Données de santé à caractère personnel en médecine du travail conditions d'hébergement des données notamment informatisées

Alain Carré

PRÉAMBULE

Cette note complète une précédente note sur la conservation, l'accès et la transmission du dossier médical en médecine du travail. En effet, elle est plus spécifiquement destinée à définir les conditions d'hébergement de ces données sous forme matérielle ou numérique dans le cadre des services de santé au travail. Nous ne reviendrons pas sur la responsabilité qui incombe au médecin du travail en matière d'accès et de transmission de ces données ni du droit des patients dans ce domaine qui sont traités dans la note précédente.

LES OBLIGATIONS RÉGLEMENTAIRES EN MATIÈRE D'HÉBERGEMENT DES DONNÉES DE SANTÉ À CARACTÈRE PERSONNEL

Les obligations concernant l'hébergement des données de santé à caractère personnel relèvent de l'article L.1111-8 du Code de la santé publique[1](CSP).

Dans ce cadre, le médecin du travail a qualité de *« personne physique (…) à l'origine (…) du recueil de ces données »*.

Le service de santé au travail assure l'hébergement et la conservation des données de santé à caractère personnel (DSCP) dans le cadre de la médecine du travail, qu'il s'agisse d'un SST autonome ou d'un SST interentreprises. En effet, l'hébergement des DSCP se fait dans des conditions techniques qui dépendent du SST : les dossiers sont conservés dans des locaux et du mobilier dont il est propriétaire, les DSCP sur support numérique sont hébergées sur des serveurs appartenant au SST ou loués par lui à cet effet.

La nature des prestations du SST dans ce domaine correspond à l'activité d'hébergement des données de santé sur tout support définie à l'article R.1111-8-8 du CSP[2] (cette activité *« consiste à héberger les données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social »*) et précisée pour les données papier par l'article R.1111-16 du CSP[3] et pour les données numériques par l'article R.1111-9 du CSP[4]. Dans ce dernier cadre cela consiste à *« assurer (…) tout ou partie des activités suivantes :*

1° La mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé.

2° La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé.

3° La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé.

4° La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information.

5° L'administration et l'exploitation du système d'information contenant les données de santé.

6° La sauvegarde des données de santé. »

Il est également précisé que *« la prestation d'hébergement de données de santé à caractère personnel fait l'objet d'un contrat »* défini à l'article R.1111-11 du CSP[5]. *« La nature des prestations d'hébergement (…) , les rôles et responsabilités de l'hébergeur et des personnes physiques (…) pour le compte desquelles les données de santé à caractère personnel sont conservées, ainsi que les stipulations devant figurer dans le contrat (…) sont précisés par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et des conseils nationaux de l'Ordre des professions de santé* ».

Comme hébergeur de DSCP, le SST doit être titulaire d'un *« certificat de conformité »* défini à l'article R.1111-10 du CSP[6] et être *« agréé par le ministre chargé de la culture pour la conservation de ces données sur support papier ou sur support numérique dans le cadre d'un service d'archivage électronique »*.

DES DISPOSITIONS D'INFORMATION DU MÉDECIN DU TRAVAIL NON CONFORMES

Ainsi, même si le médecin du travail, qui est responsable des DSCP qu'il recueille, doit s'assurer que leur hébergement, leur accès et leur transmission sont conformes au dispositions du Code de la santé publique, le plus souvent, il est confronté à une situation ancienne et aucune information spécifique ne lui est communiquée.

Or, *« l'hébergement, quel qu'en soit le support, papier ou numérique, est réalisé après que la personne prise en charge en a été dûment informée »*.

On peut donc avancer que le contrat de travail du médecin devrait comporter systématiquement une information à ce sujet, par exemple par un codicille spécifique concernant l'hébergement des DSCP quelque soit leur support.

De plus, dans la mesure où le contrat de travail comporte des clauses garantissant les moyens d'un exercice indépendant et conforme à la déontologie médicale, on peut considérer qu'une information systématique formelle, notamment sur l'hébergement des DSCP devrait être délivrée à tout médecin du travail nouvellement embauché.

Comment, si cela n'est pas fait, mettre en cause la responsabilité du médecin en cas de non application des règles concernant non seulement leur hébergement mais également leur transmission ?

