ARTICLE

LE SECRET MÉDICAL À L'ÉPREUVE DES CYBERATTAQUES : RÉFLEXIONS AUTOUR DU CAS CEGEDIM SANTÉ

IT et données personnelles | 09/03/26 | Roxane Blanc-Dubois

DATA PRIVACY SCIENCES DE LA VIE & SANTÉ CYBERSÉCURITÉ

1) Le contexte

Lors d'un reportage diffusé le 26 février 2026, France 2 a révélé l'existence d'une cyberattaque ayant visé le logiciel « MonLogicielMedical » (MLM) et conduit à la violation de données personnelles de plusieurs millions de français.

La société Cegedim Santé, éditrice du logiciel MLM, le présente comme une solution web de gestion de cabinet médical[1].

Le communiqué de presse publié par la société Cegedim à la suite du reportage confirme que « *fin 2025, un comportement anormal de requêtes applicatives sur des comptes médecins utilisateurs du logiciel MLM* » a été détecté. 1500 médecins utilisateurs du logiciel seraient concernés par l'attaque[2].

Dans son communiqué, la société distingue le dossier administratif du dossier médical afin de souligner que seules des données issues du dossier administratif des patients auraient été illégitimement consultées ou extraites. Les données concernées sont les « *nom, prénom, sexe, date de naissance, téléphone, adresse, email et commentaire administratif en texte libre à la discrétion des médecins* ».

Cependant, pour une partie des patients concernés, les zones de commentaire libre contenaient des données sensibles renseignées par les médecins utilisateurs du logiciel, telles que des informations sur l'orientation sexuelle ou les convictions religieuses.

La société Cegedim indique que la CNIL a été notifiée de cette violation de données personnelles. Il est possible que la CNIL mène actuellement un contrôle à ce sujet, compte tenu du nombre important de personnes concernées par la violation et de la médiatisation de l'affaire.

2) Les cyberattaques ciblant le secteur de la santé ne sont pas qu'une menace mais constituent une réalité aux conséquences multiples.

En 2024, les cyberattaques, tous secteurs confondus, ont **augmenté de 15%** et cette tendance haussière se confirme pour 2025-2026[3].

Le secteur de la santé est particulièrement touché[4], avec des conséquences pouvant être dramatiques :

- Paralysie d'un établissement victime d'une cyberattaque, se retrouvant dans l'incapacité de gérer les patients et entrainant une perte de chance pour eux[5] ;

- Chantage sous la menace de publier des données relatives à des pathologies afin d'extorquer des fonds (plus la maladie est stigmatisée, plus ce type de chantage peut fonctionner) ;

- Discrimination subie par les personnes dont les données sensibles ont été divulguées ;

- Prise de décision médicale inadaptée mettant en danger la vie des patients (notamment lorsque leurs données ont été modifiées par un cyberattaquant) ;

- Usurpation d'identité et arnaque (dont les chances de succès sont élevées lorsque les personnes malveillantes disposent de nombreuses données sur une même personne) ;

- Perte financière pour l'établissement victime (perte de revenus, frais de reconstruction du système d'information, coûts liés à la soustraitance des activités à l'arrêt).

Le cas Cegedim Santé est ainsi un exemple supplémentaire de violation de données dans le domaine de la santé. Compte tenu de la nature des données mises en vente sur le *dark web* à la suite de l'attaque[6], les risques d'arnaque ou de chantage ne peuvent être exclus (d'autant que des données relatives à des personnalités politiques auraient été

extraites), tout comme les risques de discrimination (au regard de la sensibilité de certaines données exposées).

Etant donné le risque élevé de la menace cyber, la question en la matière n'est plus « *une cyberattaque va-t-elle survenir ?* » mais plutôt « *quand ?* » et « *mon organisation est-elle armée et préparée* ? »

Or, face à cette réalité, l'une des questions centrales est celle des responsabilités.

3) La sécurisation des données est l'affaire de tous et surtout de chacun[7].

Chaque acteur intervenant dans la chaîne du soin doit se sentir concerné et prendre ses responsabilités pour assurer la protection des données personnelles.

