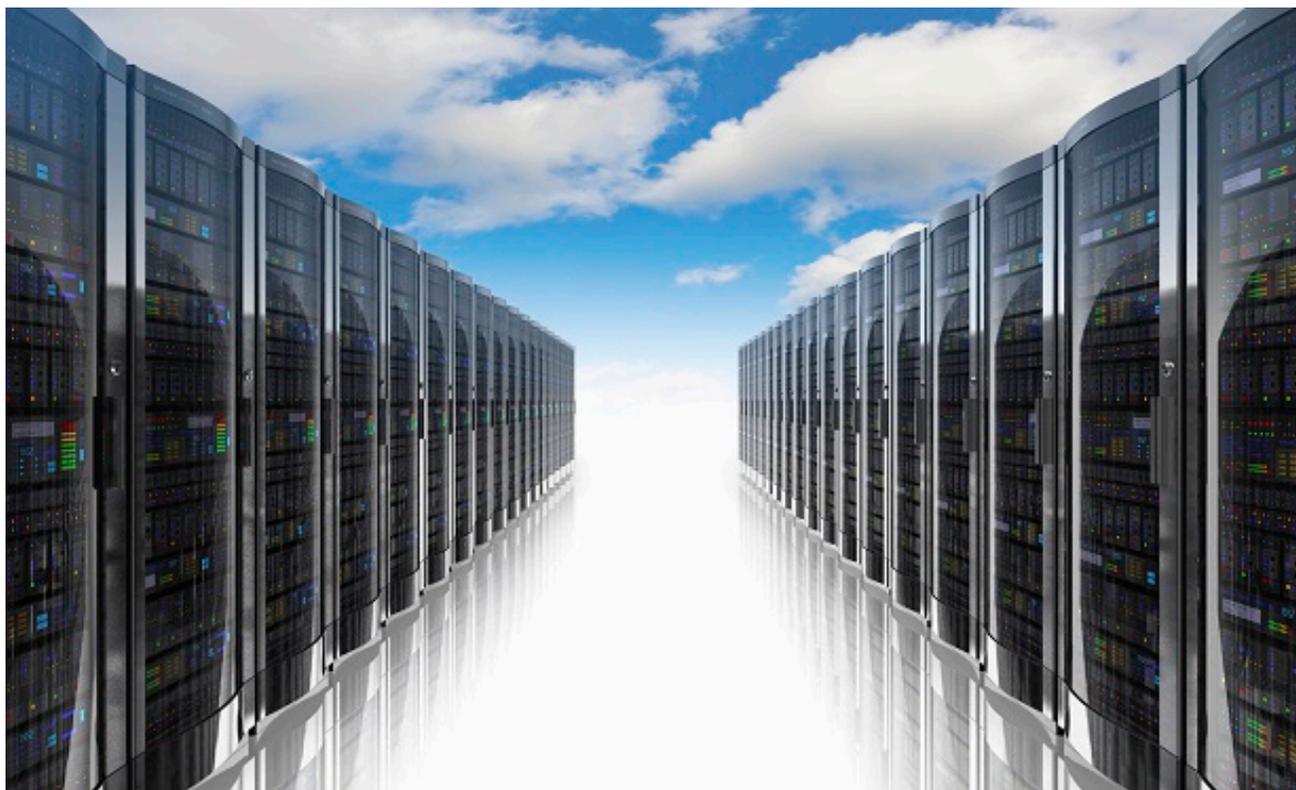


PROPERTY CASUALTY 360°

Written BY Gloria Camacho// April 05, 2018

Can data management technology help insurers reduce defense costs?

E-Discovery: Digitized files present an opportunity for insurers to get in front of pending legal actions, but the industry needs guidance regarding the collection and use of personal data.



the use of advanced data management tools has allowed insurers access to more efficient ways to electronically file and record their documentation.

In the 1990s, large insurers kept their pertinent record-keeping information in folders filed away in huge cabinets lined up at the end of the office.

