DECLARATION

14/11/2019

AU 37
Traitements des données de santé par messagerie sécurisée

TRAITEMENTS DES DONNÉES DE SANTÉ PAR MESSAGERIE SÉCURISÉE

(Déclaration N° 37)

Suite à l'entrée en application du RGPD, la plupart des autorisations uniques adoptées par la CNIL n'ont plus de valeur juridique à compter du 25 mai 2018. Dans l'attente de la production de référentiels RGPD, la CNIL a décidé de les maintenir accessibles afin de permettre aux responsables de traitement d'orienter leurs premières actions de mise en conformité.

L'autorisation unique AU-037 encadre l'échange de données à caractère personnel par voie électronique de données de santé à travers un système de messagerie sécurisée. Ces dispositifs sont mis en œuvre par les professionnels et établissements de santé et les professionnels du secteur médico-social habilités par une loi.

TEXTE OFFICIEL

Délibération n° 2014-239 du 12 juin 2014 portant autorisation unique de mise en œuvre, par les professionnels et établissements de santé ainsi que par les professionnels du secteur médico-social habilités par une loi, de traitements de données à caractère personnel ayant pour finalité l'échange par

RESPONSABLES DE TRAITEMENT CONCERNES

- Etablissements et professionnels de santé
- Professionnels des secteurs sanitaire, social et médico-social

OBJECTIF(S) POURSUIVI(S) PAR LE TRAITEMENT (FINALITES)

Permettre l'échange de données de santé au moyen d'un service de messagerie sécurisée de santé entre professionnels de santé et, plus largement, entre les professionnels des secteurs sanitaire, social et médico-social habilités par une loi à collecter et à échanger des données de santé à caractère personnel (ci-après dénommés " professionnels habilités ") dans le cadre de la prise en charge, par ces professionnels, des personnes concernées par les données échangées

UTILISATION(S) EXCLUE(S) DU CHAMP DE LA NORME

Toute autre finalité

DONNEES PERSONNELLES CONCERNEES

Les seules données à caractère personnel pouvant être traitées sont les données relatives aux professionnels habilités, celles des personnes (patients) qu'ils prennent en charge et à propos desquels des échanges d'informations sont nécessaires pour assurer la qualité et la sécurité de cette prise en charge (état de santé, situation sociale, autonomie), ainsi que les données relatives aux personnes en charge de l'administration de la messagerie :

Données relatives aux professionnels utilisateurs finaux dits professionnels habilités :

- les données d'identification (état civil), l'identifiant du professionnel (numéro d'enregistrement au répertoire partagé des professionnels de santé (RPPS), numéro d'enregistrement au répertoire ADELI ou numéro d'identification local) et les données relatives au moyen d'authentification ;
- les coordonnées professionnelles (adresse, numéros de téléphone, adresse de courriel) ;
- le(s) titre(s) professionnel(s) ;
- les adresses de messagerie sécurisées de santé créées ;
- les données techniques nécessaires à la fourniture du service de messagerie sécurisée de santé (adresse IP, cookies) ;
- les traces des actions opérées sur la messagerie sécurisée de santé.

Données relatives aux patients:

- les données d'identification (nom, prénom, date et lieu de naissance, sexe), éventuellement l'identifiant national de santé ;
- les coordonnées (adresse, numéros de téléphone, adresses de courriel) ;
- les informations strictement nécessaires à la prise en charge des personnes et relatives à leur état de santé, à leur situation sociale ou à leur autonomie

Données relatives aux personnes en charge de l'administration des équipements et logiciels mis en œuvre pour la messagerie sécurisée :

les données strictement nécessaires à leur identification peuvent être traitées (identifiant de la personne physique, nom, prénom, fonction) afin de tracer leurs actions sur le système Toute autre donnée. Le service de messagerie sécurisée ne se substitue en aucun cas au dossier médical, sanitaire ou médico-social des personnes concernées (les patients) que doivent tenir les professionnels habilités susvisés en vertu des obligations légales et règlementaires qui leur incombent. Il constitue uniquement un outil professionnel d'échange sécurisé de données de santé, et non un nouvel espace de stockage. Afin d'être conforme à la présente autorisation, un service de messagerie doit comporter un système permettant d'organiser la suppression des boîtes aux lettres (BAL) en cas d'inactivité complète, caractérisée par l'absence d'authentification de l'utilisateur pendant une période maximale d'un an. Les traces techniques sont conservées pendant un an. Les destinataires des messages échangés au moyen de leurs messageries sécurisées de santé, ayant la qualité de " professionnels habilités " telle que définie en préambule de la présente autorisation unique. Les professionnels de santé et les professionnels habilités sont soumis au secret professionnel prévu à l'article 226-13 du code pénal. Les personnes en charge de l'administration de la messagerie peuvent accéder aux données relatives aux professionnels utilisateurs finaux dans le strict cadre de leurs missions et dans le respect du secret des correspondances privées. Elles doivent, en outre, être soumises à une clause de confidentialité.

