Commission nationale de l'informatique et des libertés, délibération n° 2014-046 du 30 janvier 2014 portant autorisation unique de traitements de données à caractère personnel mis en œuvre par les prestataires de santé à domicile pour la téléobservance en application de l'arrêté du 22 octobre 2013 relatif aux dispositifs médicaux à pression positive continue (Commission nationale de l'informatique et des libertés - Traitements de données à caractère personnel - Prestataires de santé à domicile)

30/01/2014

La CNIL confirme que les patients atteints d'apnée du sommeil ne peuvent s'opposer à la télétransmission automatisée de leurs données d'observance du traitement par pression positive continue (PPC). Les prestataires de santé à domicile mettent en place un traitement de données à caractère personnel pour organiser une télétransmission automatisée et obligatoire des données d'observance produites par les dispositifs médicaux à pression positive continue (DM à PPC) utilisés dans le cadre du traitement de l'apnée du sommeil (obligation pour une prise en charge par la sécurité sociale). Cette décision précise les données pouvant faire l'objet du traitement, la durée de conservation des données, les destinataires des données, l'information des personnes, les transferts de données hors UE, le droit d'opposition, la sécurité des données et traçabilité des actions.

Délibération n° 2014-046 du 30 janvier 2014 portant autorisation unique de traitements de données à caractère personnel mis en œuvre par les prestataires de santé à domicile pour la téléobservance en application de l'arrêté du 22 octobre 2013 relatif aux dispositifs médicaux à pression positive continue

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu le code de la santé publique, notamment son article L. 1111-8 ;

Vu le code de la sécurité sociale, notamment ses articles R. 165-1 et suivants ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 8-IV, 25 (I, 1°) et 25-II ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu l'arrêté du 22 octobre 2013 portant modification des modalités d'inscription et de prise en charge du dispositif médical à pression positive continue pour traitement de l'apnée du sommeil et prestations associées au chapitre 1er du titre Ier de la liste des produits et prestations remboursables prévue à l'article L. 165-1 du code de la sécurité sociale ;

Après avoir entendu M. Jean MASSOT, commissaire, en son rapport et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

En application des dispositions des articles R. 165-1 et suivants du code de la sécurité sociale, l'arrêté du 22 octobre 2013 portant modification des modalités d'inscription et de prise en charge du dispositif médical à pression positive continue (DM à PPC) pour le traitement de l'apnée du sommeil et prestations associées modifie les modalités d'inscription sur la liste mentionnée à l'article L. 165-1 du code de la sécurité sociale des DM à PPC, notamment en organisant une télétransmission automatisée et obligatoire des données d'observance produites par les DM à PPC utilisés dans le cadre du traitement de l'apnée du sommeil.

En application du texte précité, les prestataires de santé à domicile (PSAD) mettent en place un traitement de données à caractère personnel.

Par ailleurs, les données d'observance traitées par les PSAD sont des données de santé à caractère personnel qui relèvent de l'article 8 de la loi du 6 janvier 1978 modifiée.

Dès lors, de tels traitements relèvent de l'article 25 (I, 1°) de la loi du 6 janvier 1978 modifiée et doivent, à ce titre, être autorisés par la CNIL.

En vertu de l'article 25-II de la loi du 6 janvier 1978 modifiée, la Commission peut autoriser par une décision unique une catégorie de traitements qui répondent aux mêmes finalités, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires.

Les traitements automatisés de données à caractère personnel mis en œuvre par les PSAD ayant pour finalité la téléobservance, en application de l'arrêté du 22 octobre 2013, sont de ceux qui peuvent, sous certaines conditions, relever de cette définition.

Les PSAD qui adressent à la Commission une déclaration comportant un engagement de conformité pour les traitements de données à caractère personnel répondant aux conditions fixées par la présente décision unique sont autorisés à les mettre en œuvre.

Tout traitement de données à caractère personnel qui excède le cadre ou les exigences définis par la présente autorisation unique doit en revanche faire l'objet d'une formalité spécifique.

Article 1
Sur la finalité du traitement.

Seuls peuvent faire l'objet d'un engagement de conformité par référence à la présente décision unique les traitements mis en œuvre par les PSAD aux fins de télétransmission des données d'observance du traitement de l'apnée du sommeil, produites par les DM à PPC.
Sont notamment exclus du champ d'application de l'autorisation unique les traitements de données à caractère personnel ayant pour finalités :
— la mise en place d'un dispositif de télésurveillance médicale des patients, auquel les dispositions relatives à la télémédecine s'appliquent ; et
— la mise en place de mesures d'accompagnement relevant des dispositions relatives à l'éducation thérapeutique.