In Those days, insurers were able to destroy their documents

(<http://www.propertycasualty360.com/2015/07/10/closing-the-loop-in-a-modern-insurance-document-st>) — typically the law would allow for their destruction after a five to seven-year period.

But even if a lawsuit was presented during this period, discovery would be limited to the files a carrier could produce at hand, since there was no way to trace any other form of paper trail.

Related: Discoverability of attorney-generated documents in insurance

(<https://www.propertycasualty360.com/2017/11/20/discoverability-of-attorney-generated-documents-in>)

This problem created huge discovery sanctions and increased defense costs for the insurer. When a carrier wasn't able to produce records, the court could sanction them, and by default, might find the carrier in the wrong in any given lawsuit.

Information storage: Then and now...

[Litigation in the e-discovery era](#) has hit insurers hard in terms of fees and costs.

But the use of advanced data management tools has allowed insurers access to more efficient ways to electronically file and record their documentation.

In 2007, the federal rules regarding e-discovery required the preservation and producing of e-mails and any other Electronically Stored Information (ESI) to be available through the litigation discovery process.

This started a snowballing challenge for the insurance industry, because [stored data](#)

Recent case laws have increased the obligation of a plaintiff or defendant to preserve documentation in pending lawsuits. These can be emails, text messages, word documents, spreadsheet reports and any data fling and maintenance software that the insurer uses.

Anyone in the tech world knows that [once something is submitted electronically, it can be retrieved but cannot be deleted](#). Many insurers have seen huge costs in dealing with e-discovery requirements. Thus, their technology requirements have increased their financial responsibilities.

But eventually, once they improve their data management systems, these costs should start to decline, helping also to reduce costly defense expenses and prevent potential sanctions and spoliation.

Related: [5 big cybersecurity lessons to learn from the Equifax data breach](#)

According to a recent article in [Bloomberg BNA](#), the issues and legal disputes around preservation of ESI have been in the spotlight for several years, and laws around this are still in the development stage.

Insurer insights

Here, I want to discuss some [best practices](#) for the insurer to help reduce these defense costs, but first a bit of background. Most people in insurance are aware that E-discovery is the updated, automated electronic version of pulling files to support a legal claim.

[Instead of paper files filled with contracts and other documents bearing “wet” signatures](#), however, e-discovery features a digitized version of these files, with infinitely easier and deeper accessibility.

This [innovation](#) has emerged as an area where many insurance organizations are examining their processes and IT systems to reduce costs and make budgeting more predictable. It can also prevent a significant portion of unexpected litigation costs.

Being able to cut costs should be a priority for insurers, but because it requires heavy investment in expensive technology, insurers are slow to take advantage of it. So carriers first need to understand their role in [compliance data management](#).

The most recent and important compliance law enacted in the United States was the Patriot Act of 2001, which came in response to the terrorist acts of September 11, 2001. The Patriot Act allowed the government the right to force companies to provide data as an essential part of their investigations, and the data could be held indefinitely. This caused an uproar from consumers about the abuse of their privacy, and since 2005 many lawsuits have been filed against the Patriot Act, declaring it unconstitutional. To date, Congress is still trying to keep parts of the Act alive.

But since 2001, how successful have congressional reform acts been at reducing security control and corruption in how information is stored and reported? According to Westlaw: There is no single, comprehensive federal law — nor even a general one — regulating the collection and use of personal data.

So the U.S. is at the mercy of a ragtag assemblage of federal and state laws that can overlap, agree, or contradict each other.

Related: [GDPR noncompliance poses a real insurance risk](#)

Without proper congressional acts, technology companies have come to rely heavily on best practices — industry-specific guidelines — to determine how best to collect data and preserve it.

Steps toward successful e-discovery

The information that is routinely asked for in e-discovery for [lawsuit support](#) are many of the same data points that carriers are already in the process of automating.

