

MENTIONS LEGALES

Version du 4 septembre 2026

PRESENTATION

La société Logicoss Digital Healthcare (ci-après « LOGICOSS DIGITAL HEALTHCARE » ou « LDH »), société à responsabilité limitée, enregistrée au Registre du Commerce et des Sociétés de Lyon sous le numéro 843 115 072, dont le siège social est 109 Boulevard de l'Europe, 69310 Pierre-Bénite, développe, édite et commercialise en mode SaaS (« Software as a Service ») la solution dénommée « logicoss », permettant la coordination et le suivi de dispositifs de sécurité, secours et santé mis en œuvre pendant des événements privés ou publics ou sur des sites privés ou publics, ainsi que des prestations associées.

La solution logicoss est également dénommée le Dossier Médical Informatique ou **DMI** dans la suite de ce document.

EXPLOITATION

La solution « logicoss » est accessible notamment via les adresses <https://app.logicoss.net> et <https://logicoss.net> et est la propriété de LDH.

Une application « logicoss Sensors » est également disponible sur App Store et Google Play afin de couvrir une partie du périmètre fonctionnel : tracking GPS, gateway bluetooth, etc.

Editeur : logicoss est édité par LDH.

Directeur de la publication : Gaspard LEBEL.

Siège social : 109 Boulevard de l'Europe, 69310 Pierre-Bénite , France.

Hébergement : L'hébergement de la solution logicoss est assuré par la société Amazon Web Services EMEA SARL dont le siège social est situé 38 AV JOHN F KENNEDY L 1855 99137 LUXEMBOURG et par ses deux sous-traitants français Amazon Data Services France SAS et Amazon Technological Services SAS

POLITIQUE DE CONFIDENTIALITE

La Politique de confidentialité de la société LDH est disponible au lien suivant : [Politique de confidentialité](#).

CONDITIONS D'ACCES ET D'UTILISATION

Article 1. OBJET DES CGU

Les présentes Conditions Générales d'Utilisation (ci-après « **CGU** ») ont pour objet de définir les conditions, droits, obligations, responsabilités et limites applicables à toutes utilisations du DMI par tout utilisateur.

Les CGU forment un contrat juridiquement contraignant opposable à chaque personne qui utilise le DMI.

LDH permet à chaque utilisateur d'utiliser le DMI, sous réserve du respect de l'ensemble des dispositions des présentes CGU.

Article 2. ACCEPTATION DES CGU

Chaque utilisateur est invité à lire avec la plus grande attention le présent document.

En accédant au DMI, chaque utilisateur reconnaît avoir lu, compris et accepté les présentes CGU, ainsi que la Charte d'Utilisation (ci-après), et avoir pris connaissance de la [Politique de confidentialité](#).

Article 3. CONDITIONS D'ACCES AU DMI

L'utilisateur reconnaît disposer de la compétence et des moyens nécessaires pour accéder et utiliser le DMI.

L'utilisateur se voit attribuer un accès au DMI exclusivement par un Administrateur de son Autorité d'Emploi. Cette Autorité d'Emploi a elle-même conclu un Contrat avec LDH en vue d'utiliser le DMI. Toute utilisation du DMI hors du cadre d'un Contrat est prohibée. Tout utilisateur peut accéder au DMI.

L'adresse email, le nom et éventuellement les prénoms et le mot de passe (ci-après les « **Identifiants** ») permettent à chaque utilisateur de s'identifier et de se connecter aux espaces dédiés sur le DMI.

Les Identifiants sont personnels et confidentiels et ne peuvent être modifiés que sur action de leur titulaire.

Chaque utilisateur est entièrement responsable de l'utilisation de ses Identifiants qu'il s'engage à conserver secrets et à ne pas divulguer sous quelque forme que ce soit à des tiers. En cas de perte, de vol ou de toute utilisation frauduleuse de ses Identifiants, l'utilisateur devra immédiatement en informer LDH ainsi que son Autorité d'Emploi. L'utilisateur peut solliciter le remplacement de ses Identifiants lorsqu'il existe un risque que ceux-ci soient utilisés par un tiers.

Chaque utilisateur est en conséquence seul responsable de l'utilisation du DMI réalisée avec ses Identifiants. Toute connexion ou transmission de données effectuée en utilisant les Identifiants sera réputée avoir été effectuée par l'utilisateur et sous sa responsabilité exclusive. En conséquence, LDH et tout tiers impliqué dans la fourniture du DMI ne pourra être tenu responsable de l'utilisation frauduleuse des Identifiants de l'utilisateur par un tiers.

Article 4. MISE A DISPOSITION DU DMI

LDH fera ses meilleurs efforts pour permettre une disponibilité continue du DMI pendant les périodes dédiées à son utilisation.

L'utilisateur reconnaît et accepte qu'en l'état actuel de la technique, LDH ne puisse pas garantir une disponibilité continue du DMI et que cette disponibilité peut ne pas être assurée en cas d'opérations de maintenance, de mise à jour ou à la suite d'événements échappant au contrôle de LDH pouvant créer des interruptions ou perturbations de service. Le DMI peut également ne pas être disponible en raison d'événements de force majeure tels que définis par la jurisprudence française, de dysfonctionnements relatifs aux réseaux de télécommunication et/ou tout autre dysfonctionnement technique. Dans de tels cas, LDH prendra les mesures raisonnables dont il dispose pour traiter ces interruptions ou perturbations.

L'utilisateur reconnaît et accepte que la connexion au DMI puisse être interrompue ou stoppée à tout moment par LDH. LDH s'efforcera d'en avertir préalablement les utilisateurs.

LDH se réserve également le droit de suspendre l'accès au DMI pour un ou plusieurs utilisateurs, notamment en cas :

- de perte, vol et/ou utilisation des Identifiants de l'utilisateur ;
- d'utilisation non conforme aux dispositions des présentes CGU.

Article 5. RESPONSABILITE

L'utilisateur reconnaît utiliser le DMI sous sa seule responsabilité. Il appartient notamment à l'utilisateur de se prémunir contre les risques de l'Internet et de prendre toutes les mesures nécessaires afin de protéger ses propres données, équipements et/ou logiciels de la contamination par d'éventuels virus qui pourraient affecter le matériel informatique qu'il utilise pour se connecter au DMI.

LDH et tout tiers impliqué dans la fourniture du DMI déclinent toute responsabilité en cas d'interruption du DMI, de survenance de dysfonctionnement ou de tout dommage résultant d'actes frauduleux de tiers ou d'utilisateur(s).

