Commission nationale de l'informatique et des libertés

Délibération nº 2017-215 du 13 juillet 2017 portant adoption d'une norme destinée à simplifier l'obligation de déclaration des traitements de données à caractère personnel ayant pour finalité le dépistage organisé du cancer du sein, du cancer colorectal et du cancer du col de l'utérus mis en œuvre par les structures de gestion conventionnées, et abrogeant la délibération nº 2015-175 du 11 juin 2015 (décision d'autorisation unique nº AU-043) (NS-059)

NOR : *CNIL1724568X*

La Commission nationale de l'informatique et des libertés,

Vu la convention nº 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 la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 8-II (6º) et 24-I ;

Vu le décret nº 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret nº 2015-390 du 3 avril 2015 autorisant les traitements de données à caractère personnel par les organismes gestionnaires des régimes obligatoires de base de l'assurance maladie pour l'accomplissement de leurs missions d'affiliation, d'immatriculation, d'instruction des droits aux prestations et de prise en charge des soins, produits et services ;

Vu le décret nº 2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant national de santé ;

Vu l'arrêté du 29 septembre 2006 modifié relatif aux programmes de dépistage des cancers ;

Vu l'arrêté du 23 septembre 2014 portant introduction du test immunologique dans le programme de dépistage organisé du cancer colorectal ;

Vu l'instruction nº DGS/SP5/2016/166 du 25 mai 2016 relative aux modalités de désignation des structures régionales de préfiguration de la généralisation du dépistage organisé du cancer du col de l'utérus et son annexe comprenant le cahier des charges ;

Vu l'instruction nº DGS/SP5/2016/395 du 21 décembre 2016 relative à l'évolution du dispositif des structures de gestion du dépistage organisé du cancer ;

Après avoir entendu M. Alexandre LINDEN, commissaire, en son rapport et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

Les programmes nationaux de dépistage organisé du cancer du sein, du cancer colorectal et du cancer du col de l'utérus s'inscrivent dans le cadre du Plan cancer mis en place par le Gouvernement afin de réduire la mortalité et la lourdeur des traitements liés à une prise en charge tardive. Leurs modalités d'organisation sont précisées dans des cahiers des charges nationaux publiés par arrêté. Ces programmes de dépistage organisé des cancers sont mis en œuvre par des structures départementales, interdépartementales ou régionales qui ont passé une convention avec les représentants de l'Etat et de l'assurance maladie dans leur région. A ce titre, ces structures constituent des fichiers d'invitation et de suivi des personnes concernées ; les données collectées dans ce cadre sont également utilisées à des fins d'évaluation et de pilotage des programmes.

S'agissant du dépistage organisé du cancer colorectal, les laboratoires de biologie médicale-centres de lecture des examens définis par l'arrêté précité mettent en œuvre une plateforme électronique dédiée au partage des résultats entre les différents acteurs du dépistage et comportant des données personnelles relatives à la santé des personnes.

En vertu de l'article 24 de la loi du 6 janvier 1978 modifiée, la Commission nationale de l'informatique et des libertés est habilitée à établir des normes destinées à simplifier l'obligation de déclaration des traitements les plus courants et dont la mise en œuvre, dans des conditions régulières, n'est pas susceptible de porter atteinte à la vie privée ou aux libertés.

Les traitements de données à caractère personnel, automatisés ou non, mis en œuvre par les structures de gestion conventionnées aux fins d'exercice de leurs missions dans le cadre du dépistage organisé du cancer colorectal et du cancer du sein sont de ceux qui peuvent, sous certaines conditions, relever de cette définition.

Ces traitements encadrés précédemment par une autorisation unique nº AU-043 adoptée le 11 juin 2015 (délibération nº 2015-175 du 11 juin 2015 portant autorisation unique de traitements de données à caractère personnel ayant pour finalité le dépistage organisé du cancer du sein et du cancer colorectal mis en œuvre par les

structures de gestion conventionnées) relèvent dorénavant d'une norme simplifiée avec un champ d'application élargi au cancer du col de l'utérus.

Art. 1er. – *Champ d'application.*

Seuls peuvent faire l'objet d'un engagement de conformité en référence à la présente norme les traitements, automatisés ou non, mis en œuvre par les structures en charge de la mise en œuvre des programmes de dépistage des cancers investies contractuellement par les représentants de l'Etat dans leur région.

Les structures en charge de la mise en œuvre des programmes de dépistage des cancers, placées sous la responsabilité médicale d'un ou plusieurs médecins coordinateurs du (des) programme(s), assurent l'organisation locale des dépistages organisés des cancers du sein, colorectal et utérin à l'échelle d'un ou plusieurs départements.

