Kiteworks

Sensitive Content Communications Privacy and Compliance in Healthcare

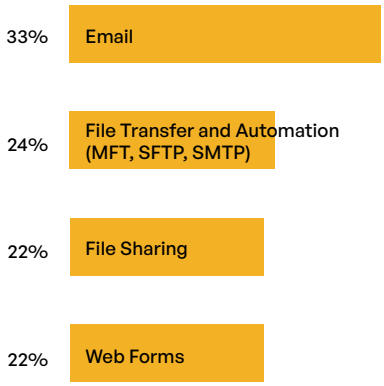
Highlights From Kiteworks' "Sensitive Content Communications Privacy and Compliance" Report

HEALTHCARE BRIEF

When it comes to protected health information (PHI) in the healthcare industry, governmental bodies have gone to great lengths to ensure it is protected. How PHI of patients—and for that matter personally identifiable information (PII) for staff—is protected is crucial for healthcare organizations. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S., Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, and General Data Protection Regulation (GDPR) in the EU mandate that healthcare providers must demonstrate that they have the right compliance tracking and controls in place.

Healthcare PHI is in the crosshairs of cybercriminals. Breaches of PHI last year hit an all-time high, impacting 45 million patients—triple from what it was three years before.[1] Nearly three-quarters of healthcare organizations indicate the cause of data breaches is related to hacking and IT incidents. Hospitals account for around 30% of all large data breaches in the U.S.[2] Healthcare industry cybersecurity professionals resoundingly report (92%) an increase in cyber risk over the past year.[3]

What Sensitive Content Communications Channel Poses the Greatest Risk?



Security and Compliance Governance

Healthcare organizations share and transfer sensitive information in various ways. Following are a few of the more prevalent use cases:

- Sharing of PHI to regulators, insurers, and healthcare providers in compliance with privacy requirements
- Enabling home healthcare technicians to create and annotate PHI on mobile devices
- Automate statement delivery to patients, insurers, and regulators
- Automate medical and facilities supply chain communications
- Automate provider electronic health record (EHR) communications with service providers like pharmaceutical centers
- Access and share PHI-related medical records online with real-time diagnosis

These activities must be strictly governed by security and compliance standards. Privacy regulations, such as HIPAA, GDPR, PIPEDA, and the California Consumer Privacy Act (CCPA), control how PHI and PII are captured, shared, used, and stored. As healthcare organizations share and transfer PHI data, they must ensure that it is done so per different privacy and compliance controls. Governance and security requirements cover both managed file transfers as well as manual file sharing and transfers.

Private PHI Communications With Third Parties

Management of third-party risk as it relates to privacy, compliance, and security is a critical requirement for healthcare organizations—hospitals, healthcare clinics, laboratories and diagnostic clinics, and nursing and assisted living facilities. Data regulations specify the need for policies around user, data, and device access, data classification and cataloguing, data expiration, and audit trail reporting.

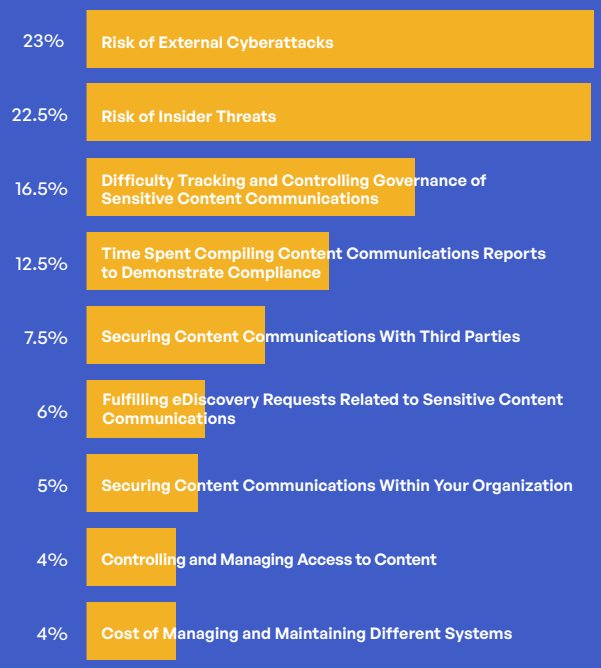
In response, healthcare organizations must have the right governance tracking and controls in place to ensure privacy and compliance—for both data at rest and in motion. This remains a challenge for many healthcare firms per a survey of global IT, security, privacy, and compliance professionals in early 2022. One of the biggest challenges involves the sharing and transfer of data with third parties. The below analysis examines only findings from those in the healthcare industry sector.

