Kiteworks

Analyse 2024 des communications de contenu sensible dans le secteur de la santé : les tendances en matière de sécurité et de conformité

CHIFFRES CLÉS

Outils de communication utilisés	17%	Plus de 7
	16%	6
	20%	5
	24%	4
	11%	3
	7%	2
	1%	1
Échange de contenu sensible avec des tiers	14%	Plus de 5 000
	24%	2 500 à 4 999
	31%	1 000 à 2 499
	11%	500 à 999
	19%	Moins de 499
Types de données les plus préoccupantes (Top 3)	74%	PI
	58%	PHI
	37%	PII
	37%	Documents financiers
	35%	CUI et FCI
	21%	LLMs de GenAI
	21%	Échanges juridiques
	16%	Fusions & Acquisitions
Top 2 des priorités sur la confidentialité et la conformité	46%	RGPD
	41%	HIPAA
	37%	Lois des États américains
	26%	Lois propres à chaque pays
	24%	Exigences SEC
	17%	CMMC
	9%	PCI DSS
Top 2 des certificats de sécurité les plus importants	49%	ISO 27001, 27017, 27018
	39%	IRAP (Australie)
	36%	NIST 800-171/CMMC 2.0
	33%	SOC 2 Type II
	27%	FedRAMP Moderate
	16%	Directive NIS 2
Nombre de piratages des communications de contenu sensible	13%	Plus de 10
	14%	7 à 9
	14%	4 à 6
	36%	2 à 3
	14%	1
	9%	Ne sait pas

Le rapport Kiteworks 2024 sur la confidentialité et la conformité des communications de contenu sensible fournit une analyse détaillée des problématiques et des pratiques dans différents secteurs d'activité, et notamment dans la santé. Ce brief reprend les principales conclusions du rapport concernant le secteur de la santé ; outils utilisés pour échanger des données sensibles, problèmes de cybersécurité, risques dans les échanges avec des tiers, menaces spécifiques et conséquences sur la conformité règlementaire.

Gestion de tous les outils de communication de contenu sensible

53 % des établissements de santé utilisent au moins cinq outils de communication pour envoyer et partager des contenus sensibles, ce qui correspond à la moyenne de l'ensemble de la cohorte. 53 % d'entre eux déclarent pouvoir suivre et contrôler les données sensibles envoyées et partagées en interne, tandis que 44 % indiquent être en mesure de le faire lorsqu'elles sont échangées en externe. Ces deux chiffres sont légèrement supérieurs aux moyennes de 51 % et 43 % enregistrés pour l'ensemble des répondants.

La prévention des fuites de propriété intellectuelle et de secrets d'entreprise (61 %) et des sanctions pour non-conformité (56 %) sont les deux priorités citées en premier par les organismes de santé. Ces chiffres sont nettement supérieurs à la moyenne de l'ensemble des personnes interrogées (56 % et 48 %). Le renforcement des réglementations en matière de protection de la vie privée dans le secteur médical, telles que l'HIPAA, explique sans doute l'importance accordée à ces deux aspects. À l'instar des autres secteurs d'activité, les répondants du secteur de la santé ont peu cité (19 %) la nécessité d'éviter les effets néfastes sur l'image de marque.

Évaluer le risque tiers pour les contenus sensibles

La gestion des risques tiers est une préoccupation majeure des établissements de santé. 38 % d'entre eux échangent des contenus sensibles avec plus de 2 500 interlocuteurs (chiffre

inférieur à la moyenne mondiale de 44 %). Étonnamment, 69 % d'entre eux comptent plus de 1000 interlocuteurs dans leur supply chain (plus que la moyenne de 66 % pour l'ensemble des secteurs d'activité). 74 % des entreprises indiquent pouvoir suivre et contrôler plus des trois quarts des contenus sensibles lorsqu'ils quittent une application (suivi de près par 79 % des industriels). C'est le secteur le plus mature sur ce point.

