Kiteworks

2024 Analysis of Sensitive Content Communications in Healthcare: Security and Compliance Trends

HIGHLIGHTS

Communication Tools in Place	17%	7+
	16%	6
	20%	5
	24%	4
	11%	3
	7%	2
	1%	1
Exchange Sensitive Content With Third Parties	14%	Over 5,000
	24%	2,500 to 4,999
	31%	1,000 to 2,499
	11%	500 to 999
	19%	Less Than 499
Data Types Biggest Concern (Top 3)	74%	IP
	58%	PHI
	37%	PII
	37%	Financial Documents
	35%	CUI and FCI
	21%	GenAI LLMs
	21%	Legal Communications
	16%	M&A
Biggest Privacy and Compliance Focus (Top 2)	46%	GDPR
	41%	HIPAA
	37%	U.S. State Privacy Laws
	26%	Country-specific Data Privacy Laws
	24%	SEC Requirements
	17%	CMMC
	9%	PCI DSS
Most Important Security Validations (Top 2)	49%	ISO 27001, 27017, 27018
	39%	IRAP (Australia)
	36%	NIST 800-171/CMMC 2.0
	33%	SOC 2 Type II
	27%	FedRAMP Moderate
	16%	NIS 2 Directive
Number of Times Experienced Sensitive Content Communications Hack	13%	10+
	14%	7 to 9
	14%	4 to 6
	36%	2 to 3
	14%	1
	9%	Don't Know

The 2024 Kiteworks Sensitive Content Communications Privacy and Compliance Report provides an in-depth analysis of the challenges and trends in managing sensitive content across various industry sectors, including healthcare. This brief focuses on the key findings related to healthcare, highlighting the tools used for sensitive content communications, cybersecurity concerns, third-party communication risks, specific cyber threats, and compliance implications.

Managing All the Sensitive Content Communications Tools

53% of healthcare organizations rely on five or more communication tools to send and share sensitive content, which is the same as the full cohort average. When it comes to tracking and controlling sensitive content, 53% of healthcare organizations said they can track and control sensitive data sent and shared internally, whereas 44% indicated they can do so when it is exchanged externally. Both are slightly better than the full respondent averages of 51% and 43%, respectively.

When it comes to sensitive content communications privacy and compliance priorities, preventing leakage of confidential IP and corporate secrets and avoidance of regulatory violations (fines and penalties) were the two top priorities for healthcare organizations—61% and 56%. These are significantly over the average of all respondents—56% and 48%. Increased enforcement of health privacy regulations such as HIPAA is likely the reason behind this higher emphasis in healthcare. Like most other industry segments, healthcare respondents marked avoidance of detrimental brand impact the least often (19%).

Assessing the Third-party Risk of Sensitive Content

Managing third-party risk is a critical challenge for healthcare organizations, with 38% reporting they exchange sensitive content with over 2,500 third parties (lower than the global cohort at 44%). An astounding 69% have over 1,000 third parties in their content supply chain (over the 66% average across all industries). When it comes to tracking and controlling sensitive content once it leaves an application, healthcare is one of the most mature industry sectors with 74% indicating they can track and control over three quarters of sensitive content when it leaves an application (closely behind 79% of manufacturers).

Assessing the State of Sensitive Content Compliance

90% of healthcare organizations revealed their measurement and management of compliance for sensitive content communications requires some to significant improvement. This is slightly more than what all respondents reported: 88%.

Healthcare firms cited GDPR as their biggest focus area over other data privacy and compliance regulations (46% ranked first or second). The second most-cited regulation was HIPAA at 41%. This one-two ranking makes full sense considering the scrutiny government bodies are paying to private health information (PHI).

When it comes to vetting and selecting security validations or certifications, healthcare firms had a relatively close bunching beyond ISO 27001, 27017, and 27018 being cited 49% of the time as their top or second-highest validation or certification. The second most-cited security validation was 10 percentage points behind at 39% (IRAP). These both align with the full cohort that listed ISO 27001, 27017, and 27018 at a 53% clip and IRAP at a 33% rate.

Assessing the Risk of Sensitive Content Security

91% of healthcare organizations indicate their measurement and management of security risk associated with sensitive content communications requires significant or some improvement (same as the global cross-industry result).

41% of healthcare organizations revealed their sensitive content was breached four or more times (27% said seven times or more). These are lower than the cross-industry cohort where 32% admitted to seven or more data breaches and 55% said they had four or more. In addition, nearly 1 out of 10 respondents (9%) in healthcare said they were not certain how many data breaches their organizations experienced.

Advanced security capabilities and practices such as encryption, multi-factor authentication, and governance tracking and control are only used for some sensitive content by healthcare organizations 44% of the time (three percentage points above the 41% by all respondents—39% admitted to some and 2% said none).

Assessing the Cost of Security and Compliance

When it comes to litigation costs, the survey found 38% of healthcare respondents indicated they spend over $3 million annually. This is below the global average where 45% admitted their litigation costs were over $3 million. A large number (13%) of healthcare respondents (13%) said they do not know how much their organizations spend on litigation costs annually, which is above the 9% in the full cohort.

Knowledge and Categorization of Data Types

65% of healthcare organizations indicated they tag and classify over three-quarters of unstructured data; this is dramatically better than the full number of respondents where 58% admitted the same. This higher rate of tagging and classification may be the result of the greater sensitivities around sensitive data in healthcare. Ironically, only 26% of healthcare respondents said only 80% or more of unstructured data needs to be tagged and classified (or 54% who said 60% or more needs to be tagged and classified).

Imperative for Robust Sensitive Content Management in Healthcare

The Kiteworks 2024 Sensitive Content Communications Report highlights the critical need for robust management of risk and compliance in sensitive content communications in healthcare organizations. Surprisingly, intellectual property (IP)—versus protected health information (PHI) at 58%—was cited as the data type posing the greatest risk by respondents (74%).

Operationally, healthcare firms spend a lot of time managing logs generated by the numerous communication tools they use to share and send sensitive content. 58% of respondents must reconcile over 11 (compared to the 48% average of all respondents), and 6% of respondents did not even know how many must be reconciled. This compiles into a huge report logjam; 11% spend 2,500 hours or more annually and another 19% spend over 2,000 hours. 64% spend over 1,500 hours annually.

Get Full Report

Kiteworks