UNE MISE EN CONFORMITÉ URGENTE ET NÉCESSAIRE

La mise en conformité récente nécessaire, au regard du règlement général de protection des données (RGPD), devrait être l'occasion de mettre en conformité l'hébergement des DSCP dans les SST.

En effet dans la réalité nous observons que les règles concernant l'hébergement de ces données sont rarement totalement respectées par les SST vis-à-vis des médecins du travail et des salariés.

De plus il semble que des dérives de nature pouvant être délictuelle existent dans certains services :

- Possibilité de transmission automatique de DSCP sur support papier ou informatique de médecin à médecin sans autorisation formelle du patient.
- Contournement du blocage informatique mis en place par le médecin du travail sur demande du travailleur.
- Destruction systématique de données d'exposition du salarié lors du changement de secteur d'un médecin.
- Destruction de dossiers hors des règles de conservation.

Les autorités administratives de tutelle des SST ne devraient-elles pas être plus vigilantes dans ce cadre ?

.....

[1] **Article L.1111-8**, Modifié par Ordonnance n°2017-27 du 12 janvier 2017 - art. 1

I.-Toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, réalise cet hébergement dans les conditions prévues au présent article.

L'hébergement, quel qu'en soit le support, papier ou numérique, est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime. La prestation d'hébergement de données de santé à caractère personnel fait l'objet d'un contrat.

II.-L'hébergeur de données mentionnées au premier alinéa du I sur support numérique est titulaire d'un certificat de conformité. S'il conserve des données dans le cadre d'un service d'archivage électronique, il est soumis aux dispositions du III. Ce certificat est délivré par des organismes de certification accrédités par l'instance française d'accréditation ou l'instance nationale d'accréditation d'un autre État membre de l'Union européenne mentionnée à l'article 137 de la loi n°2008-776 du 4 août 2008 de modernisation de l'économie. Les conditions de délivrance de ce certificat sont fixées par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés et des conseils nationaux de l'Ordre des professions de santé.

III.-L'hébergeur de données mentionnées au premier alinéa du I est agréé par le ministre chargé de la Culture pour la conservation de ces données sur support papier ou sur support numérique dans le cadre d'un service d'archivage électronique. Les conditions d'agrément sont fixées par décret en Conseil d'État pris après avis de la Commission

nationale de l'informatique et des libertés et des conseils nationaux de l'Ordre des professions de santé. L'agrément peut être retiré, dans les conditions prévues par les articles L.121-1, L.121-2 et L.122-1 du Code des relations entre le public et l'administration, en cas de violation des prescriptions législatives ou réglementaires relatives à cette activité ou des prescriptions fixées par l'agrément.

IV.-La nature des prestations d'hébergement mentionnées aux II et III, les rôles et responsabilités de l'hébergeur et des personnes physiques ou morales pour le compte desquelles les données de santé à caractère personnel sont conservées, ainsi que les stipulations devant figurer dans le contrat mentionné au I sont précisés par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et des conseils nationaux de l'Ordre des professions de santé.

V.-L'accès aux données ayant fait l'objet d'un hébergement s'effectue selon les modalités fixées dans le contrat dans le respect des articles L.1110-4 et L.1111-7. Les hébergeurs ne peuvent utiliser les données qui leur sont confiées à d'autres fins que l'exécution de la prestation d'hébergement. Lorsqu'il est mis fin à l'hébergement, l'hébergeur restitue les données aux personnes qui les lui ont confiées, sans en garder de copie. Les hébergeurs de données de santé à caractère personnel et les personnes placées sous leur autorité qui ont accès aux données déposées sont astreints au secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du Code pénal.

VI.-Les hébergeurs de données de santé à caractère personnel ou qui proposent cette prestation d'hébergement sont soumis, dans les conditions prévues aux articles L.1421-2 et L.1421-3, au contrôle de l'inspection générale des affaires sociales et des agents mentionnés aux articles L.1421-1 et L.1435-7, à l'exception des hébergeurs certifiés dans les conditions définies au II. Les agents chargés du contrôle peuvent être assistés par des experts désignés par le ministre chargé de la santé.

VII.-Tout acte de cession à titre onéreux de données de santé identifiantes directement ou indirectement, y compris avec l'accord de la personne concernée, est interdit sous peine des sanctions prévues à l'article 226-21 du Code pénal.

