

USOE DATA RETENTION PLAN

GENERAL STRATEGY FOR DEALING WITH RETENTION SCHEDULES

- Designate backups only for disaster recovery and continuity of business needs.
- It may be appropriate to have each data owner determine the retention schedule for the data they are responsible for. They would need some training as described in this document to do so.
- For any data element or dataset, document its retention time period based on what has been already defined in State Archives; or create a retention period based on the precedents already documented for similar data in State Archives. Sometimes an individual element will need to be addressed when a whole dataset (file, table or database) has more than one owner or if an individual element has shared ownership.
- Document how to comply with that retention time period requirement by either:
 1. Maintaining the data in the production database/store for the defined time period
 2. Archive those data outside of the regular disaster recovery/continuity of business process

Mark Burns (Assistant AG) markburns@utah.gov, (801) 366-0353, is a good source for FRCP & GRAMA and Retention schedules – also Bill Evans who is our Division (Ed) Chief Attorney

HOW TO FIND RETENTION SCHEDULES/RULES AND SERIES INFORMATION/GUIDANCE IN STATE ARCHIVES FOR DATA STORED AT THE USOE (4-8-2008)

GO TO: <http://archives.utah.gov/main/index.php>

CLICK ON RETENTION SCHEDULES ICON

Use just these links:

- **Retention and Classification Reports** (Unique Retention Schedules for Specific Agencies)
- **State... PDF** (html & pdf links go to the same schedules but pdf is easier to search all at once)
- **School District... PDF** (html & pdf links go to the same schedules but pdf is easier to search all at once)

Look for the retention schedule/rules at **Retention and Classification Reports** first and the School District and State PDFs second.

You may have to search all three of these areas to find the retention information you need for a particular database, file, dataset, collection stored at the USOE.

Retention and Classification Reports links to **Retention and Classification Reports by Agency**

On this page you can do a search/submit on the word “**education**” to get a complete list of all the specific education collections. From here follow the links to the education series that appear to hold the information you need. These reports are labeled with 3-5 digit Series Numbers.

A BETTER alternative is to use the index on the **Retention and Classification Reports by Agency** page to go the “S” entries and the **State Office of Education** and **Utah State Board of Education** links.

Note: There are both HTML and PDF versions which are not always identical.

For example, only the PDF version has Records Officer information (Carol Lear for USBE, Barbara Smith for USOE).

The PDF is not searchable, to make it so you must:

- 1) Save the PDF that is open in the browser to the desktop;

USOE DATA RETENTION PLAN

- 2) Open the saved PDF with Adobe (standard 8);
- 3) Export to a new Word document

As of 4-9-2008 these have been saved in H:\security-confidentiality-services-FERPA\GRAMA - RETENTION - eDiscovery FRCP.

If you click on either the **State...PDF** or **School District...PDF**; you will open a PDF in which there are general/generic retention rules.

You can just search for those of interest with keywords. **These general/generic retention schedules/rules are organized by 2 digit Schedule Numbers.**

From the **RESEARCH ICON** you can link to the Research Center and then the **Archives Catalog** (<http://historyresearch.utah.gov/catbegin.htm>) where you can enter a 5 digit Series Number (e.g. 00659, 24486)

OR

From the **RESEARCH ICON** you can link to the **Research Center** and the via the **Subject Guide** link to the **Education Records** collection. However, it fails to find some Series based just on numbers in some cases. It is better to use: **Retention and Classification Reports** (above) at <http://archives.utah.gov/main/index.php?module=Pagesetter&func=viewpub&tid=1&pid=232>

OTHER CONSIDERATIONS

- Retention Schedules can be dictated in numerous ways:
 - State Statute/GRAMA
 - Fed Statute
 - Board Rule
 - Archive Rule
 - Local Rule
- Problems with Archives' datasets and schedules
 - Some of the data listed in retention schedules at State Archives is obsolete and some retention schedules are no longer accurate
 - In many other cases there are no retention schedules for data we maintain in USOE databases.
 - The datasets listed at Archives do not always align well with our datasets. Much of what is listed at archives is a mix of reports, data files and sometime individual data elements.
 - Much of the data listed at archives is found in multiple databases at the USOE. AND, Some of the data within discrete databases at the USOE are listed in multiple archive schedules, sometime with different retention schedules.