Governance, Risk, and Compliance Survey Findings

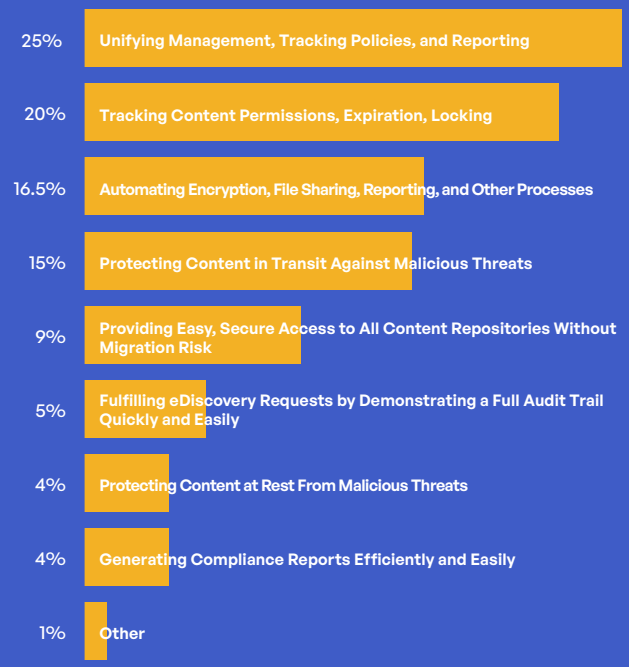
Based on findings from a survey conducted by Kiteworks and Survey Pacific in early 2022, more than 4 in 10 (42%) healthcare firms indicate their organizational governance and protection of sensitive content communications either require a new approach or need significant improvement (highest of all industries).[4] A likely reason is the lack of technologies and processes to measure risk: Only 37% have technologies and processes in place to do so.

Fewer than half of respondents believe their organizations are well-protected when it comes to third-party risk. Communications in the cloud is a problem for many healthcare firms: 45% 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, almost 20% of healthcare respondents lack confidence in the accuracy of their compliance reports.

What Are Your Top Concerns in Managing Sensitive Content Communications?



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



Governance

62%

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

42%

believe their governance and protection of third-party content communications either requires a new approach or requires significant improvement (another 14% say some improvement is needed)

35%

have technologies and processes in place to measure risk associated with third-party content communications (64% plan to do so)

Risk Management

49%

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

39%

use DLP for file sharing and file transfer with third parties (lower than all-industry average)

51.5%

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

45.5%

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

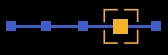
Compliance

58%

must generate over 7 compliance reports annually

51.5%

spend over 40 hours generating each compliance report (35% spend 80-plus hours)



Only 20%

feel their compliance reports are fully accurate with 19% indicating they are only somewhat accurate or inaccurate in various places

Kiteworks Private Content Network Provides Governance, Compliance, and Security

Kiteworks enables healthcare firms to create a dedicated Private Content Network (PCN) of internal and external digital communications that ensures privacy and compliance of sensitive PHI and PII. Cybercriminals and nation-states are targeting healthcare data. According to IBM and Ponemon Institute, breach costs for healthcare organizations increased 29.5% in 2021 over the prior year—with an average cost of $9.23 million per data breach (the highest of any industry).[5]

Kiteworks helps healthcare organizations to protect PHI shared with and transmitted to regulators, insurers, and providers. Its PCN also enables healthcare firms to demonstrate compliance with sensitive PHI governed by regulations such as HIPAA, PIPEDA, GDPR, and others as they mobilize care and optimize back office and supply chain operations. Unifying, tracking, controlling, and securing PHI and other sensitive content communications with the Kiteworks platform delivers healthcare organizations with a single pane of glass for sharing and transferring sensitive patient information that is fully secure and compliant with regulations.

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

References

[1] Heather Landi, "Healthcare data breaches hit all-time high in 2021, impacting 45M people," FIERCE Healthcare, February 1, 2022.

[2] "Healthcare Data Breach Trend Report 2021," Protected Harbor, March 10, 2022.

[3] "Healthcare Clients and Consumers Grade Cybersecurity Software Services, Black Book Industry 2022 Survey," Black Book Research, January 4, 2022.

[4] "2022 Sensitive Content Communications Privacy and Compliance Report," Kiteworks, April 13, 2022.

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

Kiteworks