[2] **Article R.1111-8-8**, Créé par Décret n°2018-137 du 26 février 2018 - art. 2

I. - L'activité d'hébergement de données de santé à caractère personnel mentionnée au I de l'article L.1111-8 consiste à héberger les données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social :

1° Pour le compte de personnes physiques ou morales, responsables de traitement au sens de la loi n° 78-17 du 6 janvier 1978, à l'origine de la production ou du recueil de ces données ;

2° Pour le compte du patient lui-même.

Toutefois, ne constitue pas une activité d'hébergement au sens de l'article L.1111-8, le fait de se voir confier des données pour une courte période par les personnes physiques ou morales, à l'origine de la production ou du recueil de ces données, pour effectuer un traitement de saisie, de mise en forme, de matérialisation ou de dématérialisation de ces données.

II. - Les responsables de traitement mentionnés au 1° du I, qui confient l'hébergement de données de santé à caractère personnel à un tiers, s'assurent que celui-ci est titulaire du certificat de conformité mentionné au II de l'article L.1111-8.

[3] **Article R.1111-16**, Modifié par Décret n°2011-246 du 4 mars 2011 - art. 2

S'il est mis en œuvre, l'hébergement des données de santé à caractère personnel sur support papier mentionné à l'article L.1111-8 est confié à une personne physique ou morale bénéficiant d'un agrément accordé par le ministre chargé de la Culture dans les conditions définies par les articles 20-5 à 20-8 et 20-10 à 20-13 du décret n° 79-1037 du 3 décembre 1979 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques et sous réserve des dispositions de l'article R.1111-16-1. Le contrat de prestation d'hébergement cité au deuxième alinéa de l'article L.1111-8 contient au moins les clauses suivantes :

1° La description des prestations réalisées : contenu des services, nature et volume des données, caractère d'archives publiques ou non des données hébergées, résultats attendus.

2° La description des moyens mis en œuvre par le dépositaire pour la fourniture des services.

3° La description des moyens mis en œuvre par le dépositaire pour mettre les données hébergées à disposition des professionnels ou établissement de santé ayant souscrit le contrat.

4° Les modalités retenues pour que l'accès aux données de santé à caractère personnel et leur transmission éventuelle n'aient lieu qu'avec l'accord des personnes concernées et par les personnes désignées par elles ainsi que les dispositifs permettant d'assurer cet accès et cette éventuelle transmission.

5° Les obligations à l'égard du déposant si le dépositaire procède à des modifications ou des évolutions des conditions d'hébergement.

6° Une information sur les garanties permettant de couvrir toute défaillance du dépositaire.

7° Les dispositifs de restitution des archives déposées à la fin du contrat de dépôt dans les conditions définies au quatrième alinéa du R.1112-7, assortis d'un engagement de destruction intégrale des copies que le dépositaire aurait pu effectuer pendant la durée du dépôt.

8° Une information sur les conditions de recours à des prestataires externes ainsi que les engagements du dépositaire pour que ce recours assure un niveau équivalent de garantie au regard des obligations pesant sur l'activité de conservation ;

9° Les moyens mis en œuvre pour assurer le respect des dispositions de l'article L.1111-7 relatif à l'accès des personnes à leurs informations de santé, notamment en termes de délais et de modalités de consultation.;

10° La mention des polices d'assurance que le dépositaire souscrit pour couvrir les dommages et pertes que pourraient subir les données déposées, faisant apparaître que celles-ci excluent expressément les archives déposées du champ d'application de la clause de délaissement.

Est réputée non écrite toute clause tendant à appliquer le droit de rétention aux données de santé à caractère personnel sur support papier.

[4] **Article R1111-9**, modifié par Décret n°2018-137 du 26 février 2018 - art. 2

Est considérée comme une activité d'hébergement de données de santé à caractère personnel sur support numérique au sens du II de l'article L.1111-8, le fait d'assurer pour le compte du responsable de traitement mentionné au 1° du I de l'article R.1111-8-8 ou du patient mentionné au 2° du I de ce même article, tout ou partie des activités suivantes :

1° La mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé.

2° La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé.

3° La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé.

4° La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;

5° L'administration et l'exploitation du système d'information contenant les données de santé.

6° La sauvegarde des données de santé.

