Document de management	DSI/DM/002 Version 01 Pages 11
	Date de diffusion : 13/08/2018

CODE DE CONDUITE CONCERNANT LA POLITIQUE DE PROTECTION DES DONNÉES

Destinataire	Directions de la Mutualité Française Comtoise		
Format	PDF	Support :	Ageval

Historique du document

Date	Version	Nature des modifications

Mot(s)-Clé(s)	RGPD, DSI, Sécurité, Données personnelles

Objectif(s)

- Identifier au sein de l'entreprise le circuit de l'information concernant la collecte des données personnelles, le type de données, l'archivage, la sauvegarde, les moyens de sécurité et les modes de consultations.
- Ce code de Bonne Conduite est applicable par l'ensemble des parties prenantes pour l'ensemble des activités de l'entreprise.

	Rédaction	Validation	Approbation	Diffusion
Nom	Jacques HOSOTTE	Claire GUILBAUD Laurence NEAULT Guillaume de SAGAZAN	Thomas JOUANNET	Jacques HOSOTTE
Fonction	Directeur Qualité Gestion des risques	Directrice Santé Autonomie Directrice des Ressources Humaines Directeur des Systèmes d'information	Président de la Mutualité Française Comtoise	Directeur qualité Gestion des Risques
Date	20 juin 2018	30 juillet 2018	8 Aout 2018	13 août 2018
Visa				

INTRODUCTION

Dans le secteur de la santé, la protection de la vie privée est d'une importance primordiale. Toutes les données y sont sensibles ? C'est pourquoi, il est essentiel de respecter méticuleusement la législation européenne (entre autres le Règlement Général sur la Protection des Données ou "RGPD") et nationale (la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel mais aussi la Loi du 13 juin 2005 relative aux communications électroniques) ainsi que d'en informer au maximum nos patients, nos résidents et nos clients.

La Présidence, la Direction Générale, les Directrices et les Directeurs opérationnels et l'ensemble des professionnels s'engagent à **gérer et utiliser les données personnelles de manière sécurisée, légale, loyale et transparente** afin d'assurer la continuité des soins et de traiter les dossiers dans les meilleures conditions.

Le code de Bonne Conduite ci-dessous explique quelles données sont collectées, pourquoi elles sont collectées, la durée du processus et dans quelles mesures les personnes concernées pourront les contrôler.

1. DÉFINITIONS DE « TRAITEMENT DE DONNÉES » :

Le RGPD définit le « traitement », les « données à caractère personnel » et les « données sensibles » comme :

« Traitement »: toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

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

« Données sensibles » : Dans nos établissements sanitaires, nos centres de santé dentaires, optiques, audiologie et nos EHPAD, les données de santé des patients et des résidents que nous recueillons sont considérées comme sensibles. Leur connaissance est indispensable à la continuité de la prise en charge de nos patients et de nos résidents.

Pour chaque logiciel métier est identifié un responsable de traitement des données personnelles des patients et des résidents. Le tableau récapitulatif en annexe 1 précise les éléments précédents.

Chaque responsable de traitement définit lui-même les données minimales nécessaires à la sécurité des patients, des résidents et des clients et utiles à la continuité de leur prise en charge, tout en collectant les données sensibles (patients, résidents) et personnelles (activités optique et audio) pendant la durée de leur prise en charge avec leurs propres moyens et finalités (par exemple élaboration et mise à jour d'un dossier administratif dans nos activités sanitaires et dans nos EHPAD, recherche d'adresse afin d'envoyer une facture ou un rappel de facture, enrichissement des données de santé, des prescriptions médicales, des observations médicales, réponse aux patients, résidents et aux familles et traitement des plaintes et des réclamations venant des patients, résidents, des familles, des pouvoirs publics ou des organisations de consommateurs, etc.).

2. SUJETS PROTÉGÉS PAR LE PRÉSENT CODE :

Ce code de conduite s'applique à toutes les personnes physiques suivantes :

1. Les patients de nos activités sanitaires : polyclinique de Franche Comté, Polyclinique du Parc, HAD Franche Comté et HAD Jura.
2. Les résidents de nos EHPAD.
3. Les patients des cabinets dentaires.
4. Les clients de nos activités optique et audio.
5. Les salariés de toutes nos activités.
6. Les membres des conseils d'administration.