An insurance company might need to pull any or all of the following information:

- [Contracts between agent and carrier](#)
- That your agent was licensed
- That your agent was appointed for the state in question
- A declaration page or policy in its entirety
- Any emails or correspondence
- Anything that was used to make a claim about a product or describe it
- Marketing materials
- Applications for coverage signed by the client
- DOL disclosure of commission (for FINRA)

With that roundup, it's easy to see that once all those files are digitized, the key issue becomes storing it all and being able to access it at will.

Carriers can take steps toward better and easier handling and [storage of their data](#), first by ceasing manual processes of current documentation handling — those grey filing cabinets we discussed at the beginning of this article.

They can do this, first, by making the investment in internal data management tools that have built in security processes. It's a big decision but, as time has shown, the data only gets more complicated and unwieldy with time, not less, and the insurance industry is heavily reliant on up-to-date data. Most carriers first need to figure out how to store their old records, unless they've reached the statute of limitations and the originals can be destroyed. Many companies just store them physically, but a better approach down the line is to have all those folders scanned and thus digitized.

Next, carriers should evaluate their IT Infrastructure and solutions, and begin developing retention policies on how data will be retrieved, preserved, collected and analyzed. With new data management software, you can compartmentalize the data, with multiple ways of tracking it including by the date the contract was signed, or by the date of a claim that falls within that policy period. Carriers can set this up in any way that's familiar and the easiest for them to track it, using a code, or alphabetical order, or by a contract or client name.

Related: [5 questions and answers about litigation holds](#)

Using these data management systems, companies will need to implement appropriate data preservation and management standards, in anticipation of any possible future litigation. This will smooth and ease the process of e-discovery when it happens. And to do this, one best practice is to designate and identify the role of a staff person to lead an e-discovery team in responding to e-discovery requests. This person would then be responsible for the organization's e-discovery infrastructure.

Challenges for compliance data management

[Of the many challenges facing compliance data management, one of the largest is data retention.](#) New laws are constantly being passed that require data to be retained for longer periods of time. But any law regarding data retention first requires companies to have technological systems in place to monitor the retention of these records. Do we, as consumers, expect our data to remain in a system for longer periods of time?

Some companies have failed to consider that consumers may prefer to have their data removed as soon as possible. Data retention laws and regulations require companies to retain records far in excess of what is necessary for business operations.

The reason, according to lawmakers, is to improve security. Simply explained, this allows our government to have access to records that may be used to provide law enforcement agencies with the information they need to find and convict criminals. The compliance data management industry needs to carve out a better role in finding ways to store and protect data. In a society that has grown to rely on software, this technology has provided us with a false sense of security.

So in a way, technology itself has contributed to the need for better compliance data management approaches.

Technology companies still have a long way to go in figuring out how to keep our data safe. And insurance carriers and tech companies alike need to take the necessary steps to manage data more efficiently, instead of waiting for Congress to provide the answers. Most importantly, we need the capability to balance the types of data we're required to retain for sake of defense and cost in lawsuits, while ensuring that consumers feel some sense of security. It's a tall order.

Gloria Camacho is Licensing and Compliance Manager at [VUE Software](#), where she reviews regulatory mandates and advises on compliance strategies. She can be reached at gloria@ecssi.com.

End of Article

Original Link: <https://www.propertycasualty360.com/2018/03/30/can-data-management-technology-help-insurers-reduc/?LikelyCookieIssue=true>



VUE Software.

About VUE Software

VUE Software is an innovative provider of performance-driven solutions built exclusively for the insurance industry. With over twenty-three years of experience in Life & Annuities, Health and P&C Insurance, VUE Software is one of the most experienced and established Insurance Distribution Technology providers in the business today. VUE Software is leading the Distribution Modernization movement, bringing clients a solid path to revenue growth and competitive advantage.



VUE Software is the product division of Computer Solutions and Software International, LLC. (CSSI). This Featured Article is for informational purposes only. CSSI MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. VUE Software and the VUE Software logo are either registered trademarks or trademarks of CSSI in the United States and/or other countries. All other trademarks are property of their respective owners. © 2014 Computer Solutions and Software International, LLC (CSSI).