C'est d'ailleurs la logique du RGPD qui responsabilise l'ensemble des acteurs : il impose des obligations tant aux responsables de traitement (= ceux qui décident du traitement et de ses modalités), qu'aux sous-traitants (= ceux qui traitent des données personnelles sur instruction des responsables de traitement). La sécurité des données incombe à ces deux catégories d'acteurs (article 32 du RGPD).

Dans le milieu médical, les professionnels de santé sont en principe considérés comme responsables de traitement[8], au sens du RGPD, pour les données des patients qu'ils utilisent aux fins de leur fournir les soins. Si ces professionnels font appel à un éditeur de logiciel SaaS dans ce cadre, celui-ci est en principe qualifié de sous-traitant au sens du RGPD à l'égard des données des patients.

Or, il n'est pas rare qu'un professionnel de santé, dont le cœur de métier consiste à soigner des patients, estime qu'il revient à son prestataire - éditeur de logiciel SaaS - de respecter les obligations du RGPD (comme s'il les lui déléguait).

A cet égard, s'il est vrai qu'un éditeur SaaS doit proposer une solution logicielle qui (i) tienne compte, dès sa conception, des principes de protection des données et qui (ii) garantisse, par défaut, que seules les données nécessaires à l'objectif du traitement soient traitées[9] (« *privacy by design and by default* »), il n'en demeure pas moins que le professionnel de santé[10] reste responsable du traitement au titre du RGPD. L'utilisation d'un logiciel fourni par un tiers pour l'aider à gérer sa relation avec son patient ne change pas cette qualification. A ce titre, le professionnel de santé[11] doit respecter les obligations mises à sa charge par le RGPD et vérifier, avant de sélectionner son prestaire éditeur, que celui-ci présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de façon à ce que le traitement réponde aux exigences du RGPD.

Il est aussi censé surveiller, par des **diligences raisonnables**, les actions de son sous-traitant une fois celui-ci sélectionné. La responsabilité du responsable de traitement peut être engagée en cas d'absence de **contrôle régulier** des mesures techniques et organisationnelles prises par son sous-traitant.[12]

Le caractère suffisant de ces diligences raisonnables s'apprécie en fonction des **compétences et des moyens** du responsable de traitement. Cela a pu justifier, selon nous, que la CNIL sanctionne **uniquement** un sous-traitant, éditeur d'un logiciel en santé, pour des défauts de sécurité qui lui étaient imputables et ayant permis une violation de données, lorsque les responsables de traitement utilisateurs dudit logiciel n'avaient pas de compétence IT.[13]

Il s'agit donc d'une appréciation au cas par cas.

Cela étant, si la CNIL devait constater, dans le cadre d'une cyberattaque, un manquement aux principes essentiels du RGPD – tel que le principe de minimisation des données - imputables aux responsables de traitement, elle pourrait aisément sanctionner ces responsables de traitement à ce titre.

S'agissant spécifiquement du principe de minimisation, il constitue justement un levier essentiel de sécurisation des données et de limitation des effets d'une cyberattaque.

4) Le principe de minimisation, pierre angulaire de la protection des données, fragilisé par les zones de commentaire libre

Dans une cyberattaque comme celle ayant impacté Cegedim Santé, **le principe de minimisation des données** prend tout son sens. Pour mémoire, il s'agit d'un principe posé par l'article 5 du RGPD, qui impose au responsable de traitement de ne traiter que les données strictement nécessaires pour répondre à l'objectif du traitement. Le respect de ce principe est **fondamental** pour **réduire l'impact** humain en cas de cyberattaque : moins il y a de données traitées et moins la cyberattaque aura de conséquences néfastes.

Or, avec les zones de commentaire libre telles que celles qui figurent dans le logiciel MLM (aussi appelées zones « *bloc-note* »), le risque est que certains soient tentés d'y inscrire davantage de données que nécessaire, en violation du principe de minimisation. La CNIL a d'ailleurs déjà pu relever, par le passé, des dérives liées à des commentaires excessifs, subjectifs ou inadaptés au sein de telles zones de commentaire libre et sanctionner à ce titre[14].

