Kiteworks

Healthcare: 2023 Sensitive Content Communications Privacy and Compliance

Industry Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	**24%**	7+
	46%	6
	20.5%	5
	9.5%	Less than 4
Average Annual Budget for Communication Tools	**20.5%**	$500,000+
	24%	$350,000 – $499,999
	46%	$250,000 – $349,999
	9.5%	$150,000 – $249,999
Number of Third Parties With Which They Exchange Sensitive Content	**14.5%**	5,000+
	41.5%	2,500 – 4,999
	38%	1,000 – 2,499
	6%	499 - 999
Attack Vector Weighted Score (based on ranking)	**100**	Password/Credential Attacks
	96	Denial of Service
	94	Cross-site Scripting
	84	DNS Tunneling
	78	Session Hijacking
	72	Rootkits
	72	Zero-day Exploits and Attacks
	62	URL Manipulation
	52	SQL Injection
	48	Malware (ransomware, trojans, etc.)
	46	Man in the Middle
	43	Phishing
	35	Insider Threats
Exploits of Sensitive Content Communications in Past Year	**17.5%**	10+
	38.5%	7 – 9
	43%	4 – 6
	1.5%	Fewer than 3
Level of Satisfaction With 3rd-party Communication Risk Management	**5%**	Requires a New Approach
	33%	Significant Improvement Needed
	46%	Some Improvement Needed
	16%	Minor Improvement Needed

Bad Actors Targeting Healthcare Because of the Money

Industry reports place healthcare as one of the top industry sectors targeted by rogue nation-states and cybercriminals. Research by Check Point Software found that cyberattacks on healthcare organizations increased 22% from Q1 2022 to Q1 2023.[1] One of the reasons for this increase is the fact that there is "*gold in them healthcare hills*." Certainly, the fact that healthcare organizations send, share, and store large volumes of personally identifiable information (PII) and highly sensitive protected health information (PHI) is a key factor. It should come as no surprise then that the annual "Cost of a Data Breach Report" by IBM and Ponemon Institute has listed healthcare 12 consecutive years as the industry with the highest average cost of a breach—hitting $10.10 million last year.[2]

Too Many Disaggregated Communication Tools

Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report found healthcare organizations struggle to manage file and email data communication risks—both inside their organizations and with third parties. One of the reasons is the large number of systems healthcare organizations use to send and share private data. Nearly 7 out of 10 healthcare organizations have six or more sensitive content communication systems in place, more than any other industry sector.

Ranking Third-party Content Communications Risk

Healthcare organizations were asked to rank the risk of their different communication channels, and email and web forms tied with the most number one ranks (20.5%). When ranks one and two are factored into the equation, email received the most listings (39.5%). One of the ways email poses risk is related to challenges with encryption: when recipients cannot decrypt an email because it was encrypted in a format not supported by their organization. Here, healthcare respondents said they ask the sender to resend the file(s) unencrypted in an unpublished shared drive link. Beyond email, file sharing and web forms tied with the second-highest risk assessment based on rank one and two. Governance plays an important role here: One-third only track and control access to sensitive content folders for certain content types. Another 28.5% only do so for certain departments.

Email and web forms tied for highest risk of all communication channels (aggregation of rank one and two).

Nearly 70% of healthcare organizations have 6+ sensitive content communication systems in place.

Almost 4 in 10 healthcare organizations said a new approach or significant improvement is needed to their third-party content communications.

Risk management of third-party content communications is seen as a problem across industry sectors, and healthcare is at the top of the list. 38% of respondents said they require a new approach or their current approach requires significant improvement. Another 46% indicated some improvement is needed. Survey responses corroborate concerns around risk: 98.5% of healthcare organizations experienced four or more exploits of sensitive content communications in the past year.

Better Digital Risk Management Required

Lack of robust digital rights management is a big part of the problem, though weaknesses across healthcare organizations are not the same. For example, 41.5% of respondents said they have administrative policies in place for tracking and controlling content collaborating and sharing on-premises but not in the cloud. However, at the same time, 28.5% said the opposite—namely, they have tracking and controls in place for the cloud but not on-premises. Slightly more than one-third have both the cloud and on-premises covered.

Kiteworks and Healthcare

The Kiteworks Private Content Network employs a content-defined zero-trust approach that enables healthcare organizations to unify, track, control, and secure all their sensitive content communications in one platform. Healthcare organizations can track and control access to files and folders, who can edit and share them, and to whom and where they can be shared. Centralized policy management and digital rights management that includes capabilities such as SafeVIEW and SafeEDIT deliver comprehensive governance of file and email data communications—which is particularly critical in an era of compliance.

[1] "Global Cyberattacks Continue to Rise with Africa and APAC Suffering the Most," Check Point Research, April 27, 2023.

[2] "Cost of a Data Breach Report 2022," IBM and Ponemon Institute, July 2022.

Get the Full Report

Kiteworks

Kiteworks 2023 Sensitive Content Communications Privacy and Compliance Report

Seeking to empower private and public sector organizations to manage their file and email data communication risks better, Kiteworks began publishing an annual Sensitive Content Communications Privacy and Compliance Report in 2022. Rogue nation-states and cybercriminals recognize the value of sensitive content and target the communication channels used to send, share, receive, and store it—email, file sharing, managed file transfer, web forms, APIs, and more.

The 2023 Sensitive Content Communications Privacy and Compliance Report surveyed 781 IT, security, risk, and compliance professionals across numerous industries and 15 different countries. The in-depth report, which is based on their survey responses, explores a range of issues related to file and email data communication risks—how organizations are addressing those today and plan to do so in the coming year. The analysis includes a look back to 2022 data and what changes were observed in 2023.