There seems to be five major categories of data to be retained:

1. Individual (employee's responsibility)
 2. E-mail (agency keeps for you for 1 year)
 3. Business/Financial/Budget (accounting, school finance, etc.)
 4. Organizational/Policy (all sections in the agency)
 5. Operational data (e.g. HR, Teacher Licensing, Student Information System, Assessments)
- USOE needs a Records or Archive Officer.
 - Some of the Series information at Archives for education is outdated.

USOE DATA RETENTION PLAN

- Archives Website is slow
- For more information see:

<http://archives.utah.gov/main/index.php?module=Pagesetter&func=viewpub&tid=1&pid=4>

and

<http://archives.utah.gov/main/index.php?module=Pagesetter&func=viewpub&tid=1&pid=211>

A Records Officer (as of 4-9-2008 Carol Lear is it for USBE and Barbara Smith for USOE) is "the individual appointed by the chief administrative officer of each governmental entity, or political subdivision to work with state archives in the care, maintenance, scheduling, designation, classification, disposal, and preservation of records" (UCA 63-2-103(21) (1997)). A Records Officer is someone in the office that is knowledgeable about the office's records and who has been authorized to make decisions concerning them.

The responsibilities of a records officer include:

1. Developing and providing oversight of records management programs in their agency, including training others in their agency to follow established records management guidelines, policies, and retention schedules.
2. Serving as the contact person with the Archives. Records Officers may contact their analyst at the Archives at (801) 538-3012. We offer in-office agency training and support for records management questions.
3. Inventorying agency records, developing agency retention schedules, and obtaining agency approvals. The latter refers to agency signatures needed before 1) retention schedules may be sent to the State Records Committee for approval, or 2) records stored at the State Records Center can be destroyed.
4. Implementing State Records Committee approved record retention schedules and documenting authorized destructions of obsolete records.
5. Maintaining information on what record series have been scheduled and conducting periodic reviews to update information as changes occur. Annual reviews are very helpful.
6. Reporting agency's classification designations on record series that it maintains.
7. Maintaining information on record series that have been transferred to the State Records Center to allow for their efficient retrieval.

We officially have two State Archives Records Officers, but are they really active enough? It takes considerable labor to manage retention schedules and keep data sets archived/active on an ongoing basis.

USOE DATA RETENTION PLAN

The solution lies in mapping your data sources. This should be a joint effort between legal and IT. But mapping data sources is easier said than done. For one thing, it assumes that someone in the company knows what data is relevant and where it all is. In a large company, this may be a wholly unwarranted assumption

- As indicated above, we will construct a chart showing data sets, retention periods, owners, backup schedules, and locations. However, as indicated above, rule 26 requires that relevant data must be determined as a joint IT/legal activity. This determination along with what information is not discoverable can be made only when discovery is initiated to satisfy some legal inquiry.
- Having to know the sources of relevant data is why we have the policy that **only** copies of data and documents are allowed on desktops, notebooks or any other local storage devices. The official data are always on servers in known and documented (chart mentioned above) databases.

Companies must identify the departments and employees with custody of the data, and they must create a stewardship that includes a container expert (data source), content expert, or business unit that owns the data – and a policy owner for retention, privacy, and security

- Again, the proposed table will show owners of data. Would Computer Services would be the owner of all privacy and security policies? Data ownership and retention policy ownership are sometime difficult to assign, especially when joint data such as those in the warehouse have multiple owners. Any suggestions??

4. Rule 34 (b): Form of production

Supposedly, the standard for data retention and disclosure is always “reasonableness,” Unless otherwise specified, data is supposed to be delivered in its native form. However, there are issues. For instance, if the data is in an Excel spreadsheet, it can easily be altered. But if you deliver the Excel spreadsheet as a PDF document, it won’t capture the formulas.

- In our backups we may be storing both originally formatted data along with any derived of copies data. However, during the discovery process, original relevant data will be the primary target. If an individual’s data need to be discovered then derived data and copies or original data will more than likely also be discovered.

Typically, the acceptable format should be the way the data was managed in the normal course of business. It is also recommended to keep relevant files in a location that’s provably secure from tampering.

- All production or operational data should be secure. Likewise, an individual’s data are also secure. However, there are some shared areas on the network where two or more individuals have access to common data. However, these areas are for dissemination only and should not be used to gather or change data. All data in these areas should only be copies.

