

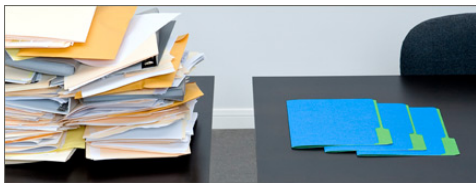
# CA Advisor

GOVERNANCE NEWSLETTER

September 2008

## Retention of Information: Managing the Lifecycle and Evolution of Records

An interview with Dr. Galina Datskovsky



The logic behind records management policies may seem ambiguous to some IT

employees, but one thing is certain: "If you don't have a policy or framework in place, you will undoubtedly get yourself in trouble sooner or later," says Galina Datskovsky, CA senior vice president and general manager, Information Governance.

And we're talking costly fines and litigation, not a tender-tap-on-the-wrist warning. Production of electronic records for discovery can be staggeringly expensive because a third-party legal team is typically hired to review that data. According to leading analysts, a company can spend an average of \$18 to \$19 million to produce and review a terabyte of data.

You need data-retention policies to help ensure that your organization is prepared in the event of discovery, audits or investigations. When determining these policies, Datskovsky says it's essential that every retention policy decision be considered within the framework of Information Governance.

So to understand data-retention policies, it's helpful to first be familiar with the premise of Information Governance, a field of information management that applies policies and risk metrics to all information assets within an organization. These assets can be paper or electronic documents, and electronic assets can include email, instant messages, voicemail records as well as structured data such as that

produced by accounting systems. All of this information must be uniformly governed in accordance with specific policies and controls.

In formulating a policy, you need to first define what your organization considers to be an official record. The next step is to determine how long you want to retain each record type. You will want to set legally defined policies that outline when you can dispose of information. Next, you will draft definitive, written guidelines that will be vetted by legal counsel and/or auditors to ensure compliance with legislation and regulations such as the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA) and regulations from the Financial Industry Regulatory Authority (FINRA). Finally, you must communicate this policy to all employees, and ensure that it is incorporated into the standard business workflow.

That's a lot of effort, but remember the end goal: The primary reason to implement data-retention policies is to enable smooth (and less-costly) discovery in the event of litigation or audit. Data-retention policies will vary by industry — pharmaceutical and financial industries, for instance, have very specific guidelines mandated by their regulatory bodies. When drafting policies, remember that everything that you have preserved automatically becomes discoverable in the event of litigation — whether you intended it to be or not.

**When drafting policies, remember that everything that you have preserved automatically becomes discoverable in the event of litigation — whether you intended it to be or not.**

That's certainly alarming, but don't start deleting files just because they could be later subject to discovery. "I absolutely recommend that people don't keep everything forever or destroy everything immediately. Both of those are very dangerous tracks," Datskovsky says.

"You have to evaluate each individual business and its practice, and then design a policy accordingly so that you are always in compliance and can show consistency in your practices."

**Data-retention policies help ensure your organization is prepared in the event of discovery, audits or investigations. When determining these policies, it's essential that every retention policy decision be considered within the framework of Information Governance.**

In some industries, regulations are ambiguous as to what type of document media is discoverable. For instance, there is no concord across industries that instant messages are considered records. But in the financial industry, the Securities and Exchange

Commission (SEC) has determined that instant messaging (IM) chat logs are indeed a record and companies are obligated to preserve them, according to Datskovsky.

Other industries? Not so much. You may not be required to keep IM documents unless you have created a policy that identifies IM as a customary and acceptable way in which you transact business. In that case, your policy should reflect that.

It's important to note that paper is still a part of daily business, and you can't enforce policies in a way that treats paper one way and electronic documents another. Consistency is key, both in the application of policy and its execution. Applying one policy to email and another to printed or electronic records — simply based on format — does not show a consistent application of policy. And if you shred a printed copy of an official electronic document once its retention expires, but fail to delete the electronic copy, you are not treating information equally in the execution of policy, and therefore would be considered "out of policy."

The situation becomes more difficult to manage when a company has multiple "convenience copies" or printouts of electronic documents that may be in employees' files, desks or scattered throughout the office. These convenience copies must all be found and shredded when their retention expires. If you don't, you are not complying with your policies and these documents would be discoverable in the event of litigation.


Companies that operate outside the United States must adhere to guidelines from all countries in which they do business. And the rules vary across national borders. Privacy laws, for instance, differ from country to country. "European privacy law is more stringent," Datskovsky says. "For instance, employee data that I could view the United States may be considered private in the European Union."

Datskovsky says global companies must also make very conscious decisions about co-mingling of data; that it may be illegal to arbitrarily transfer data between your various servers or networks in different countries. "That should be given some very serious thought," she says. "Legal, compliance and tax people in international corporations are quite aware of this, but your IT professional running the server might not be aware of it. Information about these policies must be driven down through the organization."

After the guidelines have been designed and vetted, automated solutions such as CA Message Manager and CA Records Manager can take these policies and schedules and uniformly automate them across the enterprise.

CA Records Manager is the engine for managing policies and records. It imposes policies on the records where they reside, whether that be in central repositories, shared drives, SharePoint servers or other locations. CA Records Manager also tracks paper documents and uniformly applies policies and provides an official audit trail that indicates who had access rights to the records and who accessed them. CA Records Manager helps you manage, control and discover all of your corporate content across the enterprise — regardless of media or form.

**With the right tools, organizations can make Information Governance integral to every decision because policies and management of data are centralized and automated.**



CA Message Manager, on the other hand, addresses management of email by placing messages in a central archive and controls the disposition in a systematic fashion. It will automatically delete records as their retention expires, and if the data becomes discoverable, its centralized repository makes it simpler to find the data.

With tools like these, organizations can make Information Governance integral to every decision because policies and management of data are centralized and automated. And this proactive approach means it's easier to keep your records manageable in the event of discovery or audit and to continuously trim outdated data from your network.

After all, Datskovsky says, "It's always easier to find a needle if you have less hay."

*Dr. Galina Datskovsky is Senior Vice President and General Manager of the Information Governance business unit at CA, responsible for the CA Message Manager, CA Records Manager and CA File System Manager product lines. She is also recognized as a Distinguished Engineer at CA, and joined the company in 2006 with the acquisition of MDY Group International, where she served as founder and CEO.*

*A Certified Records Manager (CRM), Datskovsky is a globally recognized expert in records management and associated technologies. Prior to founding MDY, she consulted for IBM and Bell Labs and taught at the Fordham University Graduate School of Business and Graduate School of Arts and Sciences at Columbia University. She received her CRM certification in 2004 and earned doctoral and masters degrees in Computer Science from Columbia University.*

For the latest issue of CA Advisor: Governance Newsletter, visit [ca.com/newsletters/govern](http://ca.com/newsletters/govern).  
To subscribe to receive future issues, or to manage your preferences, visit the [CA Preference Center](#).