité du système d'information définie par l'établissement et au Règlement Général de la Protection des Données (RGPD) en vigueur depuis mai 2018.

Cette Charte a été validée par la Direction générale de l'établissement. Préalablement à sa mise en œuvre, elle a été notifiée au Comité d'Établissement et à la Commission médicale d'Établissement. Elle constitue une annexe au Règlement Intérieur de l'établissement. Les membres du personnel et les personnels extérieurs sont invités à en prendre connaissance. La Charte est mise à leur disposition sur la Gestion Documentaire via AGEVAL et dans le livret d'accueil du nouvel agent
Cette Charte a fait l'objet de travaux communs au sein du groupement hospitalier de territoire (GHT) auquel appartient l'établissement/groupe d'établissements, afin d'harmoniser les pratiques d'accès et d'usage du SI des établissements et de faciliter l'utilisation des SI hospitaliers par les personnels qui exercent dans plusieurs structures au sein du GHT/groupe d'établissements.

2.CHAMP D'APPLICATION

La présente Charte concerne l'application de gestion hospitalière déployée au sein de l'établissement pour la gestion des données du patient.
Il s'agit principalement des ressources suivantes :

- Accès au DME
- Consultation
- Diagnostic Médical et infirmier
- Examens complémentaires
- Prescriptions
- Accès aux données d'hospitalisation
- Accès aux soins (Actes médicaux)
- Accès aux données d'aide à la décision
- Accès aux donnés de la pharmacie
- Accès aux ressources
- Accès aux données financières

Cette Charte s'applique à l'ensemble des professionnels de l'établissement de santé, tous statuts confondus, et concerne notamment les agents permanents ou temporaires (stagiaires, internes, doctorants, prestataires, fournisseurs, sous-traitants, bénévoles…) ayant accès à l'application de gestion hospitalière.
Dans la présente Charte, sont désignés sous les termes suivants :

- **Utilisateurs** : les personnes ayant accès à l'application de gestion hospitalière.

3. CADRE REGLEMENTAIRE

Le cadre réglementaire de la sécurité de l'information est complexe. Il porte sur les grands thèmes suivants :

- Le traitement numérique des données, et plus précisément :

- Le traitement de données à caractère personnel et le respect de la vie privée,
- Le traitement de données personnelles de santé.

- Le droit d'accès des patients et des professionnels de santé aux données médicales,
- L'hébergement de données médicales,
- Le secret professionnel et le secret médical,
- La signature électronique des documents,
- Le secret des correspondances,
- La lutte contre la cybercriminalité,
- La protection des logiciels et des bases de données et le droit d'auteur.

La présente Charte d'accès et d'usage du système d'information tient compte de la réglementation sur la sécurité de l'information en vigueur et des droits et libertés reconnus aux utilisateurs.

4.CRITÈRES FONDAMENTAUX DE LA SECURITE

4.1 PRINCIPES

L'établissement de santé héberge des données et des informations médicales et administratives sur les patients (dossier médical, dossier de soins, dossier images et autres dossiers médico-techniques…).

L'information se présente sous de multiples formes : stockée sous forme numérique sur des supports informatiques, imprimée ou écrite sur papier, imprimée sur des films (images), transmise par des réseaux informatiques privés ou Internet, par la poste, oralement et/ou par téléphone...

La **sécurité de l'information** est caractérisée comme étant la préservation de :

- **Sa disponibilité** : l'information doit être accessible à l'utilisateur, quand celui-ci en a besoin,
- **Son intégrité** : l'information doit être exacte, exhaustive et conservée intacte pendant sa durée de vie,
- **Sa confidentialité** : l'information ne doit être accessible qu'aux personnes autorisées à y accéder,
- **Sa traçabilité** : les systèmes doivent comporter des moyens de preuve sur les accès et opérations effectuées sur l'information.

4.2 UNE MISSION SECURITE

L'Hôpital fournit un système d'information qui s'appuie sur une infrastructure informatique. Elle doit assurer la mise en sécurité de l'ensemble, c'est-à-dire protéger ces ressources contre des pannes, des erreurs ou des malveillances. Elle doit aussi protéger les intérêts économiques de l'établissement en s'assurant que ces moyens sont

bien au service de la production de soins. Elle doit donc caractériser et empêcher les abus.