La responsabilité de LDH et de tout tiers impliqué dans la fourniture du DMI ne pourra être engagée pour une cause dont le fait générateur a pour origine un cas de force majeure, y compris si un tel cas de force majeure touche un de ses prestataires, ainsi que tout événement hors de son contrôle exclusif.

Dans la mesure autorisée par la loi applicable, LDH et tout tiers impliqué dans la fourniture du DMI ne sauraient être tenus responsables d'un quelconque dommage, quelle qu'en soit la cause, origine, nature et conséquence, découlant notamment :

- de l'utilisation non conforme, frauduleuse, illicite ou inappropriée du DMI par l'utilisateur ;
- de la consultation ou de l'utilisation du DMI et/ou du compte d'accès personnel de l'utilisateur par un tiers à qui l'utilisateur aurait communiqué ses Identifiants ou qui aurait eu accès au compte d'accès personnel de l'utilisateur sans faute de LDH ;
- des dommages de toute nature résultant de l'utilisation des informations fournies par le DMI ;
- de perturbations ou interruptions, bugs et/ou indisponibilité totale ou partielle du DMI, même mis en œuvre par LDH ;
- de tout dommage résultant d'une intrusion frauduleuse d'un tiers depuis le DMI.

D'une manière générale, en aucun cas LDH et tout tiers impliqué dans la fourniture du DMI ne peut être tenu de réparer les préjudices résultant d'un dommage direct ou indirect subi du fait de l'utilisation du DMI par l'utilisateur.

Article 6. COMPOTEMENT

Chaque utilisateur se doit d'utiliser le DMI de manière responsable, avec respect et courtoisie à l'égard des droits de LDH.

En accédant au DMI, l'utilisateur s'engage et garantit notamment :

- avoir un comportement conforme à l'ensemble des dispositions des présentes CGU et à respecter ces CGU ;
- respecter toutes les lois en vigueur y compris celles du pays d'où il accède au DMI ;
- communiquer des informations sur son identité exactes, exhaustives et à jour ainsi que sur l'identité de toute autre personne concernée (dans un tel cas, l'utilisateur doit s'assurer que la personne concernée a consenti à la communication de ses informations et a pris connaissance des informations relatives au traitement de ses données fournies par LDH) ;
- respecter les droits de propriété intellectuelle de LDH et des éventuels tiers ;
- agir de manière conforme à la destination du DMI.

En outre, l'utilisateur s'interdit, notamment :

- d'utiliser les fonctionnalités du DMI à des fins non prévues dans les CGU et/ou qui porteraient atteinte aux droits de LDH, d'un ou plusieurs autre(s) utilisateur(s) ou aux droits de tiers ;
- d'utiliser le DMI à des fins illicites ou illégales ;
- de communiquer à LDH des informations fausses, usurpées ou erronées ;
- de perturber ou interrompre le fonctionnement du DMI ou des serveurs ou réseaux connectés au DMI ;
- d'accéder à des données qui ne lui sont pas destinées ou d'entrer dans un serveur auquel l'utilisateur n'est pas autorisé à avoir accès ;
- de tenter de sonder, de scruter ou de tester la vulnérabilité d'un système et notamment du DMI ou de l'espace réservé à un autre utilisateur, ou encore d'enfreindre les mesures de sécurité ou d'authentification sans en avoir reçu l'autorisation ;
- d'usurper ou tenter d'usurper l'identité d'un autre utilisateur ou de tout tiers ;
- de nuire à une personne physique ou morale par le biais du DMI ;
- le piratage sous quelque forme que ce soit, l'intrusion dans des systèmes informatisés ou audiovisuels, hacking, propagation de virus, cheval de Troie ou autres programmes destinés à nuire sous quelque forme que ce soit.

Plus particulièrement, l'utilisateur s'interdit de diffuser via les encarts de texte libre et moyens de communications accessibles sur le DMI toute donnée ou contenu prohibé, illicite, illégal, contraire aux bonnes mœurs ou à l'ordre public, notamment et non limitativement des contenus à caractère diffamatoire, injurieux, obscène, offensant, violent ou incitant à la violence, ou à caractère raciste ou xénophobe, ainsi que toutes données personnelles de tiers sans leur consentement.

L'utilisateur doit se conformer aux lois et règlements applicables, notamment (sans que cette liste soit exhaustive) celles relatives à la vie privée incluant la protection des données, à la propriété intellectuelle, aux règles d'ordre public relatives aux contenus et informations pouvant être diffusés, au secret des correspondances et à l'interdiction d'interception des communications émises par voie de télécommunication.

Article 7. QUALITÉ DES INFORMATIONS

Les informations fournies sur le DMI le sont à titre informatif. LDH apporte le plus grand soin et met en œuvre tout moyen pour diffuser sur le DMI des informations de qualité.

LDH ne peut toutefois pas garantir de manière absolue l'exactitude et l'exhaustivité de l'ensemble de ces informations. Ainsi, LDH, soumis à une obligation de moyens, ne saurait être tenu pour responsable de tout préjudice, direct ou indirect, du fait d'une information mal utilisée et/ou qui se serait révélée inexacte ou incomplète ni de tous dommages résultant d'un tiers.

Article 8. LIENS HYPERTEXTES – ACCES AUX SITES TIERS

La création de liens hypertextes vers le DMI ne peut être faite qu'avec l'autorisation écrite et préalable de LDH.

Les liens hypertextes mis en place dans le cadre du DMI en direction d'autres ressources présentes sur le réseau Internet ne sauraient engager la responsabilité de LDH, ceux-ci étant communiqués à titre de commodité pour faciliter l'information du public. En conséquence, dans la mesure où LDH ne peut contrôler ces sites, LDH ne peut être tenu responsable de la mise à disposition de ces sites, et ne peut supporter aucune responsabilité quant aux contenus, publicités, produits, services ou tout autre matériel disponible sur ou à partir de ces sites.

Article 9. DROITS DE PROPRIÉTÉ INTELLECTUELLE

Le DMI y compris tous ses composants (tels que, sans s'y limiter, les marques, modèles, logos, images, textes, sons, documents, contenus et autres éléments affichés) est/sont une œuvre de l'esprit protégée(s) par la législation française et internationale en vigueur sur le droit d'auteur, le droit à la personnalité et la propriété intellectuelle, littéraire et artistique, les autres droits de propriété intellectuelle et les autres droits similaires (désignés ensemble les « Droits de Propriété Intellectuelle »). Le DMI, incluant tous ses composants, ainsi que tous les Droits de Propriété Intellectuelle y afférents, sont la propriété exclusive de LDH ou ses licenciés.