5. Rule 37 (f): Safe harbor

If you can prove that missing data has been deleted during “routine” data expunging, you are probably safe from legal sanctions. However, you must be able to prove that the deletion was indeed part of a routine process and not “event-driven.” Here we come back to good-faith effort, where producing an audit trail and monitoring are key.

However, routine deletion is no excuse for destroying something on legal hold. You must stop and suspend automatic retention and deletion systems in order to secure relevant data.

- This bothers me. Don’t retention schedules address this? If you have a retention schedule for a given category of data and follow it you should be able to easily claim safe harbor for some data in some contexts. However, after an inquiry is made you are still required to suspend any automatic events that might delete data. This was addressed in Rule 26 (f).

USOE DATA RETENTION PLAN

From: Hill, Jean
Sent: Wednesday, December 13, 2006 9:39 AM
To: Brandt, John
Subject: RE: E-Discovery Law

Follow Up Flag: Follow up
Flag Status: Red
John:

I reviewed this issue a few years ago when the Trib sued the governor over emails. Current state law has always covered what the feds have added to the court discovery rules. Official communications in any format must be retained per the state's retention schedules. This does not mean we have to have a record of every newsletter Tina sends out or reminder that some agency party is happening, but any emails between USOE and districts, legislators, vendors, or anyone else we are conducting state business with should be saved just as we are supposed to save the paper copies. How long the emails must be saved for depends on the state retention schedules but most items, I believe, are to be saved for three years. Anything that could reasonably be contested in a lawsuit should of course be saved, and perhaps for longer than three years. I will get the retention schedule for you.

The policy is simple—emails must be saved as any other correspondence would be. The bigger question is how to save all of those emails! I leave that to your capable hands!

Jean

From: Raphael, Randy
Sent: Monday, December 18, 2006 1:01 PM
To: Brandt, John
Cc: Newton, Larry; Hortin, Von; Dudley, Cathy; Houskeeper, Kathy; Hill, Jean; Hughes, David; Paro, Sharon; Southwick, Jared
Subject: FW: E-Discovery Law

Follow Up Flag: Follow up
Flag Status: Completed
John:

I intend no criticism of Maren, but based on this response, I do not think the State Archives will be offering the type of leadership on this issue I hoped for.

Good luck!

Randy

From: Maren Jeppsen [mailto:mjeppsen@utah.gov]
Sent: Monday, December 18, 2006 12:53 PM
To: Raphael, Randy
Subject: RE: E-Discovery Law

Hi Randy, the Utah State Archives Website does have quite a bit of information regarding electronic records. You can access our site at: <http://www.archives.state.ut.us/main/>. Let me know if I can help you with anything.

Sincerely,

Maren Jeppsen
Records Analyst
Utah State Archives
346 S. Rio Grande
Salt Lake City, UT 84101
mjeppsen@utah.gov

USOE DATA RETENTION PLAN

801-531-3860
fax 801-531-3867

From: Brandt, John
Sent: Wednesday, December 13, 2006 4:10 PM
To: Hill, Jean
Cc: Raphael, Randy; Hughes, David; Paro, Sharon; Southwick, Jared
Subject: RE: E-Discovery Law

Follow Up Flag: Follow up
Flag Status: Red
Jean,

I will also review these schedules between now and our meeting on the 11th.

At one time (10+ years) Randy and I worked on the agency retention schedules; but I'm not sure if anyone is officially responsible for them anymore. Maybe it's supposed to be me? Someone should probably be appointed.

Here's a list of documents (paper or electronic) Computer Services has been responsible for and what we've been using as retention times. However, in many cases we probably have data that is older just because it gets mixed in with other files on our backup tapes. We treat CACTUS like HR files; actually we've never deleted anything. The same applies to Rehab client data. Student level SIS data is up to the LEAs although the state's schedule says non transcript data must be kept only 1-4 years. Warehouse data is only four years old and we plan on keeping that indefinitely due to the need for longitudinal studies.

I'm unaware of anyone taking documents to State Archives in recent years. Computer Services has kept paper documents for three years with Mergenthaler Storage.