4.3 UN ENJEU TECHNIQUE ET ORGANISATIONNEL

Les enjeux majeurs de la sécurité sont la qualité et la continuité des soins, le respect du cadre juridique sur l'usage des données personnelles de santé.
Pour cela l'Hôpital déploie un ensemble de dispositifs techniques, mais aussi organisationnels. En effet, au-delà des outils, la bonne utilisation des moyens informatiques est essentielle pour garantir un bon niveau de sécurité. La sécurité peut être assimilée à une chaîne dont la solidité dépend du maillon le plus faible. Certains comportements humains, par ignorance des risques, peuvent fragiliser l'application de gestion hospitalière.

4.4 UNE GESTION DES RISQUES

L'information médicale, qu'elle soit numérique ou non, est un composant sensible qui intervient dans tous les processus de prise en charge des patients / résidents. Une information manquante, altérée ou indisponible, peut constituer une perte de chance pour le patient / résidents (exemples : erreur dans l'identification d'un patient [homonymie par exemple], perte de données à la suite d'une erreur d'utilisation d'une application informatique…). La sécurité repose sur une gestion des risques avec des analyses des risques potentiels, des suivis d'incidents, des dispositifs d'alertes. La communication vers les utilisateurs est un volet important de cette gestion. La présente Charte d'accès et d'usage de l'application de gestion hospitalière s'inscrit dans ce plan de communication.

5.RÈGLES DE SECURITE

L'accès au système d'information de l'établissement est soumis à autorisation de la direction.

Pour le personnel, y compris les personnels libéraux, mis à disposition et stagiaires, les droits d'accès au système d'information informatique sont déterminés selon la fiche de poste et les droits d'accès au système de téléphonie attribués selon le poste occupé ; également, conformément à la réglementation, l'accès au dossier personnel est attribué sur demande écrite, pour la durée strictement nécessaire à la consultation du dossier personnel exclusivement et sur place ; les codes d'accès sont attribués par les cadres de l'établissement ; la présente Charte d'accès et d'usage de l'application de gestion hospitalière est remise au personnel lors de la procédure de recrutement contre signature ; elle figure également sous forme résumée dans le livret d'accueil du personnel .

Le droit d'accès ne peut être cédé, même temporairement à un tiers. Tout droit prend fin lors de la cessation, même provisoire, de l'activité professionnelle de l'utilisateur, ou en cas de non-respect des dispositions de la présente Charte par l'utilisateur.

L'obtention d'un droit d'accès à l'application de gestion hospitalière de l'établissement de santé entraîne pour l'utilisateur les droits et les responsabilités précisées dans les paragraphes ci-dessous.

5.2 PROTECTION DE L'INFORMATION

Les postes de travail permettent l'accès à l'application de gestion hospitalière. Ils permettent également d'élaborer des documents bureautiques. Il est important de ne stocker aucune donnée ni aucuns documents médicaux sur ces postes (disques durs locaux). Cet espace est à usage professionnel uniquement. Le stockage de données privées sur des disques réseau est interdit.

Le cas échéant, ceux qui utilisent un matériel portable (exemples : poste, tablette, smartphone…) ne doivent pas le mettre en évidence pendant un déplacement ni exposer son contenu à la vue d'un voisin de train… ; le matériel doit être rangé en lieu sûr. De même, il faut ranger systématiquement en lieu sûr tout support mobile de données (exemples : CD, disquette, clé, disque dur…). Aucune donnée de santé à caractère personnel des patients ne doit être stockée sur des postes ou périphériques personnels.

Il faut également mettre sous clé tout dossier ou document confidentiel lorsqu'on quitte son espace de travail.

Les médias de stockage amovibles (exemples : clés USB, CD-ROM, disques durs…) présentent des risques très forts vis-à-vis de la sécurité : risques importants de contamination par des programmes malveillants (virus) ou risques de perte de données. Leur usage doit faire l'objet d'une très grande vigilance. L'établissement se réserve le droit de limiter, voire d'empêcher, l'utilisation de ces médias en bloquant les ports de connexion des outils informatiques, en cas d'utilisation itérée de clés USB potentiellement contaminées sans autorisation de la direction.

