

Insights on Data Types and Classification and Risk Management

Highlights From Kiteworks 2024 Sensitive Content Communications Privacy and Compliance Report

PREMISE

Unstructured Data That Is Not Tagged and Classified Can Pose Serious Risk

51% of Organizations Tag and Classify Less Than Half Their Unstructured Data

Healthcare is the most mature industry sector, with 65% tagging and classifying three-quarters of unstructured data

Americas are doing the best regionally

56% tag and classify more than three-quarters of their unstructured data

Not All Unstructured Data Must Be Tagged and Classified

40% of organizations said 60% or more of unstructured data needs to be tagged and classified

Largest organizations have more stringent unstructured data tagging and classification requirements:

15% of those with 30,001 employees say they tag and classify 100% of their unstructured data and another 20% say over 80% must be tagged and classified

Federal government has the highest tagging and classification requirements:

24% said all unstructured data must be tagged and classified and 17% say 80% or more

Data types posing the biggest risk and concern include:

55%

Financial Documents

44%

IP

44%

Legal Communications

40%

GenAI LLMs

Top Data Type Risk in Select Industry Sectors

50% of security and defense firms and energy and utility organizations list GenAI LLMs the most often

58% of healthcare organizations cited PHI

79% of manufacturers listed CUI and FCI

40% of pharmaceuticals and life sciences firms listed merger and acquisition (M&A) data

How Kiteworks Helps Tag and Classify Unstructured Data and Mitigate Risks



The Kiteworks Private Content Network (PCN) provides a comprehensive platform for managing sensitive data, including the ability to tag and classify data

Administrators can set specific rules and permissions for different data types entering the Kiteworks platform

Content-based risk policy applies the appropriate rights best suited to manage cyber risk using the NIST Cybersecurity Framework (CSF) 2.0

Content policies based on the data class risk profile

Next-gen digital rights management (DRM) capabilities for file expiration and revocation rules based on content-based risk policies help organizations to comply with data retention and deletion requirements under various regulations

For all the findings contained in the 2024 Sensitive Content Communications Privacy and Compliance Report, [download](#) your copy today.