Les utilisateurs ne sont pas autorisés à utiliser le DMI (y compris ses composants) à d'autres fins que celles prévues aux présentes CGU (et autres conditions applicables). À cet égard, il est entendu que la diffusion, la copie, la duplication, la modification, l'altération, le transfert, la représentation, la distribution, la reproduction, la republication, le téléchargement, l'affichage, la transmission, la traduction, la vente et/ou l'exploitation, en tout ou en partie, de tout élément de le DMI, de quelque manière et à quelque fin que ce soit, est expressément et strictement interdite (dans la mesure permise par la loi applicable).

De même, la création d'œuvres dérivées à partir de, la rétro-ingénierie, le désassemblage ou toute autre tentative de recréation du code source (sauf disposition contraire de la loi), et l'attribution, la sous-licence ou le transfert de quelque manière que ce soit de tout droit sur, vers ou lié à l'Outil de Dossier Médical Informatique (y compris l'un de ses composants), est également expressément et strictement interdit.

Toute infraction à cette disposition peut rendre son auteur passible de poursuites. LDH ou tout autre titulaire de ces droits, pourra mettre en œuvre toute mesure ou action, y compris judiciaire, pour faire cesser une atteinte à ses droits, en particulier de ses Droits de Propriété Intellectuelle et se réserve le droit de demander des dommages et intérêts en cas d'une telle atteinte.

Article 10. DONNEES PERSONNELLES

LDH protège et utilise les données personnelles transmises par les utilisateurs dans les conditions prévues dans sa [Politique de Confidentialité](#) et conformément aux mentions d'informations communiquées aux utilisateurs lors de la collecte de leurs données. L'utilisateur reconnaît en avoir pris attentivement connaissance.

Article 11. INTEGRALITE

Si une ou plusieurs stipulations des CGU sont tenues pour non valides ou déclarées invalides en application d'une loi, d'un règlement ou à la suite d'une décision définitive d'une juridiction compétente, les autres stipulations garderont toute leur force et portée.

En cas de difficultés d'interprétation entre l'un quelconque des titres figurant en tête des clauses, et l'une quelconque des clauses, les titres seront écartés et le contenu de la clause concernée prévaudra.

Article 12. MODIFICATION DES CGU

Dans la mesure autorisée par la loi applicable, les CGU sont susceptibles de faire l'objet de mises à jour de la part de LDH. Les CGU précédentes sont alors résiliées de plein droit et remplacées par la nouvelle version qui est immédiatement applicable à l'utilisateur.

Article 13. CONTACT

Si un utilisateur souhaite contacter LDH au titre des CGU ou pour toute demande relative à l'Outil de Dossier Médical Informatique, il peut écrire à l'adresse suivante : contact@logicoss.com ou contacter LDH via la page support <https://support.logicoss.com>.

Article 14. DROIT APPLICABLE

Il est expressément entendu que tout litige lié à l'utilisation du DMI ou à l'exécution, l'interprétation ou la validité des présentes CGU sera soumis à la loi et aux juridictions françaises.

Tout litige susceptible de s'élever lié à l'utilisation du DMI sera de la compétence exclusive du Tribunal de commerce de Lyon, à l'exception de tout litige relatif aux Droits de Propriété Intellectuelle, qui sera soumis à la compétence exclusive du Tribunal Judiciaire de Lyon, quels que soient le lieu d'exécution des CGU, le domicile du défendeur, et ce même en cas d'une pluralité de défendeurs, appel en garantie, procédure en référé ou conservatoire.

CHARTRE D'UTILISATION

Synthèse :

La disponibilité, la sécurité, la confidentialité et le bon fonctionnement du DMI utilisé dans le cadre de Dispositifs Santé-Secours revêt un caractère stratégique pour l'ensemble de ses membres et de ses patients. La continuité de l'activité dépend d'une utilisation raisonnée des ressources informatiques mises à disposition des Utilisateurs.

L'accès au DMI peut présenter des risques en cas d'utilisation non conforme (ex : atteinte à l'image de LDH, divulgation d'informations confidentielles, violation de Données personnelles, etc.). La réalisation de ces risques peut engager la responsabilité civile et/ou pénale des Utilisateurs fautifs.

Afin de se prémunir au mieux contre ces risques, l'Utilisateur doit respecter, lorsqu'il accède à ces Ressources ou qu'il les utilise, un certain nombre de règles, notamment :

- Les règles de confidentialité, notamment s'agissant du respect du Secret médical :
 - L'accès au dossier d'un patient n'est autorisé qu'aux professionnels faisant partie de l'équipe de soin ayant pris en charge ledit patient : tout autre accès est illégitime ;
 - L'Utilisateur ne doit pas tenter d'accéder à des dossiers pour lesquels il n'est pas habilité, et même s'il est habilité, il ne doit accéder qu'aux seuls dossiers strictement nécessaires à sa mission ;
 - L'utilisation d'une messagerie sécurisée est obligatoire pour tout échange de Données de santé avec d'autres professionnels de santé en dehors de LDH ;
 - Les Données personnelles doivent être chiffrées et stockées dans des espaces sécurisés, leur collecte limitée à ce qui est strictement nécessaire et leur durée de conservation limitée.
- Les règles de sécurité physiques et logiques, visant à préserver la pérennité du SI des Dispositifs Santé-Secours utilisant le DMI :
 - Les moyens d'authentification sont personnels, confidentiels et non transmissibles ;
 - Les Ressources informatiques utilisées par les utilisateurs pour se connecter au DMI doivent être protégées physiquement et logiquement ;
 - En cas de mise à disposition de Ressources informatiques par LDH, celles-ci doivent être utilisées à des fins professionnelles. L'utilisation à titre personnel est tolérée, mais de manière raisonnable ;
 - La configuration initiale du poste de travail doit être conservée car elle a été étudiée afin de garantir le bon fonctionnement et la sécurité du DMI ;
 - La création de comptes utilisateurs pour des Ressources Humaines non fournies par le Client de LDH, et la connexion de celles-ci au DMI suppose l'accord préalable du Client de LDH ;
 - Il est par principe interdit d'utiliser des réseaux publics wifi non sécurisés ;
 - Toutes les actions des Utilisateurs sur le DMI sont tracées et pourront être auditées.
- Les règles d'éthique, de courtoisie et de professionnalisme, applicables en toutes circonstances :
 - Le devoir de réserve, la probité, la loyauté et la confidentialité s'appliquent en toutes circonstances ;

- L'Utilisateur doit faire preuve de politesse et de respect à l'égard de ses interlocuteurs ;
- Il est interdit de nuire à l'image de marque de LDH, à ses intérêts ou à sa réputation, de quelque manière que ce soit (par son comportement ou ses propos, notamment publiés sur des réseaux sociaux).