Retention Schedules

- emails must be saved for depends on the state retention schedules but most items, I believe, are to be saved for three years
- Receipts - 3 yrs after fy end
- POs - 4 yrs after fy end
- non transcript data must be kept only 1-4 years.
- Personnel (HR files) - 65 yrs after retirement or separation
- Personnel (accounting type) - 2 yrs
- Warrants - 5 yrs after fy end
- Data entry forms - 3 yrs
- IT Systems Docs - 5 yrs
- Testing answer documents - 3 years but electronic scores indefinitely. LEAs keep them too.
- Substantive Correspondence - Record copy: Retain by agency until administrative need ends or 3 years, whichever is shorter, and then destroy.
- Official Boards and Committees (Official by statute?) - Record copy: Permanent. Retain by agency for 3 years and then transfer to State Archives. - Duplicate copies: Retain by agency for 5 years and then destroy.

John

From: Hill, Jean
Sent: Wednesday, December 13, 2006 12:57 PM
To: Brandt, John
Subject: RE: E-Discovery Law

John:
I printed out the general agency timelines and looked quickly through some of the USOE documents. It looks like much of the agency specific info defines our records without setting additional timelines. Unfortunately, the general agency timelines are a mess! Retention ranges from delete it when you're through with it to permanent and the

USOE DATA RETENTION PLAN

definitions for types of records are very vague. I will keep slogging through it but I think the more eyes trying to make sense of it the better.

Jean

New litigation rules put IT on the front lines of data access

Procedures for preparedness, data integrity, and retrieval are right around the corner. Is your enterprise ready?

By Ephraim Schwartz From Infoworld

November 17, 2006

On Dec. 1, when the latest version of the FRCP (Federal Rules of Civil Procedure) goes into effect, CIOs and their IT departments will find themselves on the firing line in most major business litigation. [Read about the [cases that started it all](#).]

The process in which businesses decide which data they are legally required to save, and which they can safely throw out, is known as "e-discovery and e-hold." Until now, businesses have been forced to make e-discovery and e-hold decisions based on a mixed bag of individual court decisions, balanced by guesswork by their corporate legal teams. The new FRCP changes all that, codifying a dangerously confusing situation.

Your company's chances of winning in court -- or staying out of court altogether -- will be greatly enhanced by creating appropriate enterprisewide procedures for retention and disposal of data and documents.

Here are five significant changes to FRCP, and the processes your company should establish in order to be legally secure.

1. Rule 26 (f): Early discussion preparedness

This rule mandates that the pretrial conference between opposing attorneys will now have a very specific purpose. A sweeping requirement obliges the company being sued to cite all storage systems that hold data relevant to the litigation, all relevant data sources and data formats, and the steps counsel has taken to prevent relevant data from being deleted. To comply, companies will need a retention program that allows the litigation department to provide and describe this information accurately.

In other words, attorneys will now be required to know how the company's entire electronic data processing system works. According to Trent Dickey, a litigation attorney at Sills Cummis Epstein & Gross, this puts IT directly on the firing line.

"Outside and inside lawyers [must become at least somewhat] proficient in computer information systems," Dickey says. Under the new rules, he explains, during the pretrial conference, company counsel will be required to describe, in detail, all data retention practices, discovery protocols, and preservation processes -- plus exactly which data is accessible, which data isn't, and why.

This is the most challenging hurdle that a company will face in litigation under the new rules, according to Deidre Paknad, president and CEO of PSS Systems, an ISV that creates software to help businesses manage the e-discovery and compliance process. She says the new rules make the e-discovery process more crucial than ever.

"Companies that can prove they made a good-faith effort won't see the brutality of a judgment like that made [against Morgan Stanley](#)," says Paknad. In that case, the company was hit with \$1.45 billion in damages because the judge and jury believed Morgan Stanley had not made a good-faith effort to discover relevant data.

USOE DATA RETENTION PLAN

The biggest risk, says Paknad, is misrepresenting your company's data. If the company isn't fully aware of exactly what it has and where it is, and relevant material is uncovered later, as happened in the Morgan Stanley case, the company will find itself in extreme legal jeopardy.

In order to mitigate that risk, legal counsel must fully understand the company's data practices and indeed must have some control over them. Counsel must be aware of the company's retention schedules and rules, including a corporate classification schema that identifies the major classes of information the company views as records. According to Paknad, there should be specific retention periods for information in each of those classes.

For instance, among financial services companies, where instant messaging is considered relevant, companies are already sampling IMs on a daily basis and matching text against a lexicon of keywords. Tape cataloging is another key ingredient in preparing IM and e-mail for retention and data discovery during the pretrial conference. Cataloging should record the dates of all information on the tape, including the server it came from and the type of data it is, says Francis Lambert, senior compliance advisor at Zantaz, a content archiving company.

