Avis de contrôle préalable concernant le système de gestion clinique des patients de la Commission européenne (CPMS)

Dossier 2017-0804

***

La Commission européenne est responsable de l'utilisation et du stockage, dans un logiciel, des données des patients relatives aux maladies rares dans l'ensemble de l'Union européenne. Même si tout le traitement est basé sur le consentement explicite, la déclaration de confidentialité devrait être améliorée pour refléter la base juridique ou la licéité du traitement et faire référence à l'exercice des droits d'effacement et de verrouillage. En outre, un délai de conservation ou une période pendant laquelle les prestataires de soins de santé réévaluent la nécessité de conserver les données devrait être défini et certaines mesures de sécurité pourraient être renforcées.

***

Bruxelles, le 6 novembre 2017

Adresse postale: rue Wiertz 60 – B-1047 Bruxelles
Bureaux: rue Montoyer 30 – B-1000 Bruxelles
Courriel: edps@edps.europa.eu – Site web: www.edps.europa.eu
Tél. +32 2-283 19 00 – Fax +32 2-283 19 50

1) Les faits

Le système de gestion clinique des patients (ci-après le «CPMS») est une application logicielle clinique basée sur l'internet mise au point pour soutenir les réseaux européens de référence (ci-après les «réseaux») concernant les maladies rares, à faible prévalence et complexes (ci-après les «maladies rares»). Ces réseaux, au nombre de vingt-quatre, sont des réseaux virtuels de prestataires de soins de santé travaillant en Europe, au-delà des frontières nationales, afin de poser un diagnostic et de prendre en charge les patients atteints de maladies rares[1]. Les maladies rares ont été définies comme celles dont le seuil de prévalence ne dépasse pas cinq personnes affectées sur 10 000[2].

Ce logiciel permet donc l'échange d'informations entre les prestataires de soins de santé[3] en Europe. La Commission gère cette application, qui a été développée par un sous-traitant.

Le CPMS contient donc des données médicales de patients atteints de maladies rares.

1.1. Les utilisateurs

Il existe deux types d'utilisateurs du CPMS.

D'une part, il y a les membres du personnel de la Commission qui sont chargés de la gestion administrative et technique, comme la gestion des problèmes et des incidents relatifs à la sécurité, qui sont compris dans les «utilisateurs» du logiciel d'application.

D'autre part, il y a les utilisateurs *réels*, à savoir les prestataires de soins de santé. Ces utilisateurs font partie d'un hôpital membre d'un réseau (ci-après le «centre»). Outre ces types d'utilisateurs, il peut également y avoir un point local de spécialistes des soins faisant partie d'un hôpital non membre (les «utilisateurs invités»). Les utilisateurs qui font partie d'un hôpital membre ont directement accès aux données de l'application; les utilisateurs invités, quant à eux, ne bénéficient de l'accès qu'en fonction des besoins et cet accès leur est accordé par le coordonnateur responsable du réseau. Pour des raisons d'organisation, les utilisateurs créeront des «demandes de groupe» et désigneront des «chefs de groupe»[4]. Les prestataires de soins de santé, en tant qu'utilisateurs, peuvent créer et participer à des groupes, afin de coopérer sur des dossiers spécifiques.

[1] L'article 12, paragraphe 1, de la directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers établit ce qui suit: «[l]a Commission aide les États membres à créer des réseaux européens de référence entre prestataires de soins de santé et centres d'expertise dans les États membres, en particulier dans le domaine des maladies rares. Les réseaux reposent sur la participation volontaire de leurs membres, qui participent et contribuent aux activités des réseaux conformément à la législation de l'État membre où ils sont établis et sont toujours ouverts aux nouveaux prestataires de soins de santé qui souhaiteraient y adhérer, à condition que ces prestataires remplissent l'ensemble des conditions et critères [...]» (JO L 88 du 4.4.2001, p. 45).

