Kiteworks

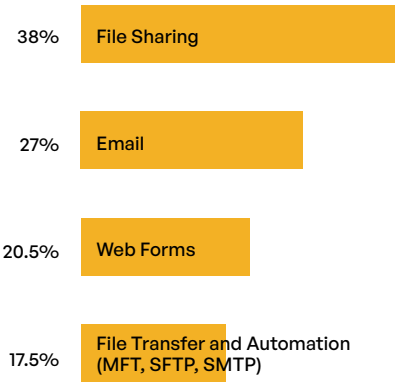
Sensitive Content Communications Privacy and Compliance in Pharmaceuticals

Highlights From Kiteworks' "2022 Sensitive Content Communications Privacy and Compliance" Report

PHARMACEUTICALS BRIEF

Proprietary information is the lifeblood of pharmaceutical companies. Development of a typical drug with a life of around 10 years costs around $2.6 billion.[1] Some of the largest data repositories exist in the pharmaceutical industry. In addition to intellectual property that includes pharmaceutical formulas, DNA, manufacturing plans, trial designs, and more, pharmaceutical companies must protect protected health information (PHI) of patients, personally identifiable information (PII) of their employees and customers, and the sharing of confidential information with biotech companies.

What Sensitive Content Communications Channel Poses the Greatest Risk?



Cybercriminals recognize this is the case and are targeting them in greater numbers. In a study of data breaches and leakage in the pharmaceutical industry between 2018 and 2021, Constella Intelligence found that 59% of total breaches and 76% of total exposures occurred since 2020. And while proprietary IP-related data certainly was a target, PII data, such as email, password, name, phone number, and date of birth, was in nearly two-thirds of instances. Indeed, 58% of pharmaceutical executives had their credentials exposed during this four-year time frame.[2] The cost of an average data breach in pharmaceuticals last year was $5.72 million.[3]

Security and Compliance Governance

Pharmaceutical companies share critical information internally and externally via various communication channels. Following are some of the more prevalent use cases:

- Protecting drug formulas, scheduling, manufacturing plans, trial designs, and DNA sequences
- Applying audit and privacy controls such as Health Insurance Portability and Accountability Act (HIPAA) to clinical trial data scheduled with contract research organizations (CROs) and physicians

- Ensuring immutable transfers of manufacturing quality data to comply with Federal Drug Administration (FDA) 21 CFR Part 11 and Governors and good practice guidelines (GxP)
- Transferring securely DNA genome sequences and other large data sets—internally as well as externally with different third parties involved in the supply chain
- Automating securely data transfers with manufacturing plants, CROs, and regulators
- Enabling governed and controlled sharing of confidential dossiers between the pharmaceutical company and biotech companies

These different activities are governed by various compliance standards that cover areas such as personally identifiable information (PII), protected health information (PHI), security foreign corruption and bribery, and securities. Privacy regulations, such as HIPAA, General Data Protection Regulation (GDPR), PIPEDA, and the California Consumer Privacy Act (CCPA), govern PHI and PII, whereas other regulations are more industry specific, such as FDA CFR and Process Analytical Technology (PAT). And as big data becomes increasingly more important in the pharmaceutical sector, tracking and controlling that data grows accordingly. For those organizations found to be in noncompliance, the cost can be dramatic—around 2.71 times more than the cost of compliance.[4]

Private PHI Communications With Third Parties

In addition to all data that is shared internally, pharmaceutical companies must exchange a lot of sensitive data with third parties—CROs, physicians, supply chain providers, biotech companies, and others. Depending on the regulation or standard, policies are specified around data type, user and device access, data classification, cataloguing, expiration, and audit trail reporting.

In response, pharmaceutical firms must have the right governance tracking and controls in place to ensure privacy and compliance—for both data at rest and in motion. As pharmaceutical companies rely on a vast network of third parties for activities such as research and development (R&D), clinical research, warehousing and logistics, and freight forwarding, their supply chain often poses a significant risk; in particular, confidential data lacking encryption and governance controls can be exposed to malicious third-party actors.