In preparing for the pretrial conference, many larger companies are deploying full-time "discovery response teams" made up of litigation attorneys and IT technicians. These teams are tasked with becoming specialists in collecting and preserving data and in learning how best to go about the process of retention, retrieval, and deletion. In the largest companies, these teams are often broken out by category, such as e-mail IT teams or server IT teams.

When a trained discovery response team is notified of possible litigation, it must swing into action immediately. For instance, a key component of complying with the rule changes in 26 (f) is determining which data needs to be rescued from any automatic deletion process that may be about to destroy it. This is known as a "legal hold."

From the time a company reasonably anticipates litigation or receives a legal request for data from another party, IT and legal must be able to identify as quickly as possible the systems and data sources where relevant information may be about to be deleted -- and they must prevent such deletion.

Employees and system administrators who are responsible for data deemed relevant to litigation must be notified of their obligations, and they must respond specifically and affirmatively when notified.

For some companies, even when an appropriate process is in place, the task of tracking notification and response on legal holds can be daunting. "For large companies, there [may be] a couple of thousand cases open at any one time," PSS's Paknad says. If that is the case, the math is terrifying: A company sending one legal-hold notification and three reminders to each of 50 data custodians would have to send 200 outbound notices for each instance. Multiply that, very conservatively, by 100 cases, and you've got 40,000 notices and responses crisscrossing on the network. And all this is merely in preparation for the pretrial conference.

There are additional changes that impact IT directly. For instance, the FRCP and the attached notes from the court recommend that at least one IT person should file a discovery deposition. "It has to be somebody that knows how the IT systems work," Sills Cummis Epstein & Gross' Dickey says. "Companies need to know, [beforehand] who is the spokesman, and that person should be deposed under oath."

A deposition from IT is certainly the smartest and safest way to go, adds Zantaz's Lambert, especially compared with the IT technician making an in-person appearance at the pretrial conference. "You don't want him in there, because it is two lawyers and a judge, and you don't want the IT person saying the wrong thing," he says.

2 and 3. Rule 26 (a) (1) [B] and Rule 26 (b) (2) [B]: Disclosure

Rule 26 covers initial disclosure of sources of discoverable information, as well as sources of information that are not discoverable due to undue burden or cost. Obviously, IT has a huge role to play here.

Rule 26 requires both parties to disclose all information that is relevant to either their claim or defense. The parties must identify information by category and location, Zantaz's Lambert notes. If pertinent data is not disclosed up front, it may not be admissible later.

USOE DATA RETENTION PLAN

However, the more interesting part of Rule 26 is (b) (2) [B], if only because interpretation of it may change depending on the case at hand. For instance, if a lawsuit is for \$150,000, it may not behoove the judge to force a company to spend \$2 million accessing hard-to-retrieve data that exists only on legacy disaster-recovery tapes. However, if the case involves a \$50 million lawsuit it could be another matter altogether.

This means a company should have a pretty good idea how much it will cost to restore data from various media, file types, and locations. The tricky part is that before you know how much it will cost to retrieve the data, you must know which data is stored where.

Comment [jhb1]: This is where it is important to keep all relevant data on servers. Only copies of data on local storage and NO individual data.

The solution lies in mapping your data sources. This should be a joint effort between legal and IT, PSS's Paknad says. But mapping data sources is easier said than done. For one thing, it assumes that someone in the company knows what data is relevant and where it all is. In a large company, this may be a wholly unwarranted assumption.

Comment [jhb2]: We need to go back to Jean and ask what is relevant daaa

With mobile executives storing information on their notebook hard drives, any given piece of data might be on a notebook flying to Milwaukee, in an Access database across the hall, or scattered across dozens of different tables built for end-of-year financial statements.

The solution is to create the data map before you need it. Because there is no business software currently available that can automatically seek out all your data sources and dump them into a document of some kind, IT and legal must come together, not only to map what the data sources are but to record which business processes they touch.

Of course, if you already have a good records-retention policy in place, it will dictate what data your company is going to keep and where it is located. Obviously, the "where" is the link to the data sources.

Companies must identify the departments and employees with custody of the data, and they must create a stewardship that includes a container expert (data source), content expert, or business unit that owns the data -- and a policy owner for retention, privacy, and security. Paknad advises.

Comment [jhb3]: Make a table with these as columns.??