[2] Voir considérant 55 de la directive susmentionnée (note de bas de page 1).

[3] L'article 3, point g), de la directive susmentionnée (note de bas de page 1) définit les prestataires de soins de santé comme «toute personne physique ou morale ou toute autre entité qui dispense légalement des soins de santé sur le territoire d'un État membre».

[4] Les utilisateurs invités ne peuvent pas être chefs de groupe.

Les prestataires de soins de santé doivent d'abord s'authentifier à l'aide d'un EU Login pour accéder à l'application[5]. La Commission (par l'intermédiaire d'un sous-traitant) fournit cet accès et est ainsi directement responsable du traitement des données administratives des prestataires de soins de santé[6].

Le service d'authentification et de gestion de l'identité de la Commission est utilisé pour enregistrer les utilisateurs afin qu'ils puissent accéder au CPMS. Après la création d'un EU Login, le compte de l'utilisateur est validé grâce à un outil de service en ligne, le service d'autorisation SAAS2, qui relève de la Commission[7]. Cet outil est utilisé pour accorder une autorisation à une partie restreinte et déterminée de personnes, au niveau des réseaux, ayant des rôles définis; seuls les utilisateurs autorisés ont accès au CPMS via cet outil.

1.2. Les catégories de données

Deux catégories de données sont traitées dans le CPMS.

Dans un premier temps, les prestataires de soins de santé encodent les données administratives réelles du patient dans le CPMS, dans la section «données d'identification». Ces données comprennent les éléments suivants: nom, prénom, genre, date et lieu de naissance et niveau d'enseignement.

Ensuite, dans la section «demande de consultation», les prestataires de soins de santé pseudonymisent le nom du patient et y substituent un surnom qui ne doit présenter aucune similitude avec le véritable nom du patient. Les autres prestataires de soins de santé, qui travaillent dans d'autres centres, auront uniquement accès au surnom et aux données médicales, mais pas aux données réelles encodées dans la section «données d'identification»[8]. Les données médicales traitées sont les suivantes: demande de consultation, description de crise, diagnostic de maladie rare, comorbidités, phénotype, caractéristiques génétiques et biobanques, antécédents familiaux, comportements en matière de santé, allergies et autres réactions indésirables, historique des maladies et troubles antérieurs, intervention de traitement spécial, historique chirurgical et de transplantation, et médication. Des images, photographies et vidéos peuvent également être traitées. Des méthodes d'anonymisation sont utilisées pour retirer des images traitées tout élément qui révélerait l'identité du patient et pour leur substituer un identifiant unique.

1.3. Pseudonymisation

D'un point de vue technique, les données relatives à la santé des patients sont d'abord encodées dans le CPMS, avant d'être pseudonymisées[9]. Lorsqu'un nouveau patient est ajouté dans le

[5] Les utilisateurs gèrent leur propre mot de passe et EU Login.

[6] Nom d'utilisateur EU Login, noms et prénoms, nom du prestataire de soins de santé, hôpital ou centre, nom du réseau, adresse électronique professionnelle et pays.

[7] Plus précisément, la direction générale de la santé et de la sécurité alimentaire.

[8] Chaque fois qu'un patient est enregistré dans le CPMS, le système génère pour lui un identifiant unique. Cet identifiant est uniquement visible par les spécialistes de la santé dans un centre ou un hôpital en particulier.

[9] La «pseudonymisation» est définie comme le traitement de données à caractère personnel de telle façon qu'elles ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations

CPMS, un identifiant automatique, ID1, est généré par le système. Cet ID1 sera ensuite stocké dans le dossier cliniques du patient, ou l'utilisateur remplacera l'ID1 par l'identifiant du dossier du patient de l'hôpital. Par la suite, lorsqu'un professionnel de la santé souhaitera encoder des données relatives à la santé pour créer un groupe de discussion, il choisira un surnom pour le patient. En remplaçant l'ID1 par un surnom, le CPMS renforce encore la pseudonymisation. Comme déjà mentionné, les données pseudonymisées sont ensuite transférées à d'autres utilisateurs du CPMS en vue de discussions de groupe et d'une évaluation du dossier d'un patient. Seuls le centre et les professionnels de la santé ont accès à l'ID1 du patient. Les autres centres et utilisateurs peuvent uniquement voir le surnom du patient. Le CPMS ne permet qu'aux utilisateurs du centre/de l'hôpital qui a enregistré les données des patients de les supprimer du système.

