ImageRight

powered by Vertafore

Retention Management

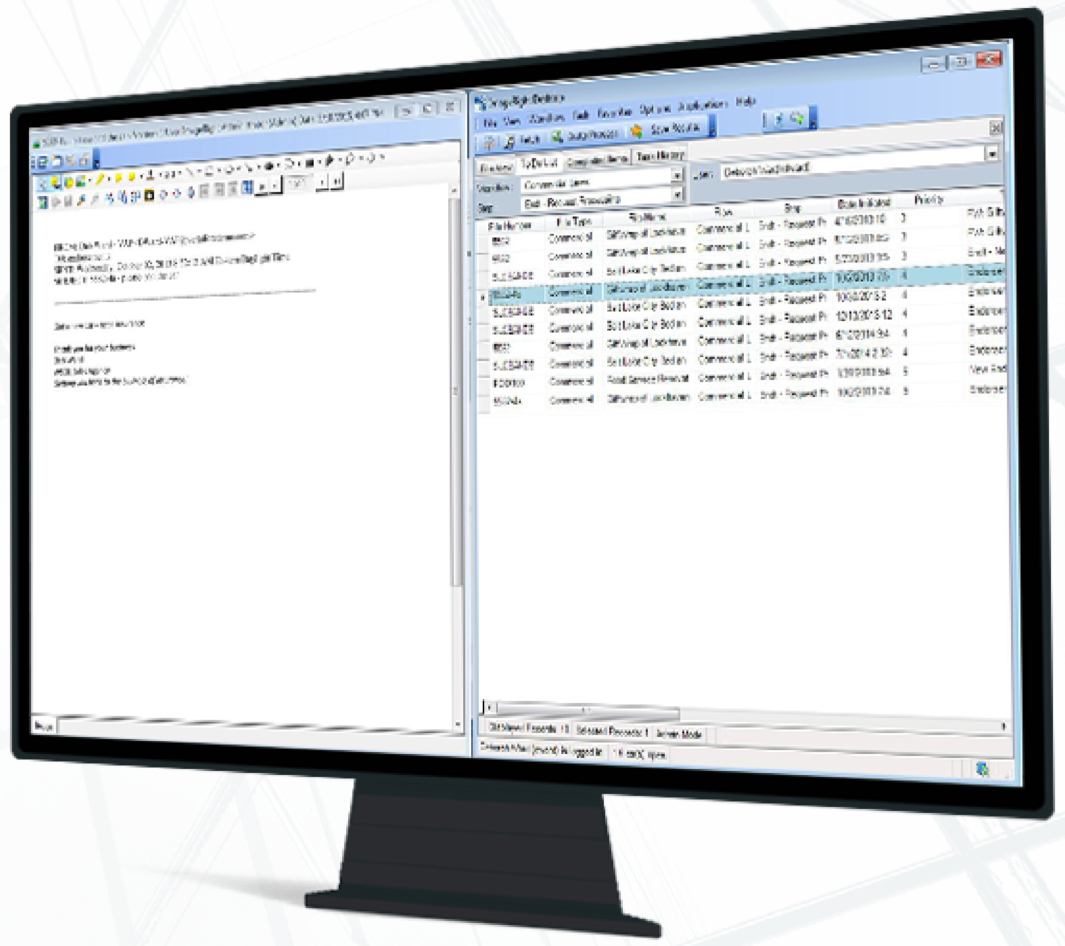
Overview

At some point, you may be required to produce electronically stored content regardless of where it resides (network drive, database, file server, etc.). You may have to prove that all of the content was produced or destroyed in accordance with established record retention policies. A good retention management system is essential to ensuring legal compliance with stipulations from state Departments of Insurance and other organizations. Your retention management system supports your ability to prove that destruction of requested documents was in accordance with a document retention policy.

Using ImageRight Retention Management, you can define retention rules and schedules in ImageRight Enterprise Management Console (EMC) to apply policies across all content stored in your ImageRight system. The uniform application of policies ensures information that is no longer useful or required is systematically destroyed (purged). The rules and schedules include the details of how long the information should be retained and the retention or destruction trigger dates that control the operation of destroying information in the system. In other words, you have the flexibility to dictate what types of content can be purged or retained in the system—automatically.

Why add Retention Management to your ImageRight solution?

- Automatically purge images and corresponding database records based on company-specific retention policies
- Ability to purge documents either manually or automatically on the document approval list
- Automatic calculation and re-calculation of retention dates and periods when a rule is changed
- Ability to set and maintain company retention policies either broadly or on a more granular level specific to certain files
- Ability to set security access so only approved users have the ability to purge files/images
- Multiple fail-safes to ensure only correct documents are being purged from the system
- Customize retention rules and periods by Drawer, File Type, File Number, Folder, Document, and Attribute criteria
- Ensure legal compliance stipulated by the state or other organizations
  - Maintain content only if it is required
  - Protect business and legal interests
  - In the event of litigation or audit, effectively prove that content was destroyed in accordance with an established retention policy
  - Documentation of in-process retention policies and monitoring
- Apply legal holds preemptively or as documents and files meet retention criteria
  - Example: Claim under litigation or involving a minor



Risks of not having ImageRight Retention Management

- Simply deleting content does not remove images or corresponding database records from the system, leaving this “deleted” content at risk of compromise in the event of a data breach
- In the event of an audit, any documents held past their legally required timeframe will become subject to investigation
- Significant time investment required of company technical staff to gather and produce documents for audits
- Incompliance with regulations such as CCPA or NY Cyber Security can result in litigation losses
- Manual upkeep of retention policies introduces risk of human error and accidental purging of content