Art. 2. – *Finalités du traitement.*

Peuvent faire l'objet d'un engagement de conformité à la présente norme les traitements automatisés ou non de données à caractère personnel ayant pour finalité la mise en œuvre de programmes de dépistage organisé du cancer du sein, du cancer colorectal et du cancer du col de l'utérus.

Au titre de ces traitements, sont visées :

- la constitution, par les structures en charge de la mise en œuvre des programmes de dépistage des cancers, et la gestion par celles-ci, des fichiers des personnes concernées, à partir des données transmises par les caisses d'assurance maladies participantes, aux fins d'invitation aux opérations de dépistage selon les critères d'éligibilité des personnes ;
- la réalisation des opérations de suivi de ces personnes dans le cadre des programmes de dépistage organisé, y compris la transmission des résultats des tests de dépistage ;
- la gestion des contacts avec les médecins traitants, les spécialistes et les centres de lecture associés aux programmes de dépistage (laboratoires de biologie médicale et structures d'anatomie et cytologie pathologique) ;
- l'évaluation des programmes de dépistage.

Art. 3. – *Nature des données traitées.*

La commission rappelle que, conformément à l'article 6 (3°) de la loi « informatique et libertés », les données traitées doivent être pertinentes, adéquates et non excessives au regard des finalités du traitement.

Peuvent être traitées, pour l'accomplissement des finalités décrites à l'article 2, les catégories de données à caractère personnel suivantes :

- données relatives à l'identification des personnes concernées telles que transmises par les caisses d'assurance maladie participantes ou les personnes concernées, à savoir : l'identifiant national de santé mentionné à l'article L. 1111-8-1 du code de la santé publique, nom de naissance et nom d'usage, le cas échéant, prénom(s), sexe, date de naissance, adresse, coordonnées téléphoniques ;
- données relatives à l'identification des professionnels de santé intervenant dans le programme, à savoir : nom, prénom(s), numéro d'inscription au répertoire partagé des professionnels de santé et adresse postale ;
- données relatives à la santé des personnes concernées, à savoir, limitativement :
  - le numéro d'identifiant ou d'invitation de la personne généré par la structure de gestion à partir des fichiers transmis par les caisses d'assurance maladie ;
  - les données relatives aux examens antérieurs et antécédents médicaux strictement nécessaires à la détermination du niveau de risque et à la définition de l'éligibilité des personnes vis-à-vis des programmes de dépistage des cancers, telles que transmises par les caisses d'assurance maladie participantes, par les personnes concernées et les professionnels de santé ;
  - le cas échéant, si les personnes concernées l'acceptent, leur(s) motif(s) de refus de participer aux opérations de dépistage ;
  - les résultats et comptes rendus des examens, et, le cas échéant, les clichés d'imagerie ;
  - les dates d'envoi des résultats au médecin et à la personne concernée ;
  - les informations sur la prise en charge médicale effective permettant de vérifier l'entrée dans une filière de soins des personnes dont le test se serait révélé positif.

Art. 4. – *Durée de conservation des données.*

Les données relatives à la prise en charge des personnes concernées sont conservées par les structures en charge de la mise en œuvre des programmes de dépistage des cancers jusqu'à la fin du suivi, décidée par la personne elle-même ou son médecin. Ces durées doivent être conformes aux dispositions législatives et réglementaires en vigueur.

A l'expiration de ce délai, les données sont supprimées ou archivées sous une forme anonyme.

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.

Art. 5. – *Destinataires des données.*

Dans la limite de leurs attributions respectives et pour l'exercice des finalités précitées, seules peuvent être habilitées à accéder aux données les personnes suivantes :

Pour les seules données relatives aux personnes qu'ils prennent en charge :

– les professionnels de santé ayant prescrit ou réalisé l'acte de dépistage ;
– le médecin coordinateur de la structure de gestion ;
– le médecin traitant ou le médecin désigné par la personne comme destinataire des résultats de l'examen de dépistage.

En outre, peuvent être destinataires des données relatives à ces personnes les personnels habilités :

– des centres de lecture associés aux programmes de dépistage ;
– des organismes d'assurance maladie, pour les seules données nécessaires à l'amélioration du processus d'invitation et au remboursement des soins dans des conditions conformes à l'article 3 du décret nº 2015-390 du 3 avril 2015 ;
– les médecins spécialistes ayant réalisé des examens complémentaires à la suite d'un test positif ;
– de l'Institut national du cancer et de l'Agence nationale de santé publique (Santé publique France) pour les seules données nécessaires à l'évaluation et au pilotage des programmes (données anonymes) ;
– des registres des cancers pour la caractérisation des lésions précancéreuses et des cancers et l'évaluation de leur incidence.

Art. 6. – *Information et droits des personnes concernées.*

Le responsable de traitement informe les personnes concernées de la mise en œuvre d'un traitement de données à caractère personnel ayant pour finalité la réalisation des opérations de dépistage organisé du cancer du sein, du cancer colorectal ou du cancer du col de l'utérus.