1.4. Formulaires de consentement et accès aux données

Pour figurer dans le logiciel, le patient doit donner son consentement explicite et indubitable au prestataire de soins de santé[10]. Il existe un formulaire intitulé «*Formulaire de consentement du patient pour le partage de données au sein du réseau européen de référence pour les maladies rares, pour les soins au patient et la création de registres pour les maladies rares*». Ce formulaire de consentement comporte trois cases: la première concerne le consentement au partage de données, la deuxième le consentement à l'inclusion dans une base de données, et la troisième la possibilité d'être contacté à des fins de recherche. Les patients doivent signer directement dans la case «J'accepte» ou dans la case «Je refuse».

Le prestataire de soins de santé chargé de l'encodage des données du patient dans la base de données ne peut accéder au CPMS sans indiquer explicitement que le formulaire de consentement a été complété[11]. Ces formulaires sont traduits dans toutes les langues officielles de l'Union européenne. Les formulaires de consentement ne sont pas téléchargés dans le CPMS une fois qu'ils sont complétés; ils sont conservés par le prestataire de soins de santé.

Seuls les prestataires de soins de santé qui ont au préalable été validés par la Commission et qui ont préalablement reçu le consentement écrit explicite pour le téléchargement d'informations se voient octroyer l'accès. Ni la Commission ni le sous-traitant n'ont, à aucun moment, accès aux données des patients, comme indiqué dans une note signée par le directeur,

supplémentaires, pour autant que celles-ci soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir cette non-attribution à une personne physique identifiée ou identifiable.

[10] La décision déléguée de la Commission définit le consentement comme suit: «consentement éclairé dans le cadre des réseaux européens de référence: l'expression libre, spécifique, éclairée et explicite des souhaits d'une personne, faite sous la forme d'une déclaration ou d'une action clairement résolue, par laquelle cette personne signifie son accord à l'échange de ses données personnelles et médicales entre les prestataires de soins de santé et les membres d'un réseau européen de référence, comme le prévoit la présente décision déléguée». Voir article 2, point e), de la décision déléguée de la Commission du 10 mars 2014 établissant les critères et conditions que doivent remplir les réseaux européens de référence et les prestataires de soins de santé qui souhaitent adhérer à un réseau européen de référence (JO L 147 du 17.5.2014, p. 71).

[11] Les prestataires de soins de santé doivent cocher une case pour chaque type de consentement donné. Les manuels d'utilisation et d'autres documents pratiques établissent que le formulaire d'inscription ne peut pas être sauvegardé à moins que la case «consentement aux soins» ne soit cochée, ce qui indique qu'un consentement valide a été donné. Il y a trois cases différentes, qui correspondent aux trois types de consentement qui peuvent être donnés dans le formulaire.

en sa qualité de responsable du traitement pour le système CPMS[12]. En d'autres termes, aucune donnée des patients n'est traitée dans le service d'authentification et de gestion de l'identité ni dans le service d'autorisation SAAS2.

1.5. Délai de conservation

Aucun délai de conservation n'est défini pour les données médicales encodées par les prestataires de soins de santé; elles seront conservées aussi longtemps que nécessaire.

1.6. Dispositifs de sécurité

[....]

