Kiteworks

Pharmaceuticals/Life Sciences: 2023 Sensitive Content Communications Privacy and Compliance

Industry Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	**28.5%**	7+
	35.5%	6
	25.5%	5
	10%	Less than 4
Average Annual Budget for Communication Tools	**28.5%**	$500,000+
	18.5%	$350,000 – $499,999
	34.5%	$250,000 – $349,999
	17%	$150,000 – $249,999
Number of Third Parties With Which They Exchange Sensitive Content	**17%**	5,000+
	35.5%	2,500 – 4,999
	35.5%	1,000 – 2,499
	8.5%	499 - 999
Attack Vector Weighted Score (based on ranking)	**100**	Rootkits
	95	Password/ Credential Attacks
	94	DNS Tunneling
	90	URL Manipulation
	81	Denial of Service
	76	Phishing
	75	Zero-day Exploits and Attacks
	70	Malware (ransomware, trojans, etc.)
	68	SQL Injection
	65	Man in the Middle
	59	Session Hijacking
	48	Cross-site Scripting
	24	Insider Threats
Exploits of Sensitive Content Communications in Past Year	**15.5%**	10+
	31.5%	7 – 9
	43%	4 – 6
	10.5%	Fewer than 3
Level of Satisfaction With 3rd-party Communication Risk Management	**14%**	Requires a New Approach
	30%	Significant Improvement Needed
	32%	Some Improvement Needed
	24%	Minor Improvement Needed

Cyber Risk in the Pharmaceutical and Life Sciences Sector

With patient information, patented drugs, clinical trials, research projects, and technological advancements stored within their systems, the pharmaceutical and life sciences industry faces significant cyber risks. The rapid pace of technological advancements, increased reliance on automation tools, and engagement with third-party vendors further compound these challenges. It is noteworthy that the average cost of a breach in the pharmaceutical sector is approximately $5.3 million, which is 1.3 times higher than the average across other industries.[1] Sensitive file and email data communications in pharmaceutical and life sciences are a prime target for rogue nation-states and cybercriminals. It includes personally identifiable information (PII), intellectual property (IP), financial documents, clinical trial data, genomic data, and more.

Inefficiencies and Risks With Numerous Communication Tools

Respondents in Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report revealed that they utilize various communication channels to exchange sensitive content. 28.5% of them used more than 7 communication tools while only 10% used 10 or fewer. 28.5% of respondents indicated their organizations spent more than $500,000 on these tools, the highest of any industry.

Over 90% of pharmaceutical and life sciences firms exchange sensitive content with third parties on a regular basis.

Ranking Third-party Content Communications Risk

The management of third-party risk is a crucial aspect for pharmaceutical companies, as they regularly share critical information externally through a variety of communication channels. These channels enable the exchange of vital data with partners, vendors, research organizations, and other stakeholders. This process introduces a level of vulnerability, where sensitive information is exposed to potential risks beyond the company's direct control.

Implementation of digital rights management to limit access to and usage of sensitive content is tied as the number one priority for content sharing and collaboration.

Email is ranked with the highest risk by survey respondents, receiving a total of 40% of combined #1 and #2 rankings. Web forms comes up second with 28% of respondents listing it as their #1 or #2 rankings. Like most other industry sectors in the report, pharmaceutical and life sciences companies revealed they need either a completely new approach or significant improvement in their sensitive content communication risk management (44%).

Better Digital Risk Management Required

When asked to rank their top priorities regarding sensitive third-party content communications, respondents highlighted key areas of focus. The highest number of top rankings, at 18.5%, was given to tracking content permissions, expiration, locking, and versioning. This signifies the importance placed on effectively managing and controlling access to sensitive content throughout its life cycle. Following closely, at 15.7%, was automating the protection of content at rest from malicious threats. This underscores the need to implement robust security measures, including encryption, to safeguard sensitive information when it is received and stored. In third place, at 14.3%, is protection of content in motion from malicious threats.

Given the extensive reliance on third parties for crucial activities, such as R&D, clinical research, warehousing, logistics, and freight forwarding, the supply chain becomes a potential source of risk. Specifically, the absence of governance controls for confidential data can expose sensitive content communications to malicious actors. Here, only 31.5% of respondents have administrative policies for tracking and controlling sensitive content collaboration and communications on-premises and across the cloud.

Kiteworks and Pharmaceuticals and Life Sciences

Pharmaceutical and life sciences companies often collaborate on drug discovery projects, which require the sharing of sensitive information such as chemical structures, biological data, and experimental results. Kiteworks enables the safe sharing and collaboration of this information, ensuring the protection of IP and compliance with data privacy regulations. Kiteworks' encryption, access controls, and audit logging capabilities help maintain the security and integrity of drug discovery project data during the collaboration process. Kiteworks facilitates the safe sharing of this sensitive information, ensuring the protection of patient privacy and compliance with data privacy regulations, such as HIPAA and GDPR.

Another significant use case for Kiteworks in pharmaceutical and life sciences firms is in the distribution of product labeling and packaging materials. Pharmaceutical and life sciences companies often need to distribute these materials to internal teams, external partners, or regulatory agencies. Kiteworks facilitates the safe distribution of these materials, ensuring the protection of intellectual property and compliance with industry regulations. These companies often need to share sensitive protected health information (PHI), such as medical records, genomic data, or clinical trial participant information, with internal teams or external partners. Kiteworks enables the safe sharing of this sensitive information, ensuring compliance with data privacy regulations such as HIPAA and GDPR.

[1] "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.