Trois éléments en particulier interrogent dans le cas d'espèce :

- Se pose la question de la légitimité même de l'existence d'une telle zone de commentaire libre dans une section présentée par Cegedim Santé comme étant purement administrative. Cegedim Santé sera peut-être amenée à devoir expliquer la raison de l'intégration de la zone de commentaire libre dans le logiciel pour la partie administrative du dossier patient. A supposer que cela soit légitime, les deux interrogations suivantes demeurent.

- Une zone de commentaire libre insérée dans une section dite « **administrative** » (selon Cegedim Santé) pouvait-elle légitimement inclure, de la part des professionnels de santé, des commentaires portant sur des données sensibles telles que la santé du patient ?

- De surcroit, des données sensibles autres que celles portant sur la santé des patients (telles que l'orientation sexuelle supposée ou les convictions religieuses d'un patient comme ont pu le rapporter les médias) étaient-elles réellement **justifiées** pour la **prise en charge** desdits patients ? Les professionnels de santé concernés doivent être en mesure de justifier en quoi ces données seraient strictement nécessaires à la prise en charge de leur patient. Dans le cas contraire, ils s'exposent notamment à des risques de sanction de la part de la CNIL. A cet égard, certains médias rapportent que le ministère de la Santé aurait indiqué, de manière générale, que « *le fait pour un médecin de consigner de telles annotations concernant le quotidien et l'intimité des patients n'enfreint pas le règlement général sur la protection des données (RGPD)* »[15].

Reste à savoir ce que conclura l'enquête et si des manquements seront identifiés et sanctionnés par la CNIL à l'égard de Cegedim Santé (notamment en tant que sous-traitant)[16] mais aussi à l'égard des professionnels de santé (en tant que responsables de traitement).

---

[1] Présentation donnée sur le site internet de Cegedim Santé.

[2] Communiqué de presse de Cegedim en date du 26 février 2026.

[3] Propos tiré du discours de Matthieu Autret, Chef de la mission contrôles et supervision à l'ANSSI, lors de la 20e Université des DPO en date du 5 février 2026.

[4] La CNIL note que les notifications de violation de données personnelles par les centres hospitaliers sont passées de 16 en 2018 à 196 en 2024. En 2024, les exfiltrations massives de données dans le secteur de la santé ont également connu une ampleur inédite (33 millions pour deux prestataires de tiers payant en février, 750 000 pour un établissement francilien en novembre).

[5] Les exemples d'attaques d'établissements de santé par ransomware impliquant le chiffrement des données de patients (lesquelles deviennent alors inaccessibles) sont nombreux. Ce genre d'attaques contraignent les établissements de santé à reporter des interventions programmées et transférer des patients vers d'autres établissements de santé.

[6] Comme rapporté par plusieurs médias.

[7] La nuance est importante car lorsqu'une tâche est attribuée à « *tout le monde* », les personnes censées gérer cette tâche se sentent moins concernées de la réaliser dans la mesure où elle compte sur les autres.

[8] Ou les établissements au sein desquels ils travaillent, le cas échéant.

[9] Guide du sous-traitant de la CNIL, édition septembre 2017. La CNIL indique, à titre d'exemple, qu'un éditeur ne devrait pas rendre techniquement obligatoire le renseignement d'un champ facultatif.

[10] Ou l'établissement au sein duquel il travaille, le cas échéant.

[11] Ou l'établissement de santé, le cas échéant.

[12] Délibération CNIL SAN-2023-006 du 11 mai 2023.

[13] Délibération CNIL SAN-2022-009 du 15 avril 2022.

[14] Recommandation CNIL du 28 février 2019 : zone bloc note et commentaires : les bons réflexes pour ne pas déraper.

[15] Par exemple, dans les articles de Franceinfo ou du Huffpost du 27 février 2026. A ce stade, nous n'avons toutefois pas identifié de prise de position écrite émanant des représentants du ministère indiquant cela. Certains médias mentionnent un point de presse organisé par le ministère : il est possible que ces propos aient été tenus à cette occasion.

[16] A noter que la société Cegedim Santé avait été sanctionnée en 2024 par la CNIL pour un tout autre traitement de données de santé, qu'elle mettait en œuvre en tant que responsable de traitement au mépris du cadre légal des formalités préalables obligatoires auprès de la CNIL. Pour plus d'information sur cette délibération de la CNIL, nous vous invitons à lire notre article sur le sujet accessible ici.