2) Analyse juridique

Le présent avis de contrôle préalable[13] au titre de l'article 27 du règlement (CE) nº 45/2001[14] (ci-après le «règlement») portera sur les aspects qui soulèvent des problèmes de conformité avec le règlement ou qui méritent une analyse plus approfondie. En ce qui concerne les aspects qui ne sont pas abordés dans le présent avis, le CEPD n'émet, sur la base des documents fournis, aucun commentaire.

Le traitement relève de l'article 27, en ceci qu'il concerne le traitement de données sensibles, à savoir des données relatives à la santé, et est susceptible d'avoir une influence sur les droits et libertés de la personne concernée.

2.1 Licéité du traitement

Il convient de clarifier d'emblée qu'il est ici question de deux traitements distincts. D'une part, il y a la collecte et le traitement des données administratives des utilisateurs par la Commission (par l'intermédiaire de son sous-traitant). Étant donné que le traitement de ces données est purement administratif et ne concerne que les données d'identification des prestataires de soins de santé, il ne rentre pas dans le champ d'application de l'article 27, paragraphe 2, du règlement, et ne nécessite pas un contrôle préalable.

[12] Voir «*Commission access to ERN-CPMS system*» (accès de la Commission au système ERN-CPMS). Note pour le dossier signée par voie électronique le 1er septembre 2017 [référence ARES (2017) 4283273].

[13] Conformément à l'article 27, paragraphe 4, du règlement, le CEPD rend son avis dans les deux mois qui suivent la réception de la notification, durée des suspensions non incluse. La notification a été reçue le 8 septembre 2017. Le CEPD doit par conséquent rendre son avis pour le 8 novembre 2017 au plus tard. Par un courrier électronique daté du 8 septembre 2017, le délégué à la protection des données (ci-après le «DPD») de la Commission a envoyé une notification en vue d'un contrôle préalable concernant le traitement appelé système de gestion clinique des patients (ci-après le «CPMS»).[13] Par un courrier électronique daté du 14 septembre 2017, le CEPD a accusé réception de la notification et a posé cinq questions complémentaires. Par un courrier électronique daté du 18 septembre 2017, le DPD de la Commission a répondu aux questions et a proposé deux dates différentes afin de procéder à une démonstration du système. Ladite démonstration a eu lieu le 28 septembre, dans les locaux de la DG SANTE.

[14] JO L 8 du 12.1.2001, p. 1.

D'autre part, il y a le traitement réalisé par les prestataires de soins de santé qui enregistrent les données des patients, y accèdent, les modifient, les consultent et les récupèrent[15]. Ce traitement est réalisé uniquement par les prestataires de soins de santé, qui sont chargés de la collecte des formulaires de consentement, mais a lieu sur une plateforme de soutien gérée par la Commission. Celle-ci, par l'intermédiaire de son sous-traitant, est responsable du stockage et de la sécurité des données et assume donc la coresponsabilité avec le centre du prestataire de soins de santé qui soigne le patient et traite les données. La Commission et les centres sont par conséquent coresponsables du traitement. Le présent avis de contrôle préalable portera uniquement sur ce second traitement, à savoir celui réalisé par les prestataires de soins de santé, dès lors qu'il concerne directement les données relatives à la santé au sens de l'article 27, paragraphe 2, point a), du règlement.

Le traitement est licite pour deux motifs différents.

Premièrement, conformément à l'article 5, point a), du règlement, le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités. L'article 12 de la directive relative à l'application des droits des patients en matière de soins de santé transfrontaliers établit les réseaux européens de référence[16]. Par ailleurs, le règlement portant établissement d'un troisième programme d'action dans le domaine de la santé[17] dispose que l'une des priorités est d'aider les patients atteints d'une maladie rare, ce qui inclut «la création de réseaux de référence [...] et la mise en place, à l'échelle de l'Union, de bases de données d'informations et de registres pour les maladies rares sur la base de critères communs». Ces actes constituent la base juridique pour la création du CPMS.