One of the biggest challenges involves the sharing and transfer of data with third parties. The following graphic examines some of the pharmaceutical industry findings.

What Are Your Top Concerns in Managing Sensitive Content Communications?

What Are Your Top Priorities Around Third-party Sensitive Content Communications?

Governance, Risk, and Compliance Survey Findings

Based on findings from a survey conducted by Kiteworks and Survey Pacific in early 2022, 3 in 10 pharmaceutical companies indicate their organizational governance and protection of sensitive content communications either requires a new approach or needs significant improvement (another 38% indicate some improvement is needed).[5] A likely reason is the lack of technologies and processes to measure risk: Fewer than half (49%) have technologies and processes in place to do so.

Almost half (49%) of respondents believe their organizations are well-protected when it comes to third-party risk. Communications in the cloud is a problem for many pharmaceutical firms: 44.5% either do not manage and monitor sensitive content shares and transfers in the cloud or only manage and monitor some of them. However, despite all the time and resources spent on compliance, 17.5% of pharmaceutical respondents lack confidence in the accuracy of their compliance reports.

Governance

62%

use 4 or more systems for tracking, controlling, and securing sensitive data communications with third parties.

30%

believe their governance and protection of third-party content communications either requires a new approach or requires significant improvement (another 38% say some improvement is needed)

49%

have technologies and processes in place to measure risk associated with third-party content communications (the remaining 51% plan to do so)

Risk Management

36.5%

use antivirus and antispam technologies to verify incoming data communications from third parties

44.5%

use DLP for file sharing and file transfer with third parties

58.5%

encrypt 75% or more of their content communications with third parties

37%

indicate their risk management and security of third-party content communications requires a new approach or significant improvement

46%

believe their organization is not well-protected against third-party content communication risks

44%

either do not or only manage and monitor some content communications in the cloud

Compliance

52%

must generate over 7 compliance reports annually

55.5%

spend over 40 hours generating each compliance report (25.5% spend 80-plus hours)

17.5%

feel their compliance reports are fully accurate with 59% saying they are mostly accurate (not contain errors)

Kiteworks Private Content Network Provides Governance, Compliance, and Security

Kiteworks enables pharmaceutical companies to create a dedicated Private Content Network (PCN) of internal and external digital communications that ensures privacy and compliance of sensitive content—ranging from PHI and PII to proprietary IP-related content. The COVID-19 pandemic heightened awareness around the pharmaceutical industry and the importance of tracking and controlling the latter. And when data breaches do occur, the cost can be dramatic. Cybercriminals and nation-states are targeting pharmaceutical data. According to IBM and Ponemon Institute, breach costs for pharmaceutical firms average around $5.06 million per breach.[6]

Kiteworks enables pharmaceutical organizations to protect critical IP related to manufacturing drug formulas, clinical trials, and production schedules. PII and PHI that pharmaceutical firms share with their supply chain, CSRs, physicians, and other third parties can be hacked in transit and in motion. Unifying, tracking, controlling, and securing this sensitive content with the Kiteworks platform creates a PCN for pharmaceutical companies that is fully secure and compliant with various standards and regulations.

For these and other highlights from Kiteworks' "2022 Sensitive Content Communications Privacy and Compliance" report, download a copy.

References

[1] Thomas Sullivan, "A Tough Road: Cost To Develop One New Drug Is $2.6 Billion; Approval Rate for Drugs Entering Clinical Development Is Less Than 12%," Policy & Medicine, March 21, 2019.

[2] "Pharma Sector Exposures Report: 2018-2021 Digital Risk Findings and Trends," Constella Intelligence, January 26, 2022.

[3] "Cost of a Data Breach Report 2021," IBM and Ponemon Institute, July 2021.

[4] "The True Cost of Compliance With Data Protection Regulations: Benchmark Study of Multinational Organizations," Ponemon Institute, December 2017.

[5] "2022 Sensitive Content Communications Privacy and Compliance Report," Kiteworks, April 13, 2022.

[6] "Cost of a Data Breach Report 2021," IBM and Ponemon Institute, 2021.

Kiteworks