Toute violation de la Charte pourra faire l'objet de sanctions contractuelles et/ou pénales. Des audits ciblés et/ou aléatoires sont menés périodiquement afin de contrôler les accès et usages des ressources, particulièrement s'agissant des accès aux dossiers patients informatisés.

1. Objet

La présente Charte a pour objet :

- De préciser les principaux droits, les devoirs et les responsabilités des Utilisateurs dans le cadre de l'accès et de l'utilisation des Ressources mises à disposition par LDH ;
- De faire prendre conscience à chaque Utilisateur de l'importance de la sécurité des Ressources, de le responsabiliser sur les règles de confidentialité et de Secret professionnel et de l'alerter sur les sanctions encourues en cas de non-respect des règles.

Le référentiel légal et les définitions des termes en majuscule utilisés dans la présente charte figurent en Annexe 1 et 2.

2. Accès

Synthèse :

- Les moyens d'authentification sont personnels, confidentiels et non transmissibles ;
- Le fait d'utiliser les moyens d'authentification d'un tiers, même avec son accord, est interdit, l'Utilisateur étant seul responsable de leur confidentialité et usage ;
- Les mots de passe doivent respecter les règles édictées par LDH et être changés régulièrement, et au plus tous les 12 mois ;
- L'accès aux informations se fait au regard des nécessités professionnelles pour l'exercice de l'activité de chaque Utilisateur ;
- L'accès au dossier d'un patient n'est autorisé qu'aux professionnels de santé faisant partie de l'équipe de soin ayant pris en charge ledit patient. Tout autre accès est considéré comme illégitime et pourra faire l'objet d'une convocation de l'Utilisateur fautif puis le cas échéant de l'application de sanctions contractuelles et pénales ;
- Les Données personnelles sont soumises à une réglementation contraignante : l'accès et l'utilisation des Données personnelles ou encore la création d'un traitement de Données personnelles doit se faire dans le respect des principes de finalité, de transparence, de confidentialité, de sécurité, de minimisation, de proportionnalité et de pertinence.

2.1. Moyens d'authentification et mots de passe

L'accès au DMI est géré par l'Autorité d'Emploi, seule habilitée à délivrer les moyens d'authentification (identifiant et mot de passe) à chaque Utilisateur, selon les procédures d'autorisation en vigueur et au regard de ses missions.

L'accès au DMI est octroyé au regard des nécessités professionnelles de chaque Utilisateur. Lorsqu'un Utilisateur estime qu'il ne dispose pas des habilitations adaptées au bon exercice de ses activités professionnelles, il doit s'adresser à son responsable hiérarchique afin de les faire modifier.

Les moyens d'authentification sont personnels, confidentiels et non transmissibles, l'Utilisateur étant seul responsable de leur confidentialité et usage. Les utilisations faites à l'aide d'un moyen d'authentification propre à chaque Utilisateur sont réputées être le fait du détenteur de ce moyen d'authentification, sauf à ce que sa bonne foi puisse être démontrée.

Il est notamment interdit :

- De communiquer ses identifiants et/ou mots de passe à un tiers et ce afin d'éviter :
 - o Le risque d'erreur médicale ou d'accident de soin commis au nom du porteur des identifiants ;
 - o Le risque de perte de traçabilité précise des actes de soin effectués.
- D'utiliser les identifiants et/ou les mots de passe d'un tiers et ce afin de prévenir :
 - o L'usurpation d'identité (infraction pénale) ;
 - o L'introduction frauduleuse dans un Système de Traitement Automatisé de Données.

L'accès de l'Utilisateur au DMI pourra être suspendu, supprimé, limité ou réexaminé, pour des raisons de sécurité et le cas échéant sans préavis, notamment :

- Lors de la cessation de son activité professionnelle au sein de son service (changement de service, mutation, etc...) ou en cas de départ, conformément à la procédure applicable dédiée à cet effet ;
- Dans certains cas de cessation temporaire de l'activité professionnelle (maladie, congé de maternité, etc. : dans ces cas, l'Utilisateur doit s'organiser pour permettre à LDH d'accéder aux données professionnelles pour assurer la continuité d'activité) ;
- Dès lors qu'un usage abusif sera révélé (et ce, sans préjudice des actions disciplinaires et/ou pénales pouvant être initiées par LDH ou toute autre tiers), par exemple :
 - o En cas d'utilisation de moyens d'authentification autres que ceux octroyés à l'Utilisateur ;
 - o En cas d'utilisation en contradiction avec les règles professionnelles applicables, notamment s'agissant du secret médical ;
 - o Plus généralement en cas de manquement à la Charte ou de manquement aux lois et réglementations en vigueur.

Le supérieur hiérarchique s'assure de manière périodique que les droits d'accès accordés aux Utilisateurs sous sa responsabilité correspondent précisément à leurs rôles et missions. Il notifie à l'Autorité d'Emploi et si besoin à LDH dans les meilleurs délais toute habilitation excessive qui dépasserait les besoins de l'Utilisateurs au regard de ses fonctions.

L'utilisation de comptes non personnels (ex. : les comptes génériques ou les comptes partagés) doit rester exceptionnelle et justifiée. Dans le cas où l'Utilisateur y a accès, il est responsable de l'usage qu'il fait de ces derniers, et se doit de respecter les règles de sécurité du présent document, au même titre que pour son compte personnel.

S'agissant du mot de passe, l'Utilisateur doit se conformer aux préconisations de LDH :

- Définir un mot de passe complexe (au moins 8 caractères et comportant majuscules, minuscules, chiffres) ;
- Veiller à le modifier régulièrement afin d'éviter toute usurpation de son identité ;
- Alerter sans délai le RSSI de l'Autorité d'Emploi et LDH en cas de suspicion de compromission d'un moyen d'authentification.

Exemples de comportements abusifs et/ou sanctionnables :

- Inscrire ses mots de passe sur support papier ou électronique à proximité ou sur les Ressources Informatiques utilisés pour se connecter au DMI, ou les stocker en clair dans un fichier ;
- Se connecter au dossier patient avec le compte d'un tiers, même avec son accord ;
- Ne jamais modifier le mot de passe, ou supprimer le mot de passe.

