Délibération n° 2021-159 du 21 juillet 2021

de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« *Echange de données de santé à travers un système de messagerie sécurisée* »

exploité par le Département des Affaires Sociales et de la Santé

présenté par le Ministre d'Etat

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe du 4 novembre 1950 ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole additionnel ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu Ordonnance Souveraine n° 5.640 du 14 décembre 2015 portant création d'une Direction de l'Action Sanitaire ;

Vu l'Ordonnance Souveraine n° 7.995 du 12 mars 2020 portant création de la Direction des Services Numériques ;

Vu l'Ordonnance Souveraine n° 8.337 du 5 novembre 2020 relative aux données de santé à caractère personnel produites ou reçues par les professionnels et établissements de santé ;

Vu l'Arrêté Ministériel n° 2018-1108 du 26 novembre 2018 portant application de l'article 3 de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée, et son annexe, le référentiel d'exigences concernant la qualification des Prestataires d'Informatique en Nuage et d'Hébergement (PINH) ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'avis déposée par le Ministre d'Etat le 25 mars 2021 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Echange de données de santé à travers un système de messagerie sécurisée* » ;

Vu la prorogation du délai d'examen de ladite demande d'avis notifiée au responsable de traitement le 21 mai 2021, conformément à l'article 19 de l'Ordonnance Souveraine n° 2.230 du 19 juin 2009, modifiée, susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 21 juillet 2021 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Afin de sécuriser l'échange de données de santé entre professionnels de santé et des secteurs sanitaires, et le cas échéant social et médico-social dans le cadre de la prise en charge des patients, le Gouvernement Princier souhaite mettre en place un service de messagerie sécurisée.

Ledit traitement, objet de la présente délibération, est donc soumis à l'avis de la Commission conformément à l'article 7 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

I. Sur la finalité et les fonctionnalités du traitement

Ce traitement a pour finalité « *Echange de données de santé à travers un système de messagerie sécurisée ».*

Les personnes concernées sont les professionnels habilités (professionnels de santé et des secteurs sanitaires, et le cas échant social et médico-social), les patients pris en charge par ces professionnels habilités, le personnel habilité de l'Administration et du prestataire.

Enfin, le responsable de traitement indique que « *La solution repose sur le principe de fonctionnement d'un coffre-fort. Le professionnel habilité rédige un message incluant ou non des pièces jointes à partir d'une boîte mail sécurisée et à destination d'un/plusieurs professionnel(s) habilité(s). Le message et les données sont stockés dans un coffre-fort et mis à disposition du destinataire. Le destinataire est prévenu de la mise à disposition de ce message et doit se connecter au serveur de messagerie pour récupérer le message de manière sécurisée* ».

Les fonctionnalités sont ainsi les suivantes :

- création d'un compte utilisateur permettant d'être intégré à l'annuaire et d'échanger des données de santé de manière sécurisée ;
- accès à la solution via une interface sécurisée accessible par authentification (login/pwd) ;
- envoi et réception des données chiffrées par la messagerie sécurisée vers un ou des membre(s) de l'annuaire de la sphère de confiance ;
- fonctionnalités d'une boîte mail : tri, recherche, création de sous-dossier, envoi, réponse et transfert de message ;
- envoi de la donnée par des connecteurs DPI (serveur d'archivage pour professionnel de santé) ;
- réception de données sur application sécurisée Android/IOS (téléchargeable depuis AppStore et PlayStore) ;

- accès à l'annuaire des professionnels de santé de la Principauté de Monaco recensés, des professionnels de santé des territoires limitrophes (Alpes-Maritimes) ;
- création de listes de distribution de professionnels de santé pour des envois multiples de données (uniquement pour la solution intégrée aux messageries d'établissement, non disponible pour la version webmail) ;
- production de statistiques d'utilisation de la messagerie sécurisée de santé (sans données de santé) ;
- création de liste de patients par le professionnel habilité ;
- envoi de données chiffrées par messagerie sécurisée vers un patient présent dans la liste des patients du professionnel ;
- interconnexion en SSO avec le Portail Monaco Santé.

