

Identifying Privacy Violations and Protecting Sensitive Data Using CommVault® Simpana® 9 Content Director

Highlights:

Simpana® 9 software Privacy Violation Management enables Compliance Officers, Security Officers, and Risk Managers to:

1. Schedule automated searches to identify data privacy violations
2. Identify various types of content including social security numbers, credit card data, and sensitive customer information
3. Tag any privacy violations and deliver a copy to the appropriate individual for review
4. Preserve a copy of the violation until appropriate action has been taken

Privacy Violation Management

CommVault® Simpana® software provides early warning of privacy violations by identifying and monitoring sensitive organizational data. Whether your business handles social security numbers, credit card data, or protected health information, Simpana software can easily detect, classify, and alert appropriate parties when internal privacy policies have been compromised.

Whether an organization is subject to third-party oversight or not, the protection of sensitive data is paramount in reducing overall corporate risk. For those businesses that are subject to data privacy mandates, the ability to identify data breaches quickly can result in significant cost savings. Simpana Content Director enables organizations to automatically identify data breaches and notify the Security Officer, Compliance Officer, Risk Manager, or General Counsel. Additionally, Content Director can be used to monitor violations over time to determine if process modifications or additional end user training is necessary to ensure compliance with data management policies.

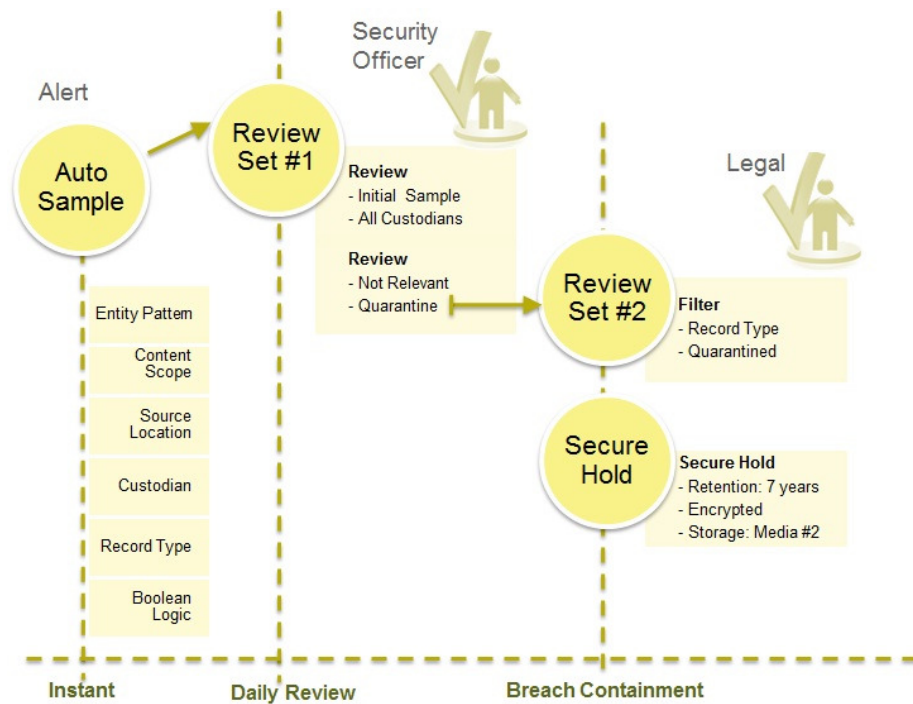


Figure 1: Sample Privacy Violation Workflow

- **Security/Compliance/Risk Management:** Issues data privacy policies including details regarding how sensitive information should be handled and stored.
- **IT:** IT develops a set of Content Director policies enabling CommVault software to identify data privacy violations. These policies can be comprised of any combination of content and metadata including social security numbers, credit card data, etc.
- **Security/Compliance/Risk Management/Legal:** Violations are classified and delivered to the appropriate individual which may include a Security Officer, Compliance Officer, Risk Manager, or General Counsel. The data can be reviewed to determine the nature and extent of the violation and appropriate action can then be taken.
- **IT:** Over time, IT can monitor the occurrence of violations and can recommend whether policy adjustments or additional end user training is necessary.

SIMPANA
SOLVES
privacy mgmt
 and the rest of your
 data and information
 management challenges.

Key Capabilities and Benefits

Capabilities	Benefits
Automated Privacy Violation Detection and Alerting	Policy-based privacy standards can be used to identify the mishandling of information including social security numbers, credit card data, protected health information, and sensitive customer data.
Out-of-the-Box, Role-Based Workflow	Enables privacy violation breaches to be identified and sent to the appropriate internal resource for review.
Automated Classification & Preservation	Provides automated classification of data based on content, including sensitive data such as protected health information (PHI), social security numbers, and credit card data. A copy of the data can then be preserved until the violation has been reviewed and addressed.
Flexible Export and Production Options	Data can be exported directly from CommVault software in multiple formats including PST, NSF, XML, or compressed native format, for delivery to third parties including regulatory auditors or outside counsel.

For more information about Simpana[®] software modules and solutions, and for up-to-date system requirements, please visit www.commvault.com