Deuxièmement, le traitement est licite, en ceci qu'il est basé sur un consentement explicite et relève donc de l'article 5, point d), du règlement: les patients doivent directement signer dans une case pour donner leur consentement ou dans une autre pour le refuser. À partir du moment où il y a une signature, aucune ambiguïté n'est possible. Le consentement explicite du patient constitue le motif de licéité du traitement.

Le CEPD relève que, par le formulaire de consentement, le patient doit donner explicitement son consentement[18]. En outre, le consentement est divisé en trois parties; les patients peuvent donc, par exemple, consentir au partage de leurs données anonymisées, mais refuser d'être

[15] Comme déjà mentionné ci-dessus, ces données sont pseudonymisées pour tous les prestataires de soins de santé à l'exception de ceux de l'hôpital d'origine.

[16] Voir note de bas de page 1.

[17] Règlement (UE) nº 282/2014 du Parlement européen et du Conseil du 11 mars 2014 portant établissement d'un troisième programme d'action de l'Union dans le domaine de la santé (2014-2020) et abrogeant la décision nº 1350/2007/CE (JO L 86 du 21.3.2014, p. 1). L'annexe I, point 4.2, définit les priorités thématiques pour le financement, parmi lesquelles se trouve la suivante: «[a]ppuyer l'action des États membres, des associations de patients et des parties concernées par une coordination à l'échelle de l'Union en vue d'aider efficacement les patients atteints d'une maladie rare. Ceci inclut la création de réseaux de référence (conformément au point 4.1.) et la mise en place, à l'échelle de l'Union, de bases de données d'informations et de registres pour les maladies rares sur la base de critères communs».

[18] Le considérant 12 de la décision déléguée de la Commission mentionnée dans la note de bas de page 6 établit qu'«[a]fin de permettre l'échange de données à caractère personnel dans le cadre des réseaux, les procédures relatives à l'obtention du consentement éclairé pour le traitement de ces données pourraient être simplifiées grâce à l'adoption d'un modèle unique de consentement, soumis aux exigences fixées par la directive 95/46/CE en ce qui concerne le consentement de la personne concernée».

contactés pour des recherches. Le CEPD considère cette méthode détaillée et explicite de consentement comme une bonne pratique. Le consentement doit être libre, spécifique et informé[19], ce qui semble être le cas, étant donné que le formulaire précise ce qui suit: «si vous décidez de ne pas donner votre consentement, cela n'aura aucune conséquence sur vos soins» et «si vous donnez votre consentement aujourd'hui, vous pouvez vous rétracter par la suite». Il est également précisé plus loin que «[...] même si vous décidez de ne pas donner votre consentement, vos médecins continueront de vous soigner dans toute la mesure de leurs moyens».

2.2 Qualité des données

Comme déjà mentionné ci-dessus, il existe, dans le cas présent, deux séries différentes de données. D'un côté, il y a les données réelles du patient, qui incluent les nom, prénom, lieu de résidence, lieu et date de naissance et niveau d'études. De l'autre, il y a le surnom ainsi que les données médicales, qui peuvent contenir des informations supplémentaires relatives à la maladie, comme des images, des vidéogrammes, etc.

Conformément à l'article 4, paragraphe 1, point c), les données à caractère personnel doivent être «adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement». Cette règle suppose un lien nécessaire entre les données et les finalités pour lesquelles elles sont traitées.

Le CEPD considère que les informations relatives au niveau d'études de la personne concernée, collectées dans les «données d'identification», ne sont pas nécessaires, ni pertinentes dans tous les cas, pour la finalité médicale visée. Il devrait donc être précisé dans l'application que ces données seront collectées uniquement si cela s'avère nécessaire à des fins médicales[20]. Par ailleurs, il est possible que la collecte d'images et de vidéogrammes rende les patients identifiables (par exemple, images faciales, ou noms apparaissant dans l'imagerie). Les centres devraient donc s'assurer que les photographies et les véritables noms soient masqués autant que possible.