2.2. Accès aux logiciels traitant des Données personnelles

Certains Utilisateurs disposent d'accès aux applications métiers traitant des Données personnelles dont des Données de santé, afin d'assurer la prise en charge des patients, ou encore dans le cadre de la gestion des ressources humaines.

La consultation frauduleuse ou la divulgation à des tiers de ces Données pourrait avoir un impact grave et irréversible sur le patient ou sur un autre Utilisateur. Les Utilisateurs sont donc soumis au secret le plus absolu sur ces données confidentielles protégées par la loi et dont la collecte, l'utilisation, la consultation, le stockage ou encore l'échange sont strictement encadrés par des mesures de confidentialité et de sécurité.

S'agissant précisément de l'accès aux Données de santé, sont soumis au Secret médical tous les Utilisateurs participant à la prise en charge des patients (ex. : professions médicales, paramédicales, personnels administratifs, sociaux, etc.) qui ont accès à des Données personnelles de santé dans le cadre de leurs fonctions.

Les conditions suivantes pour accéder aux dossiers patients doivent être impérativement respectées par ces Utilisateurs, sous peine de sanctions :

- Seuls peuvent accéder au dossier médical d'un patient les professionnels concourant directement à la prise en charge du patient, c'est-à-dire faisant partie de l'équipe de soin au sens de l'article L. 1110-12 du Code de la santé publique ;
- Ces professionnels ne peuvent accéder qu'aux seules Données du patient concerné, dans la mesure où cela est strictement nécessaire à l'exécution de leurs missions.

Accéder au dossier d'un patient en dehors des conditions ci-dessus est constitutif d'une violation du Secret médical, d'une atteinte à la vie privée des patients et susceptible de faire l'objet d'un recours contentieux du patient, contre l'Utilisateur fautif et contre son autorité d'Emploi.

Les Utilisateurs soumis au secret ne doivent pas tenter de contourner les dispositifs de sécurité ni accéder, ou tenter d'accéder, à des dossiers pour lesquels (i) ils ne sont pas habilités et (ii) même s'ils sont habilités, ils ne doivent accéder qu'aux seuls dossiers strictement nécessaires à l'exécution de leur mission. En d'autres termes, l'Utilisateur doit limiter l'usage des accès dont il bénéficie exclusivement aux tâches professionnelles qui lui sont confiées et qui en nécessitent l'utilisation.

Si un mauvais comportement est observé, des investigations seront menées et les protagonistes entendus puis sanctionnés en cas d'accès illégitime avéré.

L'Utilisateur doit alerter son supérieur :

- S'il estime ne pas disposer des habilitations adaptées au bon exercice de ses activités professionnelles (qu'elles soient trop larges ou pas assez) ;
- S'il constate qu'une personne ne dispose pas des habilitations adaptées au bon exercice de ses activités professionnelles.

Le supérieur hiérarchique s'assure que les accès octroyés à ses équipes sont adaptés à l'exercice de leurs missions. Le supérieur s'assure également que les droits d'accès accordés aux Utilisateurs sous sa responsabilité quittant leur service sont bien révoqués ou désactivés.

Enfin, en présence d'un traitement de Données personnelles (ex. : l'utilisation de Données personnelles pour un projet de recherche, utilisation d'un nouvel outil IT impliquant des données personnelles), l'Utilisateur (en tant que chef de projet) doit préalablement s'assurer qu'une revue de conformité RGPD a été effectuée auprès d'un référent DPO (notamment : réalisation d'une analyse d'impact sur la protection des données, information des patients, signature d'un contrat RGPD conforme dès qu'il y a un transfert de données à un tiers, inscription au registre des traitements, formalité CNIL réalisée le cas échéant).

Tout traitement de Données personnelles devra être effectué dans le respect des grands principes définis par le RGPD, rappelés dans la procédure interne dédiée à cet effet (limitation des finalités, minimisation des Données, confidentialité et sécurité, respect des droits des personnes).

Exemples de comportements abusifs et/ou sanctionnables :

- Consulter tout ou partie du contenu du dossier médical d'un proche, d'une personnalité publique, d'un collègue, et d'une manière générale d'un patient en dehors de toute prise en charge de ce tiers. La consultation de son propre dossier n'est pas non plus autorisée (sauf si la personne concernée est son propre médecin traitant) ;
- Révéler à des tiers non autorisés des informations couvertes par le secret ;
- Créer un dossier patient fictif ;
- Prendre des photos du dossier médical d'un patient ;
- Collecter et utiliser des Données de santé dans le cadre d'une recherche en dehors de tout cadre juridique ;
- Conserver dans son ordinateur des bases de Données personnelles sans encadrement sécurisé, ou mettre en production un projet impliquant un traitement de Données personnelles sans avoir consulté en amont le DPO de l'Autorité d'emploi.

2.3. Accès privilégiés des collaborateurs de LDH

Certains collaborateurs de LDH, Utilisateurs du DMI, disposent d'accès privilégiés à tout ou partie du DMI et des applications métiers (y compris à celles traitant des Données personnelles), leur permettant de gérer et de contrôler leur bon fonctionnement et leur sécurité (ex. : maintenance et support aux Utilisateurs).

Par leurs fonctions mêmes, ces Utilisateurs peuvent avoir connaissance d'informations confidentielles protégées par la loi. En ce sens, les règles de confidentialité renforcées visées au précédent article s'appliquent à ces Utilisateurs, également soumis au secret professionnel.

Seuls les Utilisateurs habilités de LDH sont autorisés à prendre la main à distance sur les Ressources Informatiques des Utilisateurs, afin de résoudre les problèmes signalés. Durant les heures ouvrées, la prise de main devra être réalisée avec l'accord préalable de l'Utilisateur. Par exception, en cas de situation grave, et notamment en cas d'attaque virale, la prise de main à distance pourra être réalisée sur toutes les ressources jugées suspectes sans requérir un accord préalable.

Exemples de comportements abusifs et/ou sanctionnables :

- Utiliser ses droits d'accès privilégiés de manière abusive en dehors de tout cadre ou toute mission précise ;
- Faire preuve d'indiscrétion et révéler à des tiers des informations confidentielles ;
- Prendre connaissance des mots de passe ou des messages privés des Utilisateurs.

3. Usage des Ressources

Synthèse :

- Occasionnellement, des Ressources informatiques peuvent être mises à disposition des Utilisateurs à des fins professionnelles ;
- La configuration initiale des Ressources informatiques ne doit pas être modifiée et ce pour des raisons de sécurité ;
- L'Utilisateur doit se déconnecter du DMI dès qu'il quitte son poste de travail ;
- Les obligations inhérentes au devoir de réserve, à la probité, à l'obligation de loyauté et au respect du Secret professionnel s'appliquent en toutes circonstances.