L'utilisateur ne doit pas transmettre de fichiers sensibles à une personne qui en ferait la demande et qu'il ne connaîtrait pas, même s'il s'agit d'une adresse électronique interne à l'établissement. Il doit vérifier systématiquement la fiabilité des mails qu'il reçoit avant leur ouverture.

5.3 USAGES DES RESSOURCES INFORMATIQUES

Seules des personnes habilitées de l'établissement de santé (ou par son intermédiaire la société avec laquelle il a contracté) ont le droit d'installer de nouveaux logiciels, de connecter de nouveaux PC au réseau de l'établissement et, plus globalement, d'installer de nouveaux matériels informatiques.

L'utilisateur s'engage à ne pas modifier la configuration des ressources (matériels, réseaux, …) mises à sa disposition, sans avoir reçu l'accord préalable et l'aide des personnes habilitées de l'établissement (ou par son intermédiaire la société avec laquelle il a contracté).

L'utilisation de matériels ou logiciels personnels doit impérativement être autorisée préalablement.

- **Le poste de travail**

Dans le cadre de sa mission, un collaborateur peut se voir fournir un ou plusieurs postes de travail, fixes ou nomades. Il est de son devoir d'appliquer les règles de bonne pratique liées à ce type de matériel. Notamment,
Le collaborateur doit :

- ✓ Veiller à conserver en bon état de fonctionnement le matériel et les logiciels mis à sa disposition,
- ✓ Veiller à ce que les règles de verrouillage de session soient bien appliquées sur son matériel,
- ✓ S'engager à sécuriser son matériel avec les moyens mis à disposition par la structure (système antivol, etc.).

Le collaborateur ne doit pas :

- ✓ Utiliser les équipements pour un usage personnel, sauf dans les limites fixées par la structure si elle l'a autorisé explicitement,
- ✓ Faire usage de postes de travail pour lesquels il n'a pas été explicitement autorisé.

Dans ce cas de figure, les professionnels hospitaliers sont tenus de respecter les règles de sécurité et de protection des données définies par la politique de sécurité du système d'information de l'établissement.

- **Les équipements mobiles et de stockage**

L'usage de périphériques type clés USB ou disques externes doit rester exceptionnel :
- Seuls les périphériques de stockage fournis par la structure sont autorisés,
- Tout périphérique de ce type doit faire l'objet d'un scan par l'antivirus à chaque utilisation par le collaborateur.

5.4 USACE DES LOGIN ET DES MOTS DE PASSE (OU DE CARTES CPS OU EQUIVALENT)

Chaque utilisateur dispose d'un compte nominatif lui permettant d'accéder à l'application de gestion hospitalière de l'établissement. Ce compte est personnel. Il est strictement interdit d'usurper une identité en utilisant, ou en tentant d'utiliser, le compte d'un autre utilisateur, ou en agissant de façon anonyme dans le système d'information.

Pour utiliser ce compte nominatif, l'utilisateur, soit dispose d'un login et d'un mot de passe, soit utilisé une carte CPS ou équivalent (avec un code personnel à 4 chiffres)
Le mot de passe choisi doit être robuste (8 caractères minimum, mélange de chiffres, lettres et caractères spéciaux), de préférence simple à mémoriser, mais surtout complexe à deviner. Il doit être changé tous les 6 mois. Le mot de passe est strictement confidentiel. Il ne doit pas être communiqué à qui que ce soit : ni à des collègues, ni à sa hiérarchie, ni au personnel en charge de la sécurité des systèmes d'information, même pour une situation temporaire.

- Chaque utilisateur est responsable de son compte et son mot de passe, et de l'usage qui en est fait. Il ne doit ainsi pas mettre à la disposition de tiers non autorisés un accès aux systèmes et aux réseaux de l'établissement dont il a l'usage. Il est ainsi possible pour l'établissement de vérifier *a posteriori* l'identité de l'utilisateur ayant accédé où tenter d'accéder à une application au moyen du compte utilisé pour cet accès ou cette tentative d'accès.