Le CEPD recommande de collecter des données sur le niveau d'études d'un patient uniquement si cela s'avère pertinent et nécessaire à des fins médicales. En outre, les photographies et autres informations d'identification dans les vidéogrammes et images devraient, autant que faire se peut, être masquées.

2.3 Information des personnes concernées

Premièrement, une déclaration de confidentialité assez complète est fournie aux utilisateurs de l'application, à savoir les prestataires de soins de santé. Deuxièmement, il existe un formulaire de consentement pour les patients, qui contient une courte déclaration de confidentialité concernant les droits de la personne concernée. Toutefois, ce formulaire ne contient pas tous les éléments énumérés aux articles 11 et 12 du règlement. Il ne fait notamment pas référence à la base juridique ou à la licéité du traitement ainsi qu'aux délais d'exercice des droits d'accès et de modification en cas d'erreur. Il ne contient pas non plus d'informations concernant les

[19] Groupe de travail «Article 29» sur la protection des données, avis 15/2011 sur la définition du consentement, adopté le 13 juillet 2011.

[20] Cette question a été soulevée lors de la réunion du 28 septembre 2017. Les responsables du traitement qui s'occupent de l'application ont affirmé que ces données pouvaient être importantes lorsque la santé mentale est en jeu, ainsi que lorsque le patient est un médecin, par exemple, qui peut mieux comprendre la terminologie, etc.

droits d'effacement et de verrouillage[21], ce qui devrait être le cas, ni d'informations concernant le délai de conservation.

Le CEPD recommande donc de compléter le «formulaire de consentement» en ajoutant des informations (sous la forme d'une liste à puces, par exemple) concernant la licéité du traitement, les délais d'exercice des droits, les modalités de verrouillage et d'effacement et un délai de conservation raisonnable.

2.4 Sécurité du traitement

Les responsables du traitement sont les prestataires de soins de santé (conjointement avec la Commission, qui agit en tant que coresponsable du traitement). Toutefois, le concept de prestataire de soins de santé ne couvre pas seulement les médecins, mais également «toute personne physique ou morale ou toute autre entité qui dispense légalement des soins de santé sur le territoire d'un État membre»[22]. Les médecins sont tenus par des déclarations de confidentialité ou des documents similaires. Néanmoins, il n'est pas toujours clair que les autres professionnels de la santé sont tenus par les mêmes règles. Le CEPD recommande par conséquent à la Commission de s'assurer, en sa qualité de coresponsable du traitement, que tous les utilisateurs du CPMS signent une déclaration de confidentialité similaire à celle des médecins[23].

Le CEPD recommande de s'assurer que tous les utilisateurs du CPMS signent une déclaration de confidentialité similaire à celle des médecins

Le CEPD prend note du fait que les données relatives à la santé du patient sont incluses de manière pseudonymisée, sous un «surnom». Ledit surnom doit être attribué par un prestataire de soins de santé, qui reçoit comme consigne de «ne pas insérer de données réelles» dans le formulaire d'inscription des patients. Cette consigne pourrait être renforcée en disposant plus explicitement que le surnom ne devrait présenter aucune similitude avec le véritable nom du patient. Le CEPD se réjouit du fait que le responsable du traitement, lors de la réunion du 28 septembre 2017, ait proposé de fournir des moyens techniques pour garantir un filtre et le rejet automatiques des surnoms contenant partiellement le nom ou prénom du patient.

Le CEPD recommande à la Commission de renforcer les consignes concernant le surnom en demandant explicitement aux prestataires de soins de santé de s'assurer que celui-ci ne présente aucune similitude avec les données réelles du patient.

[…]

[21] Il est néanmoins précisé dans la notification que le délai de verrouillage ou d'effacement sur la base de demandes légitimes et justifiées des personnes concernées est de quatre semaines.

[22] Voir note de bas de page 3.