3.1. Usage professionnel et raisonné des Ressources

Les Ressources informatiques ont une finalité professionnelle et appartiennent à LDH. L'utilisation à titre personnel de certaines Ressources (précisément : téléphones fixes et portables, messagerie électronique, accès Internet) est tolérée de manière exceptionnelle et raisonnable.

L'Utilisateur doit veiller à clairement identifier la nature personnelle d'un message, d'un fichier ou d'une Donnée en indiquant « Privé » ou « Personnel » dans le titre de celui-ci ou en le stockant dans un répertoire portant cette même mention. L'Utilisateur fait seul son affaire personnelle et ce en temps utile de la sauvegarde et/ou de la destruction de ces messages et fichiers identifiés comme « personnels », notamment en cas de départ de ce dernier (ces documents identifiés comme « personnels » seront supprimés après le départ de l'agent).

Toutes les Données, tous les messages électroniques, tous les SMS émis, reçus ou stockés sur le système d'Information de LDH ou sur un matériel fourni par LDH et non identifiés spécifiquement comme étant « personnels » seront, par défaut, considérés comme étant professionnels et pourront être utilisés et consultés par LDH pour assurer la continuité de l'activité.

Dans tous les cas, l'utilisation des Ressources :

- Doit être conforme aux lois et aux bonnes mœurs, respecter les dispositions de la présente Charte et les règles liées au Secret médical ;
- Doit être compatible avec la continuité de l'activité (ex. : sauvegarde systématique des informations sur les supports de stockage et répertoires réseau dédiés)
- Ne doit pas perturber ou porter préjudice à la sécurité du SI (ex. : risque d'encombrement ou d'engorgement du réseau) ;
- Ne doit pas nuire aux tâches professionnelles incombant à l'Utilisateur ou à l'image de LDH ;
- Ne doit pas porter atteinte aux règles de propriété intellectuelle qui interdisent notamment de télécharger, reproduire et/ou de diffuser des œuvres de l'esprit sans autorisation préalable de son propriétaire.

L'Utilisateur a une obligation générale et permanente de confidentialité et de discrétion attachée à l'utilisation des informations, Données et documents électroniques disponibles sur le système d'information de LDH, et ce, pour la sauvegarde du patrimoine et des intérêts de celui-ci mais également des personnes concernées par ces informations, Données ou documents (patients, personnels, partenaires, etc.).

Exemples de comportements abusifs et/ou sanctionnables :

- Transformer des messages professionnels en « personnels » ;
- Introduire, exploiter ou tenter d'exploiter une faille de sécurité et/ou en faire la publicité ;
- Copier tout ou partie des codes sources d'un logiciel en dehors des droits autorisés par les licences correspondantes ;
- Tenir ou publier des propos dénigrants, diffamants, injurieux, homophobes ou sexistes (par téléphone, sur internet/intranet, par mail ou par tout autre moyen) ;
- Supprimer, altérer ou ne pas sauvegarder des informations nécessaires à la continuité de l'activité ;
- Subtiliser des documents professionnels.

3.2. Utilisation du poste de travail

La configuration initiale du poste de travail doit être respectée car elle a été étudiée afin de garantir le bon fonctionnement et la sécurité du système d'Information. Elle ne doit jamais être modifiée sans l'accord préalable et écrit de LDH. Les postes fixes ne doivent pas être déménagés d'un local à un autre sans autorisation.

Chaque Utilisateur doit :

- Utiliser les moyens de protection fournis par LDH tels que les câbles antivols et les armoires à clé, afin d'éviter les vols ou la dégradation des équipements ;
- Systématiquement verrouiller sa session s'il est amené à laisser la station de travail sans surveillance, et d'autant plus lorsque le poste est partagé entre plusieurs Utilisateurs.
- Exemples de comportements abusifs et/ou sanctionnables :
- Contourner ou désactiver les outils de sécurité, ou modifier leur paramétrage ;
- Télécharger ou utiliser des logiciels métiers non autorisés par LDH ;
- Laisser son ordinateur sans surveillance et/ou sans verrouillage par mot de passe.

3.3.Utilisation de Ressources personnelles

Les règles applicables dans la présente Charte s'appliquent également aux Ressources non fournies par LDH et interagissant avec le DMI (équipement personnel ou fourni par des tiers). Chaque Utilisateur doit veiller à ne pas connecter des ressources personnelles dont l'origine est suspecte.

Pour des raisons de sécurité, la connexion au DMI depuis tout équipement ou matériel personnel non sécurisé (notamment ordinateurs, téléphones, tablettes, clé USB) est déconseillée et ne peut en rien engager la responsabilité de LDH.

Pour se connecter au DMI, il est demandé à chaque Utilisateur de privilégier l'usage de matériels sécurisés, et de ne les connecter qu'à des postes de travail sécurisés (pourvus d'un antivirus).

L'Utilisateur d'un équipement personnel mobile doit prendre des précautions supplémentaires pour éviter le vol de cet équipement et une utilisation usurpée de celui-ci pour se connecter au DMI. Il est interdit de stocker des fichiers de Données personnelles sur des équipements personnels.

En cas de doute, l'Utilisateur s'adressera à son supérieur hiérarchique afin de mettre en œuvre les mesures de protection pour préserver la sécurité et la confidentialité des informations stockées.

Exemples de comportements abusifs et/ou sanctionnables :

- Utiliser des clés USB non fiables ou dont la provenance est incertaine ou douteuse (ex. : Goodies) ;
- Laisser un équipement personnel sans surveillance ;
- Ne pas installer ou désactiver les outils de sécurité sur son équipement personnel.

4. Traçabilité, contrôle et audits

Synthèse :

- Toutes les actions des Utilisateurs sur le DMI sont tracées ;
- Des audits ciblés et aléatoires sont menés périodiquement afin de contrôler les accès et usages, particulièrement s'agissant des accès aux dossiers patients informatisés ;
- En cas d'accès illégitime avéré et après convocation de l'Utilisateur fautif, des poursuites pourront être engagées.

4.1. Traçabilité et contrôle

Des mesures de contrôle et de suivi sont mises en œuvre dans le strict respect des principes de transparence et de proportionnalité des moyens de collecte, ceci uniquement à des fins de sécurité, de protection et de vérification du bon accès et usage des Ressources dans le respect des règles édictées par la présente charte et pour assurer la continuité de l'activité.