Ce code de conduite s'applique également aux personnes en visite dans nos bureaux ou aux personnes qui visitent nos sites web qui peuvent nous laisser leurs coordonnées ou encore lors de l'utilisation de nos éventuelles applications mobiles.

La Mutualité Française Comtoise et tous ses professionnels respecteront leurs obligations ainsi que les droits des personnes concernées chaque fois que leurs données seront traitées par l'une ou l'autre de ses activités ou par l'un ou l'autre de ses membres.

3. FINALITÉ DU TRAITEMENT DE DONNÉES :

La Mutualité Française Comtoise et tous ses professionnels ne traitent des données à caractère personnel que si elles sont nécessaires à des finalités déterminées.

Dans le cas des dossiers de patients et de résidents, cela concerne les données nécessaires à la continuité de la prise en charge desdits patients et résidents : informations administratives, données de consultation médicale initiale, recueil de données infirmier, prescriptions médicales, transmissions ciblées, observations médicales, diagrammes de soins, partogrammes, comptes rendus d'hospitalisation, compte rendu opératoire, radios, résultats de laboratoires et lettres de sortie.

Dans le cas des dossiers de nos consultants en dentaire et de nos clients en optique et en audio les données personnelles et les données sensibles sont les suivantes : données administratives, devis, radios, observations dentaires.

Dans le cas du recouvrement d'une créance auprès d'un patient ou d'une famille de résident, les informations administratives du patient ou du résident sont traitées (nom, prénoms, dates de naissance, lieux d'habitat, motif du recouvrement).

Le processus de recouvrement se fait dans des mesures légitimes et proportionnelles.

Dans le cadre des dossiers de salariés, sont recueillies toutes les données utiles et proportionnelles à l'exercice des professions des collaborateurs : curriculum vitae, adresse postale, adresse mail, coordonnées téléphoniques, coordonnées d'une personne à prévenir en cas d'urgence, relevé d'informations bancaires, photographie, copie des diplômes, copie carte d'identité ou du titre de séjour autorisant à travailler sur le territoire français, une copie de l'attestation de Sécurité Sociales, extrait de casier judiciaire, copie de la reconnaissance éventuelle de travailleur handicapé, justificatif d'inscription à l'ordre (professionnels de santé), numéro ADELI ou numéro RPPS (pour les professionnels de santé), identités, coordonnées, numéro de sécurité sociale et date de naissance des ayant droit pour les garanties complémentaire santé et prévoyance.

4. LA SÉCURISATION DES DONNÉES :

1. La Mutualité Française Comtoise ainsi que toutes les directions fonctionnelles et les directions des activités forment leurs collaborateurs aux Bonnes pratiques d'utilisation des données sensibles et confidentielles. Le responsable de la sécurité des systèmes d'information et le directeur des systèmes d'information engagent des actions de formation annuelles à ce sujet.

2. Dans le cadre du programme d'audit interne annuel, des audits internes portent sur la sécurité et la protection des données personnelles.

3. Les responsables de traitement des données personnelles participent à la politique de sensibilisation des professionnels des activités au respect des Bonnes Pratiques des données personnelles. Le responsable de la sécurité des systèmes d'information et le directeur des systèmes d'information proposent des diaporamas de sensibilisation à la sécurité des systèmes d'information.

4. Le responsable de la sécurité des systèmes d'information et le directeur des systèmes d'information peuvent faire appel à des ressources externes spécialisées pour garantir la sécurité des réseaux, des infrastructures et les systèmes d'information utilisés. En outre, la Mutualité Française Comtoise utilise des mesures techniques afin de protéger les données en cause, comme par exemple : protection par mot de passe, pare-feu, antivirus, détection des intrusions et des anomalies et contrôles d'accès pour l'ensemble de ses collaborateurs.

5. Dans le cadre de ses relations avec ses sous traitants qui hébergent des données sensibles de patients, la Mutualité Française Comtoise s'assure auprès d'eux de leur politique de sécurité et s'engage à partager avec eux un contrat de traitement de données spécifiant que ledit sous traitant n'agira que sur la seule instruction du responsable du traitement et sera tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu.