- C'est pourquoi il est important que l'utilisateur veille à ce que personne ne puisse se connecter avec son propre compte. Pour cela, sur un poste dédié, il convient de fermer ou verrouiller sa session lorsqu'on quitte son poste. Il ne faut jamais se connecter sur plusieurs postes à la fois. Pour les postes qui ne sont pas utilisés pendant la nuit, il est impératif de fermer sa session systématiquement avant de quitter son poste le soir.
- Il est interdit de contourner, ou de tenter de contourner, les restrictions d'accès aux logiciels. Ceux-ci doivent être utilisés conformément aux principes d'utilisation communiqués lors de formations ou dans les manuels et procédures remis aux utilisateurs.

- L'utilisateur s'engage enfin à signaler toute tentative de violation de son compte personnel.

5.5 IMAGE DE MARQUE DE L'ÉTABLISSEMENT

Les utilisateurs de moyens informatiques ne doivent pas nuire à l'image de marque de l'établissement à travers la communication d'informations à l'extérieur, via les moyens informatiques auxquels ils ont accès, en interne ou en externe, ou du fait de leur accès à Internet.

6. SURVEILLANCE DU SYSTEME D'INFORMATION

6.1 CONTRÔLE

Pour des nécessités de maintenance et de gestion, l'utilisation des ressources matérielles ou logicielles, les échanges via le réseau, ainsi que les rapports des télécommunications peuvent être analysés et contrôlés dans le respect de la législation applicable, et notamment du RGPD et de la loi Informatique et Libertés.

6.2 TRACABILITE

La direction assure la traçabilité de l'ensemble des accès à l'application de gestion hospitalière pour des raisons d'exigence réglementaire de traçabilité, de prévention contre les attaques et de contrôle du bon usage des applications et des ressources.
Par conséquent, les applications de l'établissement, ainsi que les réseaux, messagerie et accès Internet intègrent des dispositifs de traçabilité permettant d'enregistrer :

- L'identifiant de l'utilisateur ayant déclenché l'opération,
- L'heure de la connexion,
- Le système auquel il est accédé,
- Le type d'opération réalisée,
- Les informations ajoutées, modifiées ou supprimées des bases de données en réseau et/ou des applications de l'hôpital,
- La durée de la connexion (notamment pour l'accès Internet).

La direction respecte la confidentialité des données et des traces auxquelles il est amené à accéder dans l'exercice de ses fonctions, mais peut être amené à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs.

6.3 ALERTES

Tout constat de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits, de fonctionnement anormal ou, de façon plus générale, toute suspicion d'atteinte à la sécurité ou tout manquement substantiel à cette charte, doit être signalé au Responsable de la Sécurité du Système d'Information (RSSI) ainsi qu'une Fiche d'Evènement Indésirable rubrique RGPD

La sécurité de l'information met en jeu des moyens techniques, organisationnels et humains. Chaque utilisateur de l'information se doit d'avoir une attitude vigilante et responsable afin que les patients bénéficient d'une prise en charge sécurisée et que leur vie privée, ainsi que celle des personnels, soit respectée.

7. RESPONSABILITES ET SANCTIONS

Les règles définies dans la présente Charte ont été fixées par la Direction générale de l'établissement de santé dans le respect des dispositions législatives et réglementaires applicables (CNIL, ASIP Santé...).

L'établissement ne pourra être tenu pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé aux règles d'accès et d'usage des ressources informatiques et des services Internet décrites dans la Charte. En cas de manquement aux règles de la présente Charte, la personne responsable de ce manquement est passible de sanctions pouvant être :

- Un rappel ou un avertissement accompagné ou non d'un retrait partiel ou total, temporaire ou définitif, de l'accès aux moyens informatiques,
- Un licenciement et, éventuellement, des actions civiles ou pénales, selon la gravité du manquement.

Outre ces sanctions, la Direction de l'Hôpital est tenue de signaler toute infraction pénale commise par son personnel au procureur de la République.