N°4718
Entrée le 07.09.2026
Chambre des Députés
Déclarée recevable et urgence non-reconnue
Président de la Chambre des Députés
(s.) Claude Wiseler
Luxembourg, le 07.09.2026

LSAP

Monsieur Claude Wiseler
Président de la Chambre des Députés
Luxembourg

Luxembourg, le 7 septembre 2026

Monsieur le Président,

Conformément à l'article 81 du règlement de la Chambre des Députés, je vous prie de bien vouloir transmettre la question parlementaire **urgente** suivante à Madame la ministre de la Santé et de la Sécurité sociale ainsi qu'à Madame la ministre de la Digitalisation.

La digitalisation croissante du secteur de la santé conduit les médecins et autres professionnels de santé à recourir à des prestataires informatiques privés pour la gestion de leurs logiciels médicaux ainsi que pour le traitement, l'hébergement et la sauvegarde des données de leurs patients.

Un récent incident de cybersécurité ayant touché un prestataire informatique actif auprès de nombreux cabinets médicaux a mis en évidence les conséquences potentiellement importantes d'une défaillance de telles infrastructures. L'incident a notamment entraîné des interruptions d'accès aux logiciels et aux historiques de patients.

Il ressort par ailleurs des informations communiquées par l'Agence eSanté que celle-ci délivre des attestations de conformité aux logiciels connectés au Dossier de soins partagé (DSP), mais que ces attestations portent sur leurs échanges avec la plateforme nationale et ne couvrent pas l'infrastructure d'hébergement utilisée par les prestataires.

Au-delà de la sécurité technique se pose dès lors également la question de la transparence de toute la chaîne de sous-traitance. Un professionnel de santé confiant les données de ses patients à un prestataire informatique doit pouvoir connaître les garanties entourant leur hébergement et leur sauvegarde, y compris lorsque le prestataire fait lui-même appel à des fournisseurs de services cloud ou à d'autres sous-traitants.

Ces interrogations sont d'autant plus importantes que les données de santé présentent un caractère particulièrement sensible et que leur indisponibilité peut également avoir des conséquences directes sur la continuité de la prise en charge des patients.

Dans ce contexte, je souhaite poser les questions suivantes à Mesdames les ministres :

- Quelles autorités sont actuellement chargées de contrôler la sécurité, la résilience et les infrastructures d'hébergement des prestataires privés qui traitent, hébergent ou sauvegardent des données de santé pour le compte de médecins et d'autres professionnels de santé ?

Groupe parlementaire du LSAP
34, rue du Marché-aux-Herbes
L-1728 Luxembourg
Tél: (+352) 22 59 14-1
Fax: (+352) 22 59 14-82
lsap@chd.lu
lsap.lu

Existe-t-il des aspects de ces infrastructures qui ne font actuellement l'objet d'aucun contrôle préalable ou périodique par une autorité publique ?

- Ces prestataires sont-ils soumis, avant de pouvoir proposer de tels services aux professionnels de santé, à un agrément, une certification, une homologation ou un audit de sécurité obligatoire portant spécifiquement sur l'hébergement de données de santé ? Dans l'affirmative, quelle autorité délivre cet agrément ou cette certification, selon quels critères et avec quelle périodicité les contrôles sont-ils renouvelés ?

- Lorsqu'un prestataire fait lui-même appel à un sous-traitant ou à un fournisseur de services cloud pour héberger ou sauvegarder des données de santé, quelles obligations d'information lui incombent à l'égard du professionnel de santé concerné ? Celui-ci doit-il être informé de l'identité du sous-traitant, de la nature des données qui lui sont confiées ainsi que du lieu de leur hébergement ? Une autorisation préalable du professionnel de santé est-elle requise ?

- Quelles obligations s'appliquent lorsque des données de santé sont confiées à un fournisseur de services cloud, notamment en matière de localisation des données, chiffrement, contrôle des accès et transferts éventuels hors du Luxembourg ou de l'Union européenne ? Le fait que les données soient chiffrées modifie-t-il les obligations applicables en matière d'information, de sous-traitance ou de contrôle ?

- Les autorités compétentes disposent-elles actuellement d'une vue d'ensemble des prestataires et sous-traitants intervenant dans l'hébergement des données de santé au Luxembourg, comprenant notamment les fournisseurs cloud utilisés, la localisation des infrastructures principales et de sauvegarde ainsi que les éventuelles chaînes de sous-traitance ?

- Quelles exigences minimales sont actuellement imposées aux prestataires en matière de sauvegarde, redondance géographique, séparation des sauvegardes, restauration après incident et continuité des activités ? Existe-t-il notamment une obligation de garantir qu'une cyberattaque affectant l'infrastructure principale ne puisse simultanément compromettre les sauvegardes nécessaires à sa restauration ?

- Les professionnels de santé disposent-ils actuellement d'un registre, label ou autre moyen officiel leur permettant de vérifier, avant de confier les données de leurs patients à un prestataire, que celui-ci ainsi que son infrastructure d'hébergement répondent à un niveau de sécurité déterminé et régulièrement contrôlé ?

- Lorsqu'un prestataire proposant des services aux professionnels de santé fait état contractuellement ou commercialement d'un taux de disponibilité, d'une redondance de ses infrastructures ou d'une garantie de continuité de service, quelles dispositions permettent de garantir que ces indications correspondent effectivement aux services et données médicales confiés au prestataire et non uniquement à la disponibilité technique du centre de données ou de l'infrastructure sous-jacente ? Quelle autorité est compétente pour contrôler de telles affirmations ?

- Au vu des enseignements de l'incident récent, le Gouvernement considère-t-il le dispositif actuel suffisant ou envisage-t-il la création d'un régime spécifique d'agrément ou de certification des

Groupe parlementaire du LSAP
34, rue du Marché-aux-Herbes
L-1728 Luxembourg
Tél: (+352) 22 59 14-1
Fax: (+352) 22 59 14-82
lsap@chd.lu
lsap.lu

prestataires et hébergeurs de données de santé, assorti d'exigences minimales obligatoires, d'audits réguliers et d'une transparence sur les sous-traitants et infrastructures cloud utilisés ?

Veuillez croire, Monsieur le Président, en l'assurance de mon profond respect.



Liz Braz
Députée

Groupe parlementaire du LSAP
34, rue du Marché-aux-Herbes
L-1728 Luxembourg

Tél: (+352) 22 59 14-1
Fax: (+352) 22 59 14-82
lsap@chd.lu

lsap.lu