Sur l'information des patients

Il appartient au responsable de traitement d'informer clairement les patients de la finalité du service de messagerie

sécurisée de santé, de ses conditions de mise en œuvre y compris en cas d'hébergement des données auprès d'un hébergeur agréé à cet effet, ainsi que des modalités d'exercice de leurs droits. Ces modalités doivent être portées à la connaissance des patients par la remise d'une brochure d'information, ou à défaut par voie d'affichage ou par une mention dans les livrets d'accueil des structures les prenant en charge.

Sur l'information des professionnels habilités

Le responsable de traitement doit informer les professionnels habilités des conditions d'utilisation du service de messagerie sécurisée de santé et des modalités d'exercice de leurs droits. Cette information doit notamment porter sur le respect des dispositions en matière de confidentialité figurant à l'article L. 1110-4 du code de la santé publique relatives aux conditions d'échange de données de santé entre deux ou plusieurs professionnels de santé. La Commission recommande que chaque professionnel soit informé qu'il lui appartient de veiller à ce que toute information qu'il jugera utile pour la prise en charge de ses patients soit reportée dans leur dossier médical. Une communication électronique émise ou reçue par une personne peut revêtir le caractère d'une correspondance privée. La violation du secret des correspondances est une infraction pénalement sanctionnée par les articles 226-15 et 432-9 du code pénal. Le responsable de traitement informe les professionnels habilités des modalités permettant de différencier les courriels professionnels des courriels personnels qu'ils peuvent être amenés à échanger par le biais du système de messagerie sécurisée. Toutefois, les données relatives à la santé des personnes doivent être traitées dans des conditions de confidentialité conformes à l'article L.1110-4 précité. Dès lors, elles ne doivent être accessibles qu'aux professionnels habilités intervenant dans le cadre de la prise en charge des personnes. Ces informations doivent être formalisées dans un document, tel qu'une charte informatique, qui doit être porté à la connaissance des personnes concernées.

Sur les droits d'accès, de rectification et d'opposition des personnes

L'exercice des droits d'accès, de rectification et d'opposition des personnes concernées par les données traitées (professionnels habilités, patients) s'opère auprès du responsable du traitement de messagerie sécurisée de santé. En cas d'opposition du patient à l'échange de données le concernant au moyen d'un service de messagerie sécurisée de santé, les professionnels habilités doivent cesser tout échange le concernant par le biais de cette messagerie et recourir à un moyen d'échange alternatif (courrier postal par exemple).

DONNEES EXCLUES DU CHAMP DE LA NORME

" Toute autre donnée.

DUREE DE CONSERVATION DES DONNEES

Le service de messagerie sécurisée ne se substitue en aucun cas au dossier médical, sanitaire ou médico-social des personnes concernées (les patients) que doivent tenir les professionnels habilités susvisés en vertu des obligations légales et règlementaires qui leur incombent. Il constitue uniquement un outil professionnel d'échange sécurisé de données de santé, et non un nouvel espace de stockage. Afin d'être conforme à la présente autorisation, un service de messagerie doit comporter un système permettant d'organiser la suppression des boîtes aux lettres (BAL) en cas d'inactivité complète, caractérisée par l'absence d'authentification de l'utilisateur pendant une période maximale d'un an. Les traces techniques sont conservées pendant un an

DESTINATAIRES DES DONNEES

Les destinataires des messages échangés au moyen de leurs messageries sécurisées de santé, ayant la qualité de " professionnels habilités " telle que définie en préambule de la présente autorisation unique. Les professionnels de santé et les professionnels habilités sont soumis au secret professionnel prévu à l'article 226-13 du code pénal. Les personnes en charge de l'administration de la messagerie peuvent accéder aux données relatives aux professionnels utilisateurs finaux dans le strict cadre de leurs missions et dans le respect du secret des correspondances privées. Elles doivent, en outre, être soumises à une clause de confidentialité.

INFORMATION DES PERSONNES ET RESPECT DES DROITS "INFORMATIQUE ET LIBERTES"

Sur l'information des patients Il appartient au responsable de traitement d'informer clairement les patients de la finalité du service de messagerie sécurisée de santé, de ses conditions de mise en œuvre y compris en cas d'hébergement des données auprès d'un hébergeur agréé à cet effet, ainsi que des modalités d'exercice de leurs droits. Ces modalités doivent être portées à la connaissance des patients par la remise d'une brochure d'information, ou à défaut par voie d'affichage ou par une mention dans les livrets d'accueil des structures les prenant en charge.