Article 2
Sur la nature des données traitées.

Les données suivantes peuvent être traitées :
— données d'identification du patient : nom, prénom, date et lieu de naissance, adresse postale, numéro de téléphone et numéro de sécurité sociale ;
— données d'identification du PSAD : raison sociale et, le cas échéant, nom et prénom ;

— données d'identification du médecin prescripteur et/ou du médecin traitant suivant le patient : nom, prénom, numéro RPPS ;
— données d'identification de la caisse d'assurance maladie obligatoire dont dépend le patient ;
— numéro de série du DM à PPC et, le cas échéant, du module de télétransmission permettant au seul PSAD de relier un appareil à un patient ;
— données de santé : durée quotidienne d'utilisation du DM à PPC, date d'installation, taux de prise en charge du patient, éventuelles durées de suspension et motifs de prise en charge par l'AMO.

La collecte et le traitement de toute autre donnée, notamment les données permettant de géolocaliser le dispositif médical, sont exclus du champ d'application de la présente autorisation unique.

En outre, la commission rappelle que, conformément aux articles 6 (4°) et 40 de la loi du 6 janvier 1978 modifiée, ces données doivent être « exactes, complètes et mises à jour ».

Article 3
Sur la durée de conservation des données.

Les données traitées sont conservées par le PSAD pendant une durée de trois ans à compter de leur collecte, afin de permettre les contrôles appropriés par les organismes compétents.

A l'expiration de ce délai, les données sont supprimées.

La conservation et l'archivage des données doivent être réalisés dans des conditions de sécurité conformes aux dispositions de l'article 34 de la loi du 6 janvier 1978 modifiée.

Article 4
Sur les destinataires des données.

L'arrêté du 22 octobre 2013 impose aux PSAD de transmettre mensuellement les données d'observance accompagnées des données d'identification des patients à l'organisme d'assurance maladie obligatoire compétent, permettant ainsi aux PSAD de calculer le forfait applicable à la situation du patient et de facturer la prestation effectuée auprès de lui.

Pour permettre d'établir la correspondance entre le numéro de série unique du DM à PPC et, le cas échéant, du module de télétransmission, le fabricant sera destinataire des données suivantes :
— numéro de série du DM à PPC et, le cas échéant, du module de télétransmission ;
— données d'identification du PSAD ;
— données d'observance que sont les durées d'utilisation quotidienne du DM à PPC.

Pour permettre la correspondance entre le DM à PPC ou le dispositif de télétransmission et le patient et sa caisse d'assurance maladie obligatoire le PSAD sera destinataire des données suivantes :
— données d'identification du DM à PPC ou du dispositif de télétransmission ;
— données d'identification du patient, dont le numéro de sécurité sociale ;
— données relatives à sa caisse d'assurance maladie obligatoire ;
— données d'observance et, le cas échéant, forfait AMO calculé par le PSAD.

Pour permettre aux organismes d'assurance maladie de calculer le forfait et pour permettre une prise en charge adaptée, ces organismes seront destinataires des données suivantes :
— données d'identification du patient, dont son numéro de sécurité sociale ;
— données d'identification du PSAD, données d'observance et, le cas échéant, forfait calculé par le PSAD.

Article 5

Sur l'information des personnes.

Une information écrite individuelle sera remise à chaque patient par le PSAD installant le DM à PPC à son domicile.

Le dispositif de télétransmission étant obligatoire, cette note d'information précise, conformément aux dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée :
— l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
— la finalité poursuivie par le traitement auquel les données sont destinées ;
— le caractère obligatoire de la transmission des données ;
— les conséquences éventuelles, à son égard, d'un défaut de réponse, notamment sur la prise en charge par l'assurance maladie obligatoire du DM à PPC ;
— les destinataires ou catégories de destinataires des données ;
— les droits que le patient tient des dispositions de la loi du 6 janvier 1978 modifiée ;
— le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne.

Article 6
Sur les transferts de données à caractère personnel hors de l'Union européenne.

