L'AUTORISATION UNIQUE RELATIVE À LA MESSAGERIE SÉCURISÉE DE SANTÉ (1) : UN OUTIL DE CONFORMITÉ

HEALTH MESSAGING SYSTEMS: CNIL FACILITATES SECURED EXCHANGE PROCESSINGS

Par **Délia RAHAL-LÖFSKOG**

RÉSUMÉ

La sécurité est l'un des enjeux majeurs de l'échange de données relatives à la santé. A cet égard, l'autorisation unique adoptée par la CNIL permet de répondre à cette exigence tout en simplifiant les démarches des responsables de traitements en leur permettant de procéder à un engagement de conformité sur le site Internet de la Commission.

MOTS-CLÉS

Messagerie, Sécurisée, Santé, CNIL, Conformité.

SUMMARY

To enable professionals to exchange personal health data related to their patients in a secure and reliable environment is a must do. Data controllers which are compliant with the single decision taken by the CNIL regarding secured health messaging systems will simply fill in the appropriate compliance commitment on CNIL's website.

KEYWORDS

Health data, Messaging systems, Data protection, Compliance.

La loi du 6 janvier 1978 modifiée, dite Informatique et Libertés, encadre le traitement des données à caractère personnel soumis à diverses formalités selon la sensibilité des données concernées. Outre la nécessité de satisfaire les principes de finalité (2) et de pertinence (3), la loi impose aussi de respecter le principe de confidentialité et de sécurité (4) des données.
S'agissant des données sensibles parmi lesquelles figurent les données relatives à la santé, le législateur pose un principe d'interdiction. Il a toutefois tempéré cette interdiction au travers d'exceptions telles que le consentement exprès et préalable de la personne concernée ou le traitement de ces données par les professionnels de santé dans le cadre de la prise en charge de leurs patients.

* Chef du service de la santé
Direction de la conformité
Commission nationale de l'Informatique et des Libertés
drahal-lofskog@cnil.fr

(1) http://www.cnil.fr/documentation/deliberations/deliberation/delib/314/

(2) Article 6-2° de la loi Informatique et Libertés : « Elles sont collectées pour des finalités déterminées, explicites et légitimes ».

(3) Article 6-3° : « Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ».

(4) Article 34 de la loi.

D'autres hypothèses requièrent l'autorisation de la CNIL, notamment lorsque les données sont échangées dans le cadre de la recherche médicale, ou collectées dans une finalité d'évaluation des pratiques de soins. C'est également le cas lorsque le traitement de ces données est justifié par l'intérêt public. Les traitements (5) sont alors soumis à l'autorisation prévue à l'article 25-I-1° de la loi Informatique et Libertés. Ceux qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires, peuvent être autorisés par une décision unique de la Commission nationale de l'informatique et des libertés (CNIL).

Cette autorisation unique constitue une des mesures de simplification que peut adopter le régulateur permettant ainsi aux responsables de traitement de s'inscrire dans le cadre défini et d'adresser à la CNIL un engagement de conformité à l'autorisation adoptée permettant la mise en œuvre immédiate du traitement. L'adoption par la CNIL, le 12 juin 2014, d'une autorisation unique relative à la messagerie sécurisée de santé (6) en est une illustration (AU-037).

Le déploiement de messageries sécurisées de santé, outre de relever de la stratégie nationale de santé, constitue un véritable enjeu pour la sécurité des données de à caractère personnel relatives à la santé lorsqu'elles sont échangées par voie électronique dans le cadre de la prise en charge des patients. En effet, les outils de messagerie font aujourd'hui partie de la pratique quotidienne des professionnels de santé appelés à s'échanger des informations relatives à leurs patients dans le respect des règles en vigueur notamment du code de la santé publique. Toutefois, l'utilisation de messageries dites domestiques peut difficilement être regardée comme un gage de sécurité et de confidentialité auquel ces professionnels doivent pourtant être attentifs.

Dans une volonté de permettre aux acteurs concernés de recourir à des outils de nature à répondre à leur pratique quotidienne tout en bénéficiant d'un cadre juridique et technique conforme à la loi, la CNIL a engagé une concertation avec les représentants de ces acteurs préalablement à l'adoption de cette décision.

L'autorisation unique n°37 permet l'échange de données relatives à la santé de personnes prises en charge dans le cadre d'un parcours de soins par l'ensemble des personnes habilitées par la loi. Elle tient donc compte des expérimentations sur le parcours de santé des personnes âgées en risque de perte d'autonomie prévues par l'article 48 de la loi du 17 décembre 2012 de financement et de la sécurité sociale (LFSS) pour 2013 permettant à des non professionnels de santé, habilités par la loi, d'échanger de telles données *« sous réserve du consentement exprès et éclairé de chaque personne, la transmission, par les personnels soignants et les professionnels chargés de leur accompagnement social, d'informations strictement nécessaires à leur prise en charge et relatives à leur état de santé, à leur situation sociale ou à leur autonomie ».*

Au-delà de la simplification des formalités que cet encadrement induit nécessairement, la conformité à cette autorisation unique peut constituer un véritable levier d'innovation permettant aux éditeurs de logiciels de connaître les exigences du régulateur et, dès lors, proposer aux utilisateurs des solutions d'emblées conformes à la notion de « privacy by design » prévue dans le futur règlement européen sur la protection des donnée à caractère personnel. ■

(5) L'article 2 de la loi Informatique et Libertés définit les traitements de donnée à caractère personnel comme « toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »

(6) 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 voie électronique de données de santé à travers un système de messagerie sécurisée.