Cette information s'effectue selon les modalités suivantes :

– la structure de gestion invite par courrier la personne éligible au programme de dépistage à consulter son médecin traitant ou un professionnel de santé agréé. Le courrier de réponse joint à ce courrier contient une note d'information établie conformément à l'article 32-I de la loi du 6 janvier 1978 modifiée qui rappelle notamment les droits d'accès, de rectification et d'opposition reconnus par les articles 38 à 40. Cette note précise le service auprès duquel ces droits peuvent s'exercer ;
– le médecin traitant ou le professionnel de santé qui réalise l'examen de dépistage informe oralement les personnes concernées conformément à l'article 32-I de la loi. Il précise les modalités d'exercice des droits d'accès, de rectification et d'opposition précités ;
– cette information est également affichée dans les locaux des professionnels de santé participants et, le cas échéant, sur la feuille de demande d'examen.

S'agissant des professionnels de santé intervenant dans le programme de dépistage :

– les structures de gestion les informent du traitement de leurs données à caractère personnel conformément à l'article 32-I de la loi ;
– si une plateforme électronique est utilisée pour la communication des résultats, les professionnels de santé sont informés lors de leur connexion à cette plateforme selon les modalités prévues à l'article 32-I de la loi.

Art. 7. – *Sécurité des données et traçabilité des actions.*

Conformément à l'article 34 de la loi « informatique et libertés », le responsable du traitement prend toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, notamment pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Le responsable de traitement définit une politique de sécurité adaptée aux risques présentés par les traitements et à la taille de l'organisme concerné. Cette politique doit décrire :

– les objectifs de sécurité ainsi que les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre ;
– les habilitations d'accès aux données, en fonction du besoin des utilisateurs du système d'information, en particulier les mesures de restriction de l'accès à l'identité des professionnels de santé intervenant dans le programme, les modalités d'accès aux traitements, dont les mesures d'identification et d'authentification ;
– les dispositifs de contrôle des identifications et habilitations et les procédures de traçabilité des accès aux informations médicales, ainsi que l'historique des connexions ;
– les mesures de sécurité devant être mises en œuvre pour les transmissions de données.

Si le format électronique est utilisé par l'intermédiaire d'une plateforme électronique de recueil, d'échange et de mise à disposition des résultats :

– les personnes doivent créer un compte personnel afin de consulter les résultats. Leur adresse électronique pourra être collectée afin de permettre l'envoi d'un courriel contenant un lien permettant d'activer le compte et de vérifier que l'adresse électronique saisie est valide ;
– le contrôle d'accès au compte des professionnels de santé doit être opéré conformément aux dispositions de l'article L. 1110-4 du code de la santé publique qui impose une authentification forte de ces professionnels par l'utilisation d'une carte de professionnel de santé (CPS) ou d'un dispositif équivalent agréé par l'organisme chargé d'émettre la CPS, pour toute transmission ou tout accès aux données de santé ;

– la transmission des informations relatives à la santé doit s'opérer dans des conditions conformes à la délibération no 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.

Dans l'hypothèse d'une transmission par télécopie, les mesures de sécurité suivantes doivent être mises en place :

– le fax doit être situé dans un local physiquement contrôlé et accessible uniquement au personnel habilité ;
– l'impression des messages doit être subordonnée à l'introduction d'un code d'accès personnel ;
– lors de l'émission des messages, le fax doit afficher l'identité du fax destinataire afin d'être assuré de l'identité du destinataire ;
– le carnet d'adresses des fax doit préenregistrer, dans la mesure du possible, les destinataires potentiels.

En cas de recours à un prestataire de service externe pour la mise en œuvre du traitement, le contrat doit prévoir :

– la limitation de l'utilisation des données à la finalité prévue par la présente autorisation ;
– une clause de confidentialité ;
– l'encadrement des modalités de destruction ou de restitution de tous les supports manuels ou informatisés de données à caractère personnel au terme de la prestation ;
– la conformité à l'article L. 1111-8 du code de la santé publique de l'hébergement des données, des modalités d'accès à celles-ci et de leurs modalités de transmission.

Art. 8. – *Abrogation de la délibération du 11 juin 2015.*

La délibération no 2015-175 du 11 juin 2015 portant autorisation unique de traitements de données à caractère personnel ayant pour finalité le dépistage organisé du cancer du sein et du cancer colorectal mis en œuvre par les structures de gestion conventionnées est abrogée.

Il n'est pas nécessaire que les organismes ayant procédé à un engagement de conformité effectués en référence à la délibération no 2015-175 du 11 juin 2015 procèdent à un nouvel engagement de conformité à la présente délibération pour les traitements qui relèveraient de son champ d'application.

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

La présidente,
I. Falque-Pierrotin