Évaluer le niveau de conformité pour les contenus sensibles

90 % des établissements de santé ont indiqué que leur système de management de la conformité des communications sensibles nécessitait des améliorations plus ou moins importantes. Ce chiffre est légèrement supérieur à celui de l'ensemble des répondants : 88 %.

Les établissements de santé ont cité le RGPD en tête de leurs priorités (46 % en premier ou deuxième). L'HIPAA arrive en deuxième position, avec 41 % des organisations qui le citent parmi leurs priorités. Ce classement est tout à fait cohérent si l'on considère l'attention portée par les organismes gouvernementaux aux informations médicales protégées (PHI).

Pour ce qui est des certifications de sécurité, les normes ISO 27001, 27017 et 27018 sont citées dans 49 % des cas, et la norme IRAP dans 39 % des réponses, loin derrière. Ces chiffres sont alignés sur ceux de l'ensemble de la cohorte qui a répertorié les normes ISO 27001, 27017 et 27018 dans une proportion de 53 % et l'IRAP à 33 %.

Évaluer les risques liés à la sécurité des contenus sensibles

91 % des établissements de santé déclarent que leur management des risques associés aux communications sensibles doit être amélioré de manière significative ou partielle (résultat identique à l'ensemble de la cohorte).

41 % des établissements de santé ont indiqué avoir subi au moins quatre violations de leur contenu sensible (27 % déclarent en avoir subi plus de sept). Ces chiffres sont inférieurs à ceux des autres secteurs, où 32 % ont admis avoir subi au moins 7 violations de données et 55 % au moins quatre. En outre, près d'un répondant sur dix (9 %) issu de la santé admet ne pas connaître avec certitude le nombre de violations de données subies par son organisation.

Les outils de sécurité avancés (chiffrement, authentification multifactorielle, suivi et contrôle de la gouvernance) ne sont utilisés que partiellement dans 44 % des établissements de santé, soit 3 points au-dessus des 41 % pour l'ensemble de la cohorte. 39 % admettent en utiliser quelques-uns et 2 % n'en utiliser aucun.

Évaluer le coût de la sécurité et de la conformité

Du point de vue financier, 38 % des établissements de santé interrogés ont déclaré avoir dépensé plus de 3 millions de dollars par an en frais de contentieux. Ce chiffre est inférieur à la moyenne mondiale, où 45 % des personnes interrogées ont admis être à plus de 3 millions de dollars. Un grand nombre de répondants du secteur de la santé (13 %) ont déclaré ne pas savoir combien leur organisation dépense annuellement en frais de contentieux, ce qui est supérieur aux 9 % de l'ensemble de la cohorte.

Connaissance et classification des types de données

65 % des établissements de santé ont indiqué étiqueter et classer plus des trois quarts des données non structurées, ce qui est nettement mieux que l'ensemble des répondants (58 %). Cela peut s'expliquer par le fait que les données médicales sont plus sensibles dans le secteur de la santé. Paradoxalement, seuls 26 % des répondants du secteur de la santé ont déclaré que plus de 80 % des données non structurées devaient être étiquetées et classifiées (et 54 % plus de 60 %).

Urgence absolue à protéger les contenus sensibles dans le secteur de la santé

Le rapport Kiteworks 2024 souligne l'importance de la gestion des risques et de la conformité pour les communications de contenu sensible dans les établissements de santé. Étonnamment, la propriété intellectuelle (PI) a été citée comme le type de données le plus exposé (74 %), devant les informations médicales protégées (PHI) à 58 %.

En pratique, ils passent beaucoup de temps à compiler les journaux d'audit générés par les nombreux outils de communication de contenus sensibles. 58 % des répondants doivent en réconcilier plus de 11 (contre 48 % en moyenne), et 6 % ne savent même pas combien il y en a. Cela représente un engorgement considérable : 11 % des personnes interrogées y consacrent au moins 2 500 heures par an, 19 % plus de 2 000 heures, et 64 % plus de 1500 heures.

Accéder au rapport complet