6. En cas de violation de données à caractère personnel susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, une fiche de signalement d'événement indésirable sera documenté et une information sera faite à la personne concernée, décrivant en des termes clairs et simples la nature de la violation de données à caractère personnel et contenant un point de contact auprès duquel des informations supplémentaires peuvent être obtenues ainsi que les conséquences probables de la violation et les mesures prises ou proposées par le responsable du traitement à ce sujet. Dans ce cas, le responsable du traitement en notifie la violation en question à l'Autorité de protection des données, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.

7. Les directions et les professionnels doivent appliquer une approche basée sur les risques : cela signifie que les professionnels sont encouragés à prendre les mesures de protections nécessaires qui correspondent au niveau de risque de leurs activités de traitement de données.

5. ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES :

Une analyse d'impact préalable relative à la protection des données est effectuée lorsqu'un traitement de données personnelles envisagé, compte tenu de sa nature, sa portée, son contexte et ses finalités, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques concernées.

L'utilisation ou l'implémentation de nouvelles technologies peut être un indicateur de l'existence d'un haut risque.

Cette analyse d'impact contient au moins :

- Une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement.
- Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités.
- Une évaluation des risques pour les droits et libertés des personnes concernées.
- Les mesures prévues afin de faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.
- Le présent code de conduite est pris en compte dans l'analyse d'impact relative à la protection des données.

6. DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO) :

Un seul délégué à la protection des données a été désigné pour la Mutualité Française Comtoise.

Pou des raisons de cohérence de vision et de démarche entre la sécurité des systèmes d'information et la sécurité des données personnelles et au regard des exigences de la politique de sécurité des systèmes d'information en établissements de santé, **le délégué à la protection des données personnelles est le responsable de la sécurité des systèmes d'information** :

Jacques HOSOTTE
MUTUALITE FRANCAISE COMTOISE
Directeur Qualité Gestion des risques
Responsable de la sécurité des systèmes d'information
67 rue des Cras
25041 BESANCON CEDEX
Portable : 06 70 35 41 06
Tél : 03 81 65 80 07

Il informe et conseille les activités et leurs professionnels au sujet de leurs obligations qui découlent du RGPD et d'autres dispositions concernant la protection de données.

Il contrôle si les mesures de protection de données sont respectées et est la personne référente pour les autorités de contrôle.

7. COMMUNICATION DES DONNÉES À DES TIERS :

Les données à caractère personnel ne sont pas transférées à des tiers, sauf dans les cas suivants :

- Dossiers anonymisés du PMSI. L'accès par des industriels de santé aux données du Programme de Médicalisation des Systèmes d'Information (PMSI) de l'Agence technique de l'information sur l'hospitalisation (ATIH) sont mises à disposition via une solution sécurisée. Le responsable de traitement (médecin DIM) a l'obligation de documenter les projets menés dans le registre des activités de traitement. Les études menées doivent présenter un caractère d'intérêt public et aucun appariement avec d'autres données à caractère personnel n'est possible. Ledit responsable de traitement doit enregistrer leurs traitements auprès d'un répertoire public tenu par l'INDS. Les industriels devront recourir à un bureau d'études/laboratoires de recherches ayant réalisé un engagement de conformité au référentiel fixé par l'arrêté du 17 juillet 2017 auprès de la CNIL. Ils devront également faire réaliser un audit indépendant tous les 3 ans sur l'utilisation des données et le respect de l'interdiction des finalités interdites.

- La direction financière et la direction des ressources humaines peuvent faire appel à des mandataires ou à des avocats. La Mutualité Française s'assure auprès d'eux qu'ils traitent les données personnelles des patients, résidents et des professionnels, tout comme nous, d'une manière sûre, respectueuse, légale, loyale et transparente.

- Dans le cadre de recherches et d'enquêtes, il arrive que nous utilisions des données anonymes à des fins de recherche ou d'enquête et le cas échéant pour l'information de la direction générale, aux autorités publiques ou des communications de presse. Ces données ne sont jamais reliées à des personnes identifiables.

8. LES DROITS ET POSSIBILITÉS D'ACTION DES PERSONNES CONCERNÉES :

Les personnes concernées ont le droit d'accès gratuit aux données qui les concernent.

Elles peuvent demander :

- Si nous traitons ou non des données à caractère personnel,
- Pour quelles finalités nous les traitons,
- Les catégories de données que nous traitons,
- À quelles catégories de destinataires nous les communiquons,
- L'origine des données traitées et
- La logique sous-jacente au traitement automatisé de certaines données à caractère personnel.