[23] Voir, à cet égard, les «Lignes directrices du CEPD concernant le traitement des données relatives à la santé sur le lieu de travail par les institutions et organes communautaires». Septembre 2009. Ces lignes directrices fournissent des recommandations concernant «l'application de codes de conduite ou de déclarations de confidentialité pour toutes les personnes impliquées dans le traitement qui ne sont pas tenues au secret professionnel».

2.5 Délai de conservation

Conformément à l'article 4, paragraphe 1, point e), du règlement, les données à caractère personnel doivent être «conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement». Les données à caractère personnel conservées pendant des périodes plus longues «à des fins historiques, statistiques ou scientifiques [...] ne seront conservées que sous une forme qui les rend anonymes, soit, si cela est impossible, [...] ne seront stockées qu'à condition que l'identité de la personne concernée soit cryptée».

Aucun délai de conservation n'est défini. Selon la Commission, les professionnels de la santé conserveront les données dans le CPMS aussi longtemps que nécessaire.

La Commission devrait fixer un délai raisonnable en fonction des finalités du traitement. Ledit délai pourrait être différent pour les données traitées à des fins de diagnostic et de traitement (dont la présence dans le CPMS ne semble plus pertinente après guérison définitive) et les données traitées pour la recherche (lorsque les patients ont donné leur consentement)[24]. Pour ces dernières, le délai de conservation pourrait être plus long, étant donné que les données sont conservées d'une manière anonymisée ou cryptée et sécurisée. Sinon, la Commission pourrait demander aux prestataires de soins de santé de réévaluer régulièrement la nécessité de conserver les données (par exemple, tous les 10 ou 15 ans après l'enregistrement dans la base de données).

Le CEPD recommande de fixer un délai de conservation concret afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire. Une autre solution serait de demander périodiquement aux prestataires de soins de santé qui ont enregistré les données de réévaluer la nécessité de conserver lesdites données.

Recommandations

Dans le présent avis, le CEPD a formulé plusieurs recommandations visant à garantir la conformité avec le règlement. Sous réserve de la mise en application de ces recommandations, le CEPD considère qu'il n'existe aucune raison de conclure à une violation des dispositions du règlement.

En ce qui concerne les **recommandations** suivantes, le CEPD attend leur **mise en application et des justificatifs** attestant de leur mise en application dans un délai de **trois mois** suivant la date de publication du présent avis:

- collecter des données sur le niveau d'enseignement d'un patient uniquement si cela s'avère nécessaire et pertinent à des fins médicales. Par ailleurs, les photographies et

[24] Les lignes directrices susmentionnées établissent que «[d]e manière générale, en ce qui concerne la conservation des données médicales, le CEPD estime qu'une période de 30 ans peut, dans la majorité des cas, être considérée comme étant la durée de conservation maximale autorisée de données dans ce contexte» (voir point 4).

informations complémentaires contenues dans les vidéogrammes et images doivent, autant que faire se peut, être masquées;

- compléter le «formulaire de consentement» en ajoutant des informations (sous la forme d'une liste à puces, par exemple) concernant la licéité du traitement, les délais d'exercice des droits, les modalités de verrouillage et d'effacement et un délai de conservation raisonnable;

- s'assurer que tous les utilisateurs du CPMS signent une déclaration de confidentialité similaire à celle des médecins;

- renforcer les consignes concernant le surnom en demandant explicitement aux prestataires de soins de santé de s'assurer qu'il ne présente aucune similitude avec les données réelles du patient;

- […]

- fixer un délai de conservation concret afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire; ou demander périodiquement aux prestataires de soins de santé qui ont enregistré les données de réévaluer la nécessité de conserver lesdites données.

Le CEPD se réjouit du fait que la Commission a déjà commencé à mettre en application certaines des recommandations à la suite de la réunion du 28 septembre.

Fait à Bruxelles, le 6 novembre 2017

(signé)

Wojciech RAFAŁ WIEWIÓROWSKI