DS NEWSLETTER savoir faire
NEWSLETTER – INFORMATIONS JURIDIQUES PROPOSÉES PAR LE CABINET DS AVOCATS

Données de santé : apprivoisez vos risques !

ASIE

CONTEXTE

Ces dernières années, avec la mise en œuvre par le gouvernement chinois d'une série de politiques telles que « *Internet+ Santé* », les hôpitaux, les institutions médicales et même les fournisseurs d'équipements médicaux se sont progressivement numérisés. Cependant, si la numérisation des soins médicaux est pratique, elle augmente également le risque de fuite de données personnelles particulièrement sensibles pour les individus.

En effet, les données de santé peuvent être le dossier le plus complet contenant des données personnelles d'un individu. Elles peuvent inclure des données personnelles sensibles, telles que des informations relatives à l'état de santé physique ou mental passé, actuel et futur d'un individu, mais aussi d'autres informations fournies aux institutions médicales lors du parcours de soins , telles que des informations bancaires, le numéro de carte de crédit, etc. Une fois divulguées, ces informations peuvent non seulement avoir un impact négatif sur la vie privée des personnes concernées, mais également entraîner un préjudice matériel.

INTRODUCTION DE LA NORME SUR LES DONNÉES DE SANTÉ

Pour pallier ce risque, en 2021, la Chine a publié une série de lois, de règlements et de normes nationales sur les données personnelles.

Outre la loi sur la sécurité des données (« *DSL* ») et la loi sur la protection des informations personnelles (« *PIPL* »), une norme nationale jouant un rôle de guide pratique, « *Information Security Technology-Guide for Health Data Security* » (GB / T 39725-2020) est entrée en vigueur le 1er juillet 2021 (la « Norme »).

La PIPL consacre le statut de données sensibles des données de santé et fixe certaines exigences pour le traitement de ces données sensibles, mais sans entrer dans les détails. La Norme nationale précise ces exigences en tenant compte des différents scénarios et types de données.

Tout d'abord, la Norme définit les « *données de santé* » comme « *les données personnelles relatives à la santé et les données relatives à la santé traitées à partir des données personnelles relatives à la santé, y compris les résultats de l'analyse globale des groupes, les prévisions de tendances, les statistiques sur la prévention et le traitement des maladies, etc.* ».

- En outre, la Norme résume les mesures de sécurité recommandées pour les données personnelles dans des scénarios de soins de santé courants, notamment la coopération hospitalière, la télémédecine, la collecte de données, la gestion des données de capteurs, les applications mobiles, la recherche clinique, l'assurance, la maintenance à distance des dispositifs médicaux, etc. Quant aux mesures techniques recommandées, elles comprennent les mesures d'organisation interne, la classification des données, le contrôle des accès, la gestion des droits des utilisateurs, le contrôle du cryptage, la protection des équipements, la gestion de la sécurité des réseaux, la gestion de la coopération externe en matière de données, les conseils en matière de désidentification, etc.

- De plus, elle suggère la gestion des données de santé par classification, ce qui est conforme aux exigences de la PIPL, de la loi sur la sécurité des données (« *DSL* ») et de la loi sur la cybersécurité (« *CSL* ») concernant la gestion des données (personnelles).

Afin de différencier et d'affiner les exigences en matière de mesures de sécurité selon différents scénarios et données, la Norme classe les données de santé en six catégories :

1. les données d'identification personnelle (le nom, la carte d'identité, le numéro de téléphone, etc ;)
2. les données relatives à l'état de santé (antécédents médicaux, résultats de tests, etc ;)
3. les données relatives aux dossiers médicaux (dossiers médicaux des patients externes, dossiers d'admission, etc ;)
4. les données relatives aux paiements des frais médicaux (informations relatives aux paiements par l'assurance médicale, montant de la transaction, type d'assurance, etc ;)
5. les données sur les ressources du secteur de la santé (données de base sur les hôpitaux, données sur le fonctionnement des hôpitaux, etc) ; et,
6. les données de santé publique (données sur les épidémies de maladies infectieuses, données sur les naissances et les décès).

- En fonction de l'importance et du niveau de risque, la Norme classe les données de santé en cinq niveaux de risque : du niveau 1 au niveau 5, les exigences en matière de restrictions et de mesures de contrôle devenant progressivement plus strictes.

- En plus d'être conforme au droit supérieur en termes de système de gestion hiérarchique et classifié, cette Norme précise les droits des personnes concernées qui ont un droit d'accès (le droit d'interroger, de demander des copies), de rectification et d'ajout, et des droits de recherche rétrospective (la personne concernée a le droit d'effectuer une recherche rétrospective historique sur l'utilisation ou la divulgation des données par le responsable du traitement ou son sous-traitant, avec une période rétrospective minimale de six ans).

- Il convient de noter que cette Norme introduit un nouveau concept d' « *utilisateur des données* », qui n'apparaît pas dans la PIPL. L'utilisateur des données n'est ni le responsable du traitement, ni le sous-traitant, ni la personne concernée. L'utilisateur des données est mentionné dans certains scénarios d'utilisation de certaines données relatives à la santé (par exemple, pour les hôpitaux qui doivent effectuer un audit interne, l'auditeur serait considéré comme un utilisateur de données). Les obligations de l'utilisateur des données varient en fonction du scénario, ainsi que du type et du niveau des données qu'il utilise.

- En outre, en raison de la particularité du domaine de la santé, cette Norme définit également quatre situations dans lesquelles le responsable du traitement peut utiliser ou divulguer des données personnelles de santé sans le consentement spécifique de la personne concernée :

1. lorsque les données sont communiquées à la personne concernée elle-même ;
2. pour un traitement, un paiement ou des soins de santé ;
3. lorsque l'intérêt public est en jeu ou lorsque les lois et règlements l'exigent ;
4. lorsque des jeux de données limitées sont utilisés à des fins de recherche scientifique, d'éducation médicale ou sanitaire ou de santé publique. (Un jeu de données limitées fait référence à un ensemble de données personnelles sur la santé qui ont été partiellement tokénisées mais qui reconnaît et identifie l'individu correspondant et doit donc être protégé. Dans les cas ci-dessus, le responsable du traitement peut s'appuyer sur les exigences légales et réglementaires, l'éthique professionnelle, la déontologie et le jugement professionnel pour déterminer quelles données personnelles de santé peuvent être utilisées ou divulguées).

- Exportation des données : la Norme indique clairement que le responsable du traitement ne doit pas stocker les données de santé dans un serveur à l'étranger. L'exportation de données de santé personnelles en dehors de la Chine est possible (par exemple à des fins de recherche universitaire) mais sous réserve de certaines conditions (désidentification, approbation du comité de sécurité ou des services gouvernementaux compétents selon l'importance et le volume des données). Dans tous les cas, le consentement spécifique de la personne concernée est également nécessaire.

SUGGESTION

La PIPL n'étant pas suffisamment claire en ce qui concerne certaines exigences de conformité, du moins pour les données relatives à la santé, la Norme a « traduit » les obligations légales générales en lignes directrices détaillées, qui sont suffisamment pratiques pour que les responsables du traitement de données relatives à la santé, les sous-traitants et les utilisateurs de données puissent les suivre.
Nous recommandons aux professionnels de santé, aux institutions médicales et aux autres entités liées au secteur de la santé d'engager dès que possible une démarche de mise en conformité conformément aux exigences de la Norme.

Pour toute information complémentaire, merci de contacter :

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

Isabelle DOYON
Lawyer- Shanghai Office
DOYON@dsavocats.com