La Commission constate ainsi que la finalité du traitement est déterminée et explicite, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

II. Sur la licéité et la justification du traitement

Le responsable de traitement indique que le traitement dont s'agit est tout d'abord justifié par un motif d'intérêt public de l'Etat de Monaco.

A cet effet, la Commission prend acte que ledit traitement va « *permettre l'échange et le partage de manière sécurisée des données de santé entre les professionnels et établissements de santé, et plus largement de tous professionnels habilités à en recevoir communication sur le territoire de la Principauté de Monaco* ».

Elle constate que « *Les articles 7 et 11 de l'Ordonnance Souveraine n° 8.337 du 5 novembre 2020 relative aux données de santé à caractère personnel produites ou reçues par les professionnels et établissements de santé prévoient en ce sens que toutes mesures pour assurer la disponibilité, l'intégrité, la confidentialité et la traçabilité des données contenues dans les dossiers médicaux des patients, doivent être prises par les acteurs du secteur médical (professionnels exerçant dans un établissement de santé ou non)* ».

La Commission relève en outre que « *le Référentiel d'exigences concernant la qualification des prestataires d'informatique en nuage et d'hébergement (PINH) pris au titre du paragraphe C) de l'article 3 de l'Ordonnance Souveraine n°5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée (en Annexe à l'Arrêté Ministériel n° 2018-1108 du 26 novembre 2018) permet de fixer un cadre d'exigences applicables en matière de sécurité des informations pour les prestataires d'informatique en nuage et d'hébergement et notamment pour les données dites sensibles* ».

Le responsable de traitement indique également que dans le cadre de la transition numérique, la Délégation Interministérielle chargée de la Transition Numérique (DITN) *« a pour mission de développer des usages et pratiques numériques en matière de e-santé ainsi que d'effectuer une sensibilisation constante dans l'échange des informations sensibles relatives aux patients, avec l'aide du Service Métier (la Direction de l'Action Sanitaire du DASS) dans le but de créer en Principauté un espace de confiance au sein duquel les professionnels habilités pourront échanger des données de santé de manière dématérialisée et en toute sécurité* ».

A cet effet, il indique que « *de par ses missions, la Direction des Services Numériques de la DITN est chargée de porter les projets relatifs au développement de services numériques en matière de e-santé d'une part, et de structurer et animer un ecosytème de partenaires technologiques pour le compte du Gouvernement en matière de e-santé d'autre part* ».

La Commission prend note que *« la Direction de l'Action Sanitaire rattachée au Département des Affaires Sociales et de la Santé de la Principauté a pour mission de contribuer à l'élaboration*

de la politique de santé publique de Monaco afin d'assurer une planification de l'offre de soins au regard des besoins de la population » et que *« De fait, le présent traitement relatif à l'utilisation d'une messagerie sécurisée de santé permet d'exercer de manière pertinente et appropriée les missions »* dont sont investis les Services concernés du Gouvernement Princier (DSN/DASA).

Le responsable de traitement précise ainsi que « *L'Etat de Monaco met donc à disposition des professionnels du secteur de la santé un outil permettant d'assurer un niveau élevé de protection des données de santé des patients en créant un espace de confiance pour l'échange et le partage de ces données* » et que « *le traitement est directement adressé :*

- *Aux usagers et aux acteurs concernés du secteur de la santé à savoir les professionnels de santé ou tout autre professionnel habilité qui ont pour obligation d'assurer la sécurité des données de santé collectées de leurs patients dans le cadre du parcours de soins, d'une part ;*
- *Aux patients pris en charge sur le territoire de la Principauté de Monaco dont la sécurité des données les concernant se voit renforcée, d'autre part* ».

Le responsable de traitement indique par ailleurs que le traitement est justifié par le consentement des personnes concernées.

A cet égard, la Commission relève que « *Lors de la première connexion, le professionnel habilité doit accepter les Conditions Générales d'Utilisation afin de poursuivre son utilisation de la Messagerie Sécurisée de Santé. Il a également la possibilité de les télécharger* ».

Elle note en outre que « *Le consentement des patients au traitement de leurs données à caractère personnel dans le cadre de la messagerie sécurisée est recueilli par le professionnel habilité dans le cadre de la gestion de ses dossiers patients* ».

La Commission prend acte à cet effet des précisions du responsable de traitement selon lesquelles « *concernant les Patients, chacun doit être informé par le professionnel habilité, et consentir préalablement à la collecte et au traitement de ses Données Personnelles dans le cadre de l'utilisation de la Messagerie Sécurisée de Santé* ».

Au vu de ce qui précède, la Commission considère que le traitement est licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations nominatives traitées

Le responsable de traitement indique que les informations nominatives traitées sont :

- identité/situation de famille :
  - *patient :* nom, prénom, date de naissance ;
  - *professionnel habilité* : nom, prénom, identification professionnelle ;
- adresses et cordonnées :
  - *patient* : téléphone, adresse de messagerie électronique ;
  - *professionnel habilité* : adresse, téléphone, adresse de messagerie électronique, adresse de messagerie sécurisée de santé créée ;

- formation/ diplôme et vie professionnelle :
  - *professionnel habilité* : titre professionnel ;
- informations temporelles, horodatage :
  - *données de connexion du professionnel habilité* : adresse IP, logs (date, structure du professionnel de santé, actions effectuées, code postal, profession, spécialité, nom, prénom, canal), identifiants de connexion, information d'horodatage, adresse de messagerie sécurisée créée ;
  - *données de connexion du personnel habilité de l'Administration et/ou du prestataire* : adresse IP, logs, identifiant de connexion, information d'horodatage, adresse de messagerie sécurisée créée ;
- contenu des échanges : information et commentaires libres du professionnel habilité ;
- données cookies : cookies de session (connexion par webmail uniquement)
  - *stockés côté utilisateur* : identifiant de cookie ;
  - stockés côté serveur : identifiant de cookie, ID Utilisateur, Adresse IP utilisée pour la connexion, horodatage ;
- consentement du patient à faire partie de la liste « *patients* » du professionnel habilité : consentement donné par le patient au professionnel habilité, horodatage du consentement ;
- données de santé : toutes les informations strictement nécessaires à la prise en charge du patient, et relatives à son état de santé, sa situation sociale ou à son autonomie, notamment les diagnostics médicaux (maladie, pathologie, affection ou risque, handicap, état physiologique biomédical, antécédents familiaux), les données relatives aux soins (résultats d'examens, traitements), et le numéro ou symbole pour identifier de manière unique à des fins de santé.

Les informations relatives à l'identité/situation de famille, aux adresses et coordonnées, à la formation, aux diplômes et à la vie professionnelle, le contenu des échanges et les données de santé ont pour origine l'utilisateur (professionnel habilité).

Les informations relatives au consentement du patient ont pour origine le personnel habilité qui prend en charge le patient.

Les informations temporelles ont pour origine le système.

Enfin, les données cookies ont pour origine le navigateur de l'utilisateur de la messagerie sécurisée de santé.

La Commission considère ainsi que les informations collectées sont « *adéquates, pertinentes et non excessives* » au regard de la finalité du traitement, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

IV. Sur les droits des personnes concernées

➢ *Sur l'information préalable des personnes concernées*

L'information préalable des personnes concernées est effectuée par le biais d'une mention intégrée dans un document d'ordre général.

A l'analyse du document joint au dossier, la Commission constate que celui-ci est conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

➢ *Sur l'exercice du droit d'accès, de modification et de mise à jour*

Le responsable de traitement indique que le droit d'accès s'exerce sur place ou par voie postale auprès du Département des Affaires Sociales et de la Santé.

A cet égard, la Commission rappelle que la réponse à ce droit d'accès doit s'exercer dans le mois suivant la réception de la demande.

A la lecture des pièces jointes au dossier, la Commission constate par ailleurs qu'« *un justificatif d'identité, en noir et blanc, pourra être demandé au requérant* ».

A ce titre, elle précise que si une copie d'un document d'identité était demandée, la transmission et le traitement de ce document devront faire l'objet de mesures de protection particulières comme rappelé dans sa délibération n° 2015-113 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Sous cette réserve, la Commission constate que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 la Loi n° 1.165 du 23 décembre 1993.

V. Sur les personnes ayant accès au traitement

Les personnes habilitées à avoir accès au traitement sont :

- le prestataire/fournisseur de la messagerie sécurisée : tous droits (administration, infogérance et maintenance) ;
- les professionnels habilités : lecture, écriture et envoi de mails sécurisés ;
- les patients des professionnels de santé : lecture des mails sécurisés ;
- le personnel habilité de la Direction des Systèmes d'Information des établissements de santé (droits d'administration de l'application, à savoir création et suppression de compte) : lecture, écriture et envoi de mails sécurisés (pas d'accès au contenu des messages échangés entre les utilisateurs mais accès unique à l'interface d'administration des structures et des comptes utilisateurs associés) ;
- le personnel habilité de l'Administration (droit d'administration de l'application (création/suppression de comptes) : lecture, écriture et envoi de mails sécurisés (pas d'accès au contenu des messages échangés entre les utilisateurs mais accès unique à l'interface d'administration des structures et des comptes utilisateurs associés).

Considérant les attributions de chacune de ces personnes, et eu égard à la finalité du traitement, les accès susvisés sont justifiés.

La Commission constate que la messagerie est chiffrée et que seules les personnes habilitées ont accès au contenu des coffres.

En ce qui concerne le prestataire, elle relève cependant qu'à l'exception des pièces jointes, son personnel en charge de l'infogérance peut avoir accès au contenu du message.

Si elle prend acte que ces accès sont tracés, la Commission demande toutefois que les professionnels de santé habilités soient informés de ces potentiels accès.

Elle rappelle par ailleurs que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestation de service. De plus, ledit prestataire est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

Sous ces conditions, considérant les attributions de chacune de ces personnes, et eu égard à la finalité du traitement, les accès susvisés sont justifiés.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet d'une interconnexion avec un traitement ayant pour finalité « *Gestion du portail de e-Santé de la Principauté de Monaco* ».

La Commission prend acte que ce traitement a été légalement mis en œuvre.

VII. Sur la sécurité du traitement et des informations

Les mesures prises pour assurer la sécurité et la confidentialité du traitement et des informations qu'il contient n'appellent pas d'observations.

La Commission rappelle toutefois que les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

De même, la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception.

Enfin, elle rappelle que, conformément à l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du présent traitement.

VIII. Sur la durée de conservation

Les informations relatives à l'identité/situation de famille, aux adresses et coordonnées, à la formation, aux diplômes et à la vie professionnelle sont conservées le temps d'usage de la solution par le professionnel habilité.

A cet égard, la Commission prend note des précisions du responsable de traitement selon lesquelles les données sont supprimées lorsque le service n'est plus utilisé par le professionnel habilité ou si le patient retire son consentement.

Le contenu des échanges et les données de santé sont conservés 3 mois.

Les informations temporelles sont conservées 1 an.

Enfin, les données cookies sont conservées un maximum de 13 mois.

La Commission considère que ces durées sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Rappelle que :

- la réponse au droit d'accès doit s'exercer dans le mois suivant la réception de la demande ;

- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort ;

- la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception.

Demande que les professionnels de santé habilités soient informés des potentiels accès par le personnel en charge de l'infogérance au contenu des messages échangés.

Sous le bénéfice de la prise en compte de ce qui précède,

la Commission de Contrôle des Informations Nominatives **émet un avis favorable à la mise en œuvre par le Ministre d'Etat du traitement automatisé d'informations nominatives ayant pour finalité « *Echange de données de santé à travers un système de messagerie sécurisée* ».**

Le Président

Guy MAGNAN