Les services compétents de LDH tracent quotidiennement les actions des Utilisateurs afin :

- De contrôler le respect du Secret professionnel à travers les contrôles de traces portant sur les outils métiers, particulièrement s'agissant de l'accès aux dossiers médicaux informatisés ;
- De garantir le bon fonctionnement des Ressources, la continuité d'activité, le volume d'utilisation, de détecter des anomalies de faire évoluer les Ressources en fonction des besoins ;
- De vérifier que les règles en matière de sécurité sont correctement appliquées et conformes à la politique de sécurité ;
- De détecter toute défaillance ou anomalie de sécurité, volontaire ou accidentelle, passive ou active, d'origine matérielle ou humaine ;
- De contrôler plus généralement le respect des règles d'utilisation et de sécurité du système d'information ;
- De pouvoir identifier et, le cas échéant, sanctionner des usages contraires à la présente charte, aux législations et réglementations applicables ;
- De pouvoir fournir des preuves nécessaires pour mener les enquêtes en cas de contentieux visant un Utilisateur ou un tiers, ou plus généralement de répondre aux requêtes des autorités publiques habilitées (services de police, autorités judiciaires...).

Précisément, LDH surveille, analyse et audit de façon périodique les dispositifs professionnels dont l'utilisation du DMI.

Cette surveillance consiste en une analyse des traces laissées par l'Utilisateur à l'occasion de l'utilisation du DMI. Les Données collectées sont entre autres :

- L'identifiant de l'Utilisateur ayant déclenché l'opération ;
- L'heure de la connexion ;
- Le type d'opération réalisée ;
- Les informations consultées, ajoutées, modifiées ou supprimées sur le DMI.

Les traces de connexion au DMI sont par principe conservées pendant 1 an (sauf obligations légales ou réglementaires particulières de conserver ces données sur une durée plus longue). Les traces des accès et actions réalisées sur les Données nominatives de santé sont conservées conformément à l'article R. 1112-7 du Code de la santé publique.

4.2. Accès par LDH aux Ressources de l'Utilisateur

Pour assurer la continuité de son activité, en cas de risque particulier susceptible de porter préjudice à LDH, à l'un de ses agents ou à un tiers (ex. : risque de sécurité, d'atteinte à la confidentialité ou de non-conformité réglementaire) ou dans le cas d'une enquête judiciaire, LDH pourra accéder et consulter :

- Les traces nominatives et actions d'un Utilisateur aux applications ;
- L'ensemble des Données, messages et fichiers professionnels stockés dans les Ressources confiées à l'Utilisateur. Dans ce cas où les Données, messages et fichiers sont expressément marqués par l'Utilisateur comme étant « personnels », LDH pourra y accéder en présence du propriétaire ou celui-ci dûment prévenu.

Les modalités d'accès aux informations médicales garantiront le respect du Secret médical. Elles ne pourront avoir lieu qu'en présence du professionnel de santé dépositaire de l'information après avoir

été préalablement informé, et à défaut de la présence du professionnel de santé, celle d'un représentant de la Commission Médicale d'Etablissement Locale ou Centrale.

Il est précisé que l'accord / la présence des Utilisateurs n'est pas requise en cas d'urgence (ex. : risque de sécurité du SI ou de manquement réglementaire, enquête judiciaire) ni pour les audits des traces nominatives d'un Utilisateur aux applications traitant des Données personnelles.

4.3. Audits réalisés afin de prévenir et sanctionner les accès illégitimes (violation du secret)

Dans l'objectif de prévenir et sanctionner les accès illégitimes aux dossiers traitant des Données personnelles, l'Utilisateur est informé que des audits sont menés par LDH, visant à étudier les traces d'accès aux dossiers traitant des Données personnelles.

Deux types d'audits peuvent être entrepris :

- Des audits ciblés sur un ou plusieurs Utilisateurs, en cas de signalement remonté à la DPO à l'adresse dpo@logicoss.com, par un tiers ou par la personne concernée (demande de droit d'accès suite à une suspicion d'accès illégitime au dossier médical) ;
- Des audits aléatoires sur un ou plusieurs Utilisateurs choisis au hasard, sur une journée donnée.

La procédure d'audit est en synthèse la suivante :

- Recherches des traces d'accès aux Données personnelles de santé par les Utilisateurs habilités de LDH ;
- Présentation des analyses pseudonymisées en commission dédiée à cet effet ;
- Édition du rapport de contrôle, signé par la DPO ;
- Convocation des agents incriminés par la hiérarchie pour confirmer ou infirmer le caractère illégitime des accès ;
- Sanctions en cas d'accès illégitime avéré.

4.4. Remontée des incidents

Toute anomalie suspectée ou avérée concernant le SI de LDH (ex. : les vols ou pertes de matériel, les vols ou pertes d'informations, ou les dysfonctionnements du poste de travail, un incident sur une application), ou toute violation des règles décrites dans le présent document, doivent être signalées :

- Au support SI ou ;
- Au responsable hiérarchique.

En outre, en cas d'accès accidentel à un mail, une pièce jointe ou un site Internet illicite ou potentiellement dangereux (site corrompu ou susceptible d'être vecteur d'une infection virale), l'Utilisateur doit immédiatement se déconnecter et informer le support SI.

Une fois déclarés, les incidents sont traités par les services compétents en fonction de leur nature.

5. Sanctions

En cas de non-respect de la présente Charte, LDH se réserve le droit de prendre des sanctions disciplinaires, dans le respect des procédures applicables, et ceci sans préjuger des éventuelles poursuites judiciaires, pénales et ordinaires qui pourraient être initiées à l'encontre des Utilisateurs concernés.

A titre d'exemples :

- Au titre des sanctions disciplinaires, l'Utilisateur fautif encourt notamment :
 - o Un avertissement ;
 - o Un blâme ;
 - o Une radiation du tableau d'avancement ou une rétrogradation au grade inférieur ;
 - o Une exclusion temporaire ou définitive ;
 - o Un licenciement ou révocation.
- Au titre des sanctions pénales :
 - o L'Utilisateur soumis au secret peut être condamné à un an d'emprisonnement et 15 000 euros d'amende en cas de révélation d'une information à caractère secret ;
 - o L'Utilisateur qui accède et/ou se maintient frauduleusement dans un SI peut être condamné à 3 ans d'emprisonnement et à 100 000 € d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce dernier, la peine est de 5 ans d'emprisonnement et de 150 000 € d'amende.
- Au titre des sanctions ordinaires, le Conseil de l'Ordre sera saisi et l'Utilisateur fautif pourra être sanctionné par ses pairs, encourageant ainsi une interdiction temporaire ou définitive d'exercer (radiation).