4. Rule 34 (b): Form of production

Supposedly, the standard for data retention and disclosure is always "reasonableness," but Rule 34 (b) can lead to difficulties when the format for delivery is considered. Unless otherwise specified, data is supposed to be delivered in its native form. However, there are issues. For instance, if the data is in an Excel spreadsheet, it can easily be altered. But if you deliver the Excel spreadsheet as a PDF document, it won't capture the formulas.

Typically, the acceptable format should be the way the data was managed in the normal course of business -- but suppose you're using SAP software for invoicing. Your company might wish to deliver an invoice or an e-mail in the form of a PDF, while your adversary may demand to see your entire database. "If the metadata for an e-mail is important," PSS's Paknad says, "you may have to produce the e-mail in native format."

Paknad also recommends keeping relevant files in a location that's provably secure from tampering, as whichever party wants to see the data will also want to be assured it was not, and could not have been, altered.

5. Rule 37 (f): Safe harbor

If you can prove that missing data has been deleted during "routine" data expunging, you are probably safe from legal sanctions. However, you must be able to prove that the deletion was indeed part of a routine process and not "event-driven." Here we come back to good-faith effort, where producing an audit trail and monitoring are key.

However, Sills Cummis Epstein & Gross' Dickey counsels that routine deletion is no excuse for destroying something on legal hold. "You must stop and suspend automatic retention and deletion systems in order to secure relevant data," he says.

USOE DATA RETENTION PLAN

Bottom line: You are legally required to secure all relevant data. If you screw up here, the court can say you are obstructing justice, and the judge may assume that the data was detrimental to your case – as in [Zubulake v. UBS Warburg](#).

Software solutions

Although the onus for compliance will always be on the business itself, many companies are looking to their ERP vendors for solutions. For instance, as PSS's Paknad notes, Fortune 20 companies are going to expect that their transaction and knowledge management systems support retention periods and legal holds. At the moment, few enterprise applications are doing that.

A sea change is exactly what the Fortune 20 will expect in the next year or two; in fact, it's already happening. Paknad says that her Fortune 20 clients are implementing policies for 2007 that will require all systems brought online to support retention lifecycles, legal holds, and collection requests for litigation.

In 2007 and 2008, these features will trickle down to software being used by the Fortune 1000 and beyond. Clearly, every company that may face litigation will be looking for a rapid evolution of systems and features in their enterprise software to make it compliant with the new Federal Rules of Civil Procedure.

It's more than a good idea. It's the law.

DRAFT

USOE DATA RETENTION PLAN

Rules About to Change in e-Discovery Game

By [Jennifer Schiff](#)

November 7, 2006

New federal rules will take effect next month requiring corporations to produce documents in legal cases or face stiff penalties, raising yet another regulatory compliance issue for IT departments.

On December 1, several [amendments to the Federal Rules of Civil Procedure](#) regarding a company's duty to preserve and produce electronically stored information (ESI) in the face of litigation — or pending litigation — are scheduled to take effect. The rules (specifically Civil Rules 16, 26, 33, 34 and 37) have already been adopted in some states, like New Jersey, and other states, including Texas and California, have already implemented some of the new rules.

As with most new compliance rules, there is some confusion and hand-wringing on the part of enterprises as to what the amendments really mean. In this case, the big question companies are asking of their attorneys, IT people, vendors and compliance officers is: Do the new rules mean we have to drastically alter the way we preserve, retrieve and produce electronic data? The answer to that question: It depends. It depends on what practices, procedures and technology you already have in place (if any), and how susceptible your enterprise is to a lawsuit.

If your company has clearly stated, consistent, across-the-board policies and procedures in place on ESI preservation and production in the event of litigation, you may be protected. If your company doesn't, you could be vulnerable to crippling sanctions and fines. Not sure where you stand? Keep reading.

First, Save All the E-mails

To help find out what the new rules really mean for companies, we went to the experts. While all of them agreed there is no one "silver bullet" IT solution that will automatically bring an enterprise into compliance with the new rules, all is not lost.

Many of the problems enterprises face in light of the new rules have more to do with change management — policies and procedures — than with expensive IT solutions. And even if a careful readiness review by your IT experts, compliance team and attorneys finds that you must invest in a content management, e-mail archiving, e-discovery, indexing or other solution, that investment is almost sure to be less expensive than paying dozens or hundreds of attorneys \$200 an hour or more to sift through months or years of decentralized, unstructured ESI (such as e-mail) or getting slapped with huge fines and sanctions for failing to comply with the new federal rules.