Le droit d'accès peut être exercé par un écrit au responsable du traitement de chaque logiciel.

Afin d'exercer le droit d'accès et pour empêcher toute divulgation non autorisée ou illicite d'informations personnelles, une preuve d'identité est exigée : une copie de la face avant de la carte d'identité du demandeur ou de la personne concernée.

Chaque responsable de traitement de données s'engage à répondre aux demandes d'accès dans les meilleurs délais, et au plus tard dans un délai d'un mois. Ce délai commence à partir de la réception par le responsable du traitement de données de la demande écrite ainsi que de tous les éléments utiles et nécessaires

Qui plus est, le responsable du traitement fait parvenir une copie des données personnelles traitées à la personne concernée. Si le responsable du traitement ne fournissait pas la réponse correcte à la demande, le délégué à la protection des données saisirait la cellule opérationnelle des risques et le Comité Exécutif de la Mutualité Française Comtoise afin de contrôler la conformité entre le suivi de la demande et la déontologie des responsables de traitement des données.

Dans le cadre où une plainte serait formulée par le demandeur, celle-ci sera examinée par la cellule opérationnelle des risques. S'il s'avère qu'elle est justifiée, la cellule opérationnelle des risques en relation avec le responsable du traitement concerné sera invitée à apporter une solution, communiquée au plaignant.

De plus, un plaignant peut s'adresser à l'Autorité de Protection des Données, la CNIL, notamment dans le cas où aucune réaction à la demande n'est obtenue ou si la demande est refusée ou si la réponse n'est pas satisfaisante.

Il convient ici de faire l'état des droits des patients, résidents et clients :

- Le droit de rectification,
- Le droit d'effacement,
- Le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques la concernant ou l'affectant de manière significative.
- Le droit de minimisation des données : celui-ci entérine le fait que le responsable du traitement devra être en capacité de garantir que « seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement seront traitées » comme défini dans l'article 25 du règlement. Autrement dit, les responsables de traitement devront veiller dès le départ, à limiter la quantité de données traitées. De même, une fois la finalité du traitement atteinte, les données devront être systématiquement supprimées, sauf obligation de conservation légale particulière.

L'obligation est aussi faite au propriétaire des données de signaler toute modification, comme un changement de domicile ou un changement d'adresse email. D'ordinaire cette obligation est comprise dans le contrat sous-jacent à la récupération des données personnelles.

9. REGISTRE DES ACTIVITÉS DE TRAITEMENT :

Le délégué à la protection des données et les responsables de traitement tiennent un registre de leurs activités de traitement de données personnelles.

Ce registre contient : le type de données traitées, les finalités du traitement, les destinataires des données, l'endroit où les données seront conservées, comment les données seront sécurisées et les délais de conservation ainsi que les catégories des personnes concernées par le traitement (employés, fournisseurs, clients, débiteurs, etc.).

10. DÉLAIS DE CONSERVATION DE DONNÉES PERSONNELLES :

10.1. Dossiers patients et dossiers résidents :

La durée de conservation des dossiers patients (dossier administratif + dossier médical) est de vingt ans (période allongée le cas échéant pour les mineurs).

Cette durée constitue une durée de conservation des archives minimale en raison de leur adéquation éprouvée avec les réalités médicales et scientifiques et de la garantie du droit d'accès des patients à leur dossier, cette durée pouvant bien évidemment être allongée par les médecins spécialisés dans le traitement ou la prévention de pathologies requérant une plus longue période d'observation, pour éliminer tout risque connu de révélation du dommage.

Les modalités d'archivage des données personnelles des patients et des résidents seront les suivantes :

Les dossiers doivent être conservés dans des conditions permettant d'assurer leur confidentialité et leur pérennité.

1 – Dossier « papier » :

Le reliquat des dossiers après transmission et tri peut s'avérer important et constituer un encombrement pour un établissement. Il a été fait appel à une société d'archivage. Un contrat lie les deux parties.

2 – Dossier « informatique » :

L'écrit sous forme électronique ne vaut preuve qu'à condition que son auteur puisse être dûment identifié et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité et porte la date de création du document.