Dans les cas où les communications de données précitées concernent un transfert vers une personne morale établie dans un pays non membre de l'Union européenne n'accordant pas une protection suffisante au sens de l'article 68 de la loi du 6 janvier 1978 modifiée, elles doivent s'opérer conformément aux dispositions spécifiques de la loi du 6 janvier 1978 modifiée relative aux transferts internationaux de données, et notamment son article 69, alinéa 8.

Il est satisfait à ces dispositions lorsque la personne morale au sein de laquelle travaille le destinataire des données a adhéré au Safe Harbor, dans la mesure où la société américaine concernée a expressément fait le choix d'inclure les données de ressources humaines dans le champ de cette adhésion.

Il est également satisfait à ces dispositions lorsque le destinataire a conclu un contrat de transfert basé sur les clauses contractuelles types émises par la Commission européenne dans ses décisions du 15 juin 2001, du 27 décembre 2004, ou lorsque le groupe auquel appartiennent les entités concernées ont adopté des règles internes dont la CNIL a préalablement reconnu qu'elles garantissent un niveau de protection suffisant de la vie privée et des droits fondamentaux des personnes.

S'il est satisfait à ces conditions et si le traitement dont le transfert est issu est par ailleurs conforme à l'ensemble des autres dispositions de la présente délibération, celle-ci porte également autorisation du transfert envisagé en application de l'article 69, alinéa 8, de la loi du 6 janvier 1978 modifiée.

Article 7
Sur le droit d'opposition des personnes.

L'article 38 de la loi du 6 janvier 1978 modifiée prévoit que toute personne a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement, tout en précisant que cette disposition ne s'applique pas lorsque le traitement répond à une obligation légale.

Dès lors que l'arrêté du 22 octobre 2013, en ce qu'il rend obligatoire le dispositif de télétransmission, écarte expressément le droit d'opposition, dans le cadre de la présente autorisation unique, il est rappelé que le droit d'opposition est exclu.

Article 8
Sur les droits d'accès et de rectification des personnes.

Les droits d'accès et de rectification inscrits dans les articles 39 et 40 de la loi du 6 janvier 1978 modifiée doivent être mis en œuvre et pouvoir être exercés auprès du PSAD en lien avec le patient.

Article 9
Sur la sécurité des données et la traçabilité des actions.

Des mesures de protection physique et logique adéquates doivent être prises pour préserver la sécurité du traitement et des informations, empêcher toute utilisation détournée ou frauduleuse des informations, notamment par des tiers non autorisés, et préserver l'intégrité des données.

Les transferts de données entre le dispositif de télétransmission et son fabricant ainsi que ceux entre le fabricant du DM à PPC et le PSAD sont sécurisés par l'utilisation de protocoles de communication sécurisés, dont notamment le protocole HTTPS.

Les données d'observance sont transmises par le PSAD aux organismes d'assurance maladie obligatoire de manière sécurisée grâce à la mise en place d'un système de chiffrement réputé fort.

Le cas échéant, les clés de chiffrement utilisées doivent être accessibles à un nombre limité de personnes et renouvelées régulièrement.

Le PSAD met en œuvre des mécanismes permettant de s'assurer de l'intégrité des données d'observance du DM à PPC, par exemple en mettant en place un dispositif de signature automatique des données, préalable à leur transmission par le dispositif de télétransmission.

Des profils d'habilitation sont prévus afin de gérer les accès aux données en tant que de besoin. Un contrôle des habilitations est régulièrement effectué, au minimum une fois par an.

Les accès aux données sont opérés sur des réseaux sécurisés (VPN, SSL) et tracés. Ces traces font l'objet d'un audit régulier. Une durée de conservation de ces traces est définie.

En cas d'externalisation, les données sont hébergées conformément à l'article L. 1111-8 du code de la santé publique.

Le responsable de traitement prend les mesures nécessaires pour assurer la sécurité et la confidentialité des données qu'il détient et pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance.

En cas de recours à un prestataire de service, le responsable du traitement doit imposer à ce prestataire, par voie contractuelle, de n'utiliser les données qu'aux fins prévues, de s'assurer de leur confidentialité et de procéder à la destruction ou à la restitution de tous les supports manuels ou informatisés de données à caractère personnel au terme de sa prestation.

Article 10
Sur la publication.

La présente délibération sera publiée au Journal officiel de la République française.

Pour la présidente :

Le vice-président délégué,

DIRECTION DES AFFAIRES JURIDIQUES

E. de Givry