"What I think is most important about the new rules is that they underscore the importance of the duty to preserve [electronic data] and put processes in place for very early discussion between parties about the scope of that preservation and what's to be done afterwards," says Stephen Whetstone, a former litigator and currently vice president of client development and strategy at e-discovery company Stratify Inc. "Most companies do not have their house in order when it comes to preservation and document management policies. The new rules attempt to impose some structure in a litigation context against an existing backlog, which is not necessarily a bad thing."

A Gigabyte of Prevention is Worth a Terabyte of Cure

According to a recent report by the Business Performance Management Forum and AXS-One Inc., 36.4 percent of the senior executives and subject matter experts interviewed said their companies had no technologies or policies in place to manage a legal discovery order involving electronic records. Even more troubling, 33 percent said they had no corporate policy in place covering electronic records management in general — and 20 percent didn't know if they even had a policy.

Here's another troubling set of statistics: an October 2005 study by law firm Fulbright & Jaworski revealed that companies with at least \$1 billion in annual revenue are engaged in an average of 147 lawsuits simultaneously, while companies with average revenues under \$1 billion were juggling 37 lawsuits at any given time. On top of that, nearly

USOE DATA RETENTION PLAN

one-third of firms surveyed spent more than 2 percent of their gross revenues on legal expenses, while 10 percent spent more than 5 percent.

So perhaps putting in place policies, procedures and technology that aid in records management and retention and reduce the cost of litigation is not such a bad thing.

Size Doesn't Matter

Many companies that don't make close to \$1 billion may be reading this and thinking that the new Federal Rules of Civil Procedure don't apply to them. But they would be wrong. Even small companies are susceptible, though the likelihood of them spending tens or hundreds of thousands of dollars to prevent potential sanctions or fines is small.

"I don't think the size of the company is the way to look at it," says Ken Rubin, senior vice president of corporate strategy at information protection and storage giant Iron Mountain. "I think it's the risk exposure. While there is generally a correspondence between size and risk, it also depends on your industry. If you're a small medical devices company, you have a lot of litigation risk, more so than a manufacturing organization. It depends on your business. But in general, large organizations — Fortune 500 and Global 2000 organizations — should all be worried about this."

'The Dog Ate My Homework' Won't Cut It

According to Rubin, the days of "the dog ate my homework" — or in this case, "my robodog ate my data" — excuse are over.

"In the old days, if a company's information was stuck in a bunch of information silos and they didn't have common processes and good procedures and said it would be overly burdensome [to produce the data], the judges would be sympathetic," he says. "That is going to end. In order to demonstrate good faith, you have to put in place processes and technology that help you bridge the gaps between all of your storage silos."

Steps Businesses Should Take To Prepare for Litigation

- Formalize document preservation and retention policies and procedures in a consistent, compliant, "good faith" records management program.
- Establish a litigation readiness team of Legal, IT, and Records Management that will establish the eDiscovery process and deal with eDiscovery issues.
- Inventory systems and sources of data, and identify their content, location and preferred form of production.
- For key systems, perform an initial assessment of the cost and methods of production to identify "not reasonably accessible" systems.
- Identify system custodians (administrators) and make sure they understand their roles.
- Apply retention policies to the systems and data sources.
- Develop, document, institute and verifiably enforce formal litigation hold and data preservation procedures.

Source: Iron Mountain white paper, "Rule 26 and Other

USOE DATA RETENTION PLAN

Amendments to the Federal Rules of Civil Procedure: New challenges for litigation readiness."

"People have to have a better understanding of what they're creating, what information they're storing and for how long they're storing it," adds Brian Babineau, an analyst at Enterprise Strategy Group, who agrees that

most companies don't know where all of their data is kept.

On top of that, says Babineau, companies are going to have to develop consistent processes for managing (storing and deleting) data and "be able to assign a cost of accessibility for that information over time. So for example, now they're going to store everybody's e-mail consistently for 90 days online and it's going to cost them X amount to retrieve it. After 90 days they'll store it for another two years and it's going to cost Y to access it."

Still, Babineau doesn't see the new rules as bad news. "I think this is actually good news for enterprises, because there's more clarity around electronic discovery than there ever was."

Creating a 'Treasure Map'

So how do companies go about complying with the new rules? They need to have a "topographical map of where all their electronic records