Les sanctions seront appliquées proportionnellement à la gravité de la faute commise ainsi qu'au préjudice subi.

Nonobstant les sanctions visées ci-dessus, LDH pourra également procéder à la restriction ou à la suspension immédiate des droits d'accès de l'Utilisateur à tout ou partie des Ressources informatiques. L'Utilisateur est alors informé par écrit des constats motivant l'intervention et pourra faire valoir sa position.

LDH pourra également décider une suspension immédiate des droits d'accès à titre conservatoire.

Concernant les Utilisateurs liés par un contrat de prestation ou une convention avec LDH, tels que les intérimaires, les partenaires ou les fournisseurs, toute violation des règles de la Charte pourra engendrer la rupture dudit contrat sans préjudice de tout dommages et intérêts que LDH pourrait être fondée à réclamer.

6. Entrée en vigueur et procédure

La présente Charte entre en vigueur à compter de sa mise à disposition sur l'écran de connexion du DMI.

La Charte sera modifiée en fonction du contexte législatif et réglementaire. Toute modification sera notifiée aux Utilisateurs par le biais du mailing, de la publication intranet et par voie d'affichage et, selon la nature des modifications, par une information (modification non substantielle) ou par un avis (modification substantielle) des instances représentatives centrales.

Pour toute question relative au document, la Direction Générale et le DPO de LDH peut être consulté.

7. Annexes

Annexe 1 : Définitions

CNIL : désigne la Commission Nationale Informatique et Libertés, créée par la loi Informatique et Libertés du 6 janvier 1978 et chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, publics et privés. La CNIL a un pouvoir de contrôle et de sanction.

Données personnelles : désigne toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (exemple : un nom, une photo, une radio, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc.)

Données personnelles sensibles : désigne des Données personnelles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des Données génétiques, des Données biométriques aux fins d'identifier une personne physique de manière unique, des Données concernant la santé ou des Données concernant la vie sexuelle.

Données personnelles de santé : désigne les Données relatives à la santé physique ou mentale, passée, présente ou future, 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.

DPO : désigne le délégué à la protection des données de LDH désigné à la CNIL, en charge de contrôler la conformité de LDH au regard de la réglementation applicable en matière de protection des données personnelles.

LIL : désigne la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Ressources informatiques ou Ressources : désigne tout élément physique ou logique, matériel, informatique, interagissant avec tout ou partie avec le DMI et comprenant :

- Des éléments matériels, tels que notamment : infrastructures de tout type, serveurs, data center, mais également les hubs, firewalls, équipements réseaux, équipements individuels remis à l'Utilisateur, tout périphérique et tout autre matériel informatique, connectique ou bureautique en ce compris les plateformes, câbles du réseau, photocopieurs, ordinateur et téléphones fixes ou portables, scanners, imprimantes, etc. ;

- Des éléments logiciels ou immatériels tels que notamment le système d'information (SI), les réseaux, les logiciels, progiciels, applications, fichiers, Données et bases de Données, l'intranet, l'extranet, le système de messagerie, les services Internet, etc.
- Les règles applicables dans la présente Charte s'appliquent également aux Ressources non fournies par LDH et interagissant avec le DMI (équipement personnel ou fourni par des tiers).

RGPD : désigne le Règlement Général sur la Protection des Données personnelles (RGPD), qui fixe le cadre légal en matière de protection des données personnelles.

RSSI : désigne le responsable de la sécurité des systèmes d'information.

Secret médical : désigne l'obligation de discrétion professionnelle imposée à l'ensemble des utilisateurs du DMI, et représente un droit fondamental pour le patient. La violation du secret médical, (condamnable par le code pénal et le code de la santé publique) est par exemple caractérisée lorsque des tiers non autorisés accèdent, quand bien même ils auraient les habilitations pour le faire, aux Données de santé de patients à l'insu de ces derniers et en dehors du cadre de la prise en charge.

Secret professionnel : désigne le principe de confidentialité applicable à certaines fonctions qui implique l'interdiction de divulguer à des tiers ou à des personnes non autorisées, des informations à caractère confidentiel (information sur les salaires notamment).

SI : désigne le Système d'information de LDH, englobant notamment le DMI.

Utilisateur : désigne :

- Toute personne physique, quel que soit son statut (professionnel de santé ou pas), son niveau hiérarchique ou son lieu d'accès, notamment : les salariés, les contractuels, les bénévoles, les volontaires, les stagiaires, ou encore les intérimaires qui, de manière permanente ou occasionnelle accède et/ou utilise le DMI ;

Violation de Données personnelles : une violation de sécurité, entraînant de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles Données.

Annexe 2 : Référentiel légal

Dans le cadre de l'accès et de l'utilisation des Ressources, les Utilisateurs se doivent d'être en conformité vis-à-vis des lois et des réglementations en vigueur, en particulier :

- Le Code Pénal :
 - Atteinte au secret médical ;
 - Consultation illégitime d'un dossier patient en dehors de la prise en charge ;
 - Intrusion frauduleuse dans un SI, fraude informatique ;
 - Usurpation d'identité ;
 - Atteinte aux bonnes mœurs (diffamation, injure, incitation à la haine, pornographie...).
- Le Code de la Santé Publique :
 - Respect absolu du secret médical, de la déontologie et des règles éthiques associées ;

- Respect des règles d'accès aux dossiers patients ;
- Respect des conditions d'hébergement de Données de santé.
- Le Règlement Général sur la Protection des Données personnelles (RGPD) et la Loi Informatique, Fichiers et Libertés (LIL) :
 - Revues de conformité / analyses d'impacts / inscription au registre ;
 - Information des personnes et collecte de Données strictement nécessaire à la finalité ;
 - Respect des droits des personnes (opposition, rectification, etc...).
- Le Code civil :
 - Secret des correspondances ;
 - Respect de la vie privée ;
 - Respect du droit à l'image.
- Le Code de la Propriété Intellectuelle :
 - Protection des logiciels, des écrits, des images, des marques et des bases de Données, des publications des recherches (contrefaçon) ;
 - Téléchargements illégaux ;
 - Respect des autorisations accordées.
- Le Code du travail :
 - Application des sanctions disciplinaires ;
 - Procédures de sanctions (convocation, échelle des sanctions).
- Les codes de déontologie applicables aux Utilisateurs :
 - Respect absolu du secret médical, de la déontologie et des règles éthiques associées ;
 - Respect des règles d'accès aux dossiers patients.