[5] **Article R.1111-11**, modifié par Décret n°2018-137 du 26 février 2018 - art. 2

I.-Le contrat d'hébergement mentionné au dernier alinéa du I de l'article L.1111-8 est conclu entre l'hébergeur et son client. Il contient au moins les clauses suivantes :

1° L'indication du périmètre du certificat de conformité obtenu par l'hébergeur, ainsi que ses dates de délivrance et de renouvellement.

2° La description des prestations réalisées, comprenant le contenu des services et résultats attendus notamment aux fins de garantir la disponibilité, l'intégrité, la confidentialité et l'auditabilité des données hébergées.

3° L'indication des lieux d'hébergement.

4° Les mesures mises en œuvre pour garantir le respect des droits des personnes concernées par les données de santé dont notamment :

- *les modalités d'exercice des droits de portabilité des données ;*
- *les modalités de signalement au responsable de traitement de la violation des données à caractère personnel ;*
- *les modalités de conduite des audits par le délégué à la protection des données.*

5° La mention du référent contractuel du client de l'hébergeur à contacter pour le traitement des incidents ayant un impact sur les données de santé hébergées.

6° La mention des indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, le niveau garanti, la périodicité de leur mesure, ainsi que l'existence ou l'absence de pénalités applicables au non-respect de ceux-ci.

7° Une information sur les conditions de recours à d'éventuels prestataires techniques externes et les engagements de l'hébergeur pour que ce recours assure un niveau de protection équivalent de garantie au regard des obligations pesant sur l'hébergeur.

8° Les modalités retenues pour encadrer les accès aux données de santé à caractère personnel hébergées ;

9° Les obligations de l'hébergeur à l'égard de la personne physique ou morale pour le compte de laquelle il héberge les données de santé à caractère personnel en cas de modifications ou d'évolutions techniques introduites par lui ou imposées par le cadre légal applicable.

10° Une information sur les garanties et les procédures mises en place par l'hébergeur permettant de couvrir toute défaillance éventuelle de sa part.

11° La mention de l'interdiction pour l'hébergeur d'utiliser les données de santé hébergées à d'autres fins que l'exécution de l'activité d'hébergement de données de santé.

12° Une présentation des prestations à la fin de l'hébergement, notamment en cas de perte ou de retrait de certification et les modalités de mise en œuvre de la réversibilité de la prestation d'hébergement de données de santé.

13° L'engagement de l'hébergeur de restituer, à la fin de la prestation, la totalité des données de santé au responsable de traitement.

14° L'engagement de l'hébergeur de détruire, à la fin de la prestation, les données de santé après l'accord formel du responsable de traitement et sans en garder de copie.

II.-Lorsque le responsable de traitement de données de santé ou le patient mentionnés au I de l'article R.1111-8-8 fait appel à un prestataire qui recourt lui-même pour l'hébergement des données à un hébergeur certifié, le contrat qui lie le responsable de traitement ou le patient avec son prestataire reprend les clauses mentionnées au I telles qu'elles figurent dans le contrat liant le prestataire et l'hébergeur certifié.

NOTA :

Conformément à l'article 3 I et II du décret n°2018-137 du 26 février 2018, les présentes dispositions entrent en vigueur le 1er avril 2018. Toutefois, le 4° de l'article R.1111-11 dans sa rédaction issue de l'article 2 dudit décret entre en vigueur le 25 mai 2018.

[6] **Article R.1111-10**, Modifié par Décret n°2018-137 du 26 février 2018 - art. 2

I.-Le certificat de conformité mentionné au II de l'article L.1111-8 est délivré par un organisme de certification sur le fondement d'un référentiel de certification élaboré par le groupement d'intérêt public mentionné à l'article L.1111-24 et approuvé par arrêté du ministre chargé de la Santé, pris après avis de la Commission nationale de l'informatique et des libertés.

II.-L'organisme de certification mentionné au II de l'article L.1111-8 est accrédité par le Comité français d'accréditation ou par tout autre organisme d'accréditation signataire d'un accord de reconnaissance mutuelle multilatéral pris dans le cadre de la coordination européenne des organismes d'accréditation conformément à un référentiel d'accréditation élaboré par le groupement d'intérêt public mentionné à l'article L.1111-24 en lien avec les organismes d'accréditation concernés et approuvé par arrêté du ministre chargé de la Santé.

III.-Le groupement d'intérêt public mentionné à l'article L.1111-24 assure le suivi et la mise à jour de ces référentiels.