Cette notion de fidélité et de durabilité a été traduite par le critère fonctionnel global « d'intégrité ». L'intégrité d'un document numérique peut être assurée, en pratique, par différents moyens techniques :

- Copie fidèle : elle doit visuellement se présenter comme l'original avec les indications du papier à en-tête et la signature de l'expéditeur. Il convient d'opter pour des systèmes de stockage optique, horodaté, non réinscriptibles (Worm) ou disques magnétiques, rendus non réinscriptibles à l'aide d'un logiciel.
- Copie horodatée : le document n'a de valeur que si la preuve est apportée qu'il a été créé et stocké sous forme numérique au jour de son établissement.
- Copie durable : les documents doivent rester lisibles très longtemps. Il convient d'opter pour les formats électroniques standardisés (basés sur XML, PDF ou TIFF (pour les images)). Quand les documents archivés ne sont plus conformes, il peut être nécessaire de les convertir. Le support utilisé pour l'archivage doit lui aussi offrir des garanties de pérennité. Les supports non gravés, CD et DVD, n'offrent pas de garantie de pérennité. Le disque optique numérique non réinscriptible est la solution à privilégier, encore qu'on ne soit pas tout à fait assuré de la durée de vie, même des supports en verre au-delà de 5 à 10 ans

10.2. Dossiers clients et dossiers des professionnels :

En ce qui concerne les documents administratifs des clients (audio et optique) et des professionnels, les données personnelles sont conservées à ce jour sans date de destruction prévue.

11. LES SITES WEB :

Nos sites web peuvent être visités sans devoir partager des données à caractère personnel quelconques. Les personnes concernées peuvent interagir au sein de nos sites en nous laissant leurs coordonnées et des commentaires.

Nous veillons de la même manière à respecter leurs droits de rectification ou d'effacement si l'un de nos visiteurs venait à nous le demander.

12. PRISE DE CONTACT AVEC LE DELEGUE A LA PROTECTION DES DONNEES :

Pour toute information concernant le contenu du RGPD et sa mise en œuvre, la prise de contact auprès du délégué à la protection des données peut se faire par écrit, téléphoniquement, électroniquement ou via les sites web respectifs.

Le droit d'accès aux données des personnes concernées ainsi que les requêtes de rectification ou de suppression doivent se faire par écrit comme susmentionné au chapitre 8.

13. APPLICATION ET CHANGEMENTS DU PRESENT CODE DE BONNES PRATIQUES :

Tous les professionnels de l'entreprise s'engagent à appliquer le présent code de conduite de la sécurité des données personnelles.

Les personnes concernées (patients, résidents, clients) peuvent en demander ou consulter la dernière version sur les sites web de la Mutualité Française Comtoise.

Les professionnels de l'entreprise peuvent consulter ledit code de conduite dans le logiciel Ageval (logiciel de gestion documentaire).

Le délégué à la protection des données est à même de proposer une mise à jour dudit code de conduite sur la base de l'évolution des textes règlementaires européens ou nationaux.

Le dernier code de conduite a, en cas de conflit, priorité sur les versions antérieures des codes de conduite.

Annexe1

Activité	Identification du traitement	Responsable du traitement
Etablissement Hébergement Personnes Agées Dépendantes	Logiciel NET SOINS	Claire GUILBAUD
Optique Audio	Logiciel COSIUM Bases clients exportées	Christelle GAUTIER Cyril BAERH)
Dentaire	JADE MON DOCTEUR	Christelle GAUTIER
Direction Financière	Données administratives Données immobilières Assemblée générale Dossier admission résident Logiciel SAGE X3 Logiciel NETFACTU Logiciel SuiteOffice	Philippe THOMAS
Direction Qualité	Logiciel AGEVAL	Laure PEUVRIER
Direction Générale	Données transmises aux institutions	Sandrine BRENET
Direction Ressources Humaines	Logiciel ALICIA	Laurence NEAULT
Hospitalia Mutualité (MCO)	Hôpital Manager DPI Bloc Opératoire Direct consult GAP	Annick LEMAIRE Yannick RIGAUD
Hospitalia Mutualité (HAD)	ANTHADINE	Delphine MESSELET
Direction Achat Logistique	Logiciel SAGE X3 (base fournisseurs)	Pierre SARRAND
Communication	Prises de contact internet	Frédéric BEZOMBES
Présidence	Données liées aux administrateurs et délégués AG	Marie Claire BORDY