Sur l'information des professionnels habilités Le responsable de traitement doit informer les professionnels habilités des conditions d'utilisation du service de messagerie sécurisée de santé et des modalités d'exercice de leurs droits. Cette information doit notamment porter sur le respect des dispositions en matière de confidentialité figurant à l'article L. 1110-4 du code de la santé publique relatives aux conditions d'échange de données de santé entre deux ou plusieurs professionnels de santé. La Commission recommande que chaque professionnel soit informé qu'il lui appartient de veiller à ce que toute information qu'il jugera utile pour la prise en charge de ses patients soit reportée dans leur dossier médical. Une communication électronique émise ou reçue par une personne peut revêtir le caractère d'une correspondance privée. La violation du secret des correspondances est une infraction pénalement sanctionnée par les articles 226-15 et 432-9 du code pénal. Le responsable de traitement informe les professionnels habilités des modalités permettant de différencier les courriels professionnels des courriels personnels qu'ils peuvent être amenés à échanger par le biais du système de messagerie sécurisée. Toutefois, les données relatives à la santé des personnes doivent être traitées dans des conditions de confidentialité conformes à l'article L.1110-4 précité. Dès lors, elles ne doivent être accessibles qu'aux professionnels habilités intervenant dans le cadre de la prise en charge des personnes. Ces informations doivent être formalisées dans un document, tel qu'une charte informatique, qui doit être porté à la connaissance des personnes concernées.

Sur les droits d'accès, de rectification et d'opposition des personnes L'exercice des droits d'accès, de rectification et d'opposition des personnes concernées par les données traitées (professionnels habilités, patients) s'opère auprès du responsable du traitement de messagerie sécurisée de santé. En cas d'opposition du patient à l'échange de données le concernant au moyen d'un service de messagerie sécurisée de santé, les professionnels habilités doivent cesser tout échange le concernant par le biais de cette messagerie et recourir à un moyen d'échange alternatif (courrier postal par exemple).

SECURITE ET CONFIDENTIALITE

Le responsable de traitement doit utiliser un service de messagerie sécurisée de santé conforme aux exigences de sécurité imposées par l'article 34 de la loi du 6 janvier 1978 modifiée. Il doit réaliser ou s'assurer qu'a été réalisée, lorsqu'il fait appel à un prestataire éditeur d'une solution de messagerie sécurisée de santé, une analyse des risques que le système de messagerie fait peser sur les libertés et la vie privée des personnes concernées. Les services de messageries sécurisées de santé doivent assurer une identification et une authentification fiables des professionnels habilités, afin de garantir la confiance dans ces dispositifs. La mise en place d'un service de messagerie sécurisée de santé doit, en outre, satisfaire aux conditions suivantes :

1) Le service de messagerie doit garantir l'identité de l'émetteur et du destinataire d'un message en vérifiant leur appartenance à un référentiel d'identification national ou local.

Le responsable de traitement est garant de l'identification et de l'authentification des professionnels habilités. En application de l'article de l'article 6-1° de la loi du 6 janvier 1978 modifiée, un traitement de données à caractère personnel doit satisfaire à une condition de licéité. Pour l'accès et l'utilisation d'un compte de messagerie :

- s'agissant des professionnels de santé, l'authentification doit être réalisée au moyen d'une carte de professionnel de santé (CPS) ou d'un dispositif équivalent agréé par l'organisme chargé d'émettre la CPS ;
- s'agissant des autres professionnels habilités, l'utilisateur final doit s'authentifier de manière forte, c'est-à-dire par un procédé qui requiert au minimum deux facteurs d'authentification distincts parmi ce que l'on sait (par exemple un mot de passe), ce que l'on a (par exemple un certificat électronique ou une carte à puce) et une caractéristique qui nous est propre (par exemple une empreinte).

Le service de messagerie sécurisée de santé doit être doté d'un dispositif assurant la traçabilité des actions d'utilisation et d'exploitation du service.

2) Le service de messagerie doit assurer la sécurité des messages et des pièces jointes lors de leur transfert.

Le service de messagerie sécurisée de santé doit être mis en œuvre de façon à garantir la sécurité des messages et pièces jointes, notamment leur confidentialité et leur intégrité durant leur transfert entre le poste des professionnels habilités (l'utilisateur final-émetteur et l'utilisateur final-destinataire). Le service de messagerie sécurisée de santé doit assurer la conservation sous une forme sécurisée des messages et des pièces jointes Le responsable de traitement doit assurer la disponibilité, l'intégrité, la traçabilité et la sécurité physique et logique des messages et des pièces jointes qu'il conserve. Lorsque le responsable de traitement ne conserve pas par ses propres moyens les données de santé à caractère personnel échangées et collectées par le biais d'un service de messagerie sécurisée de santé, il doit veiller à ce que les serveurs de messagerie soient conservés par un hébergeur agréé à cet effet, dans les conditions conformes aux articles L.1111-8 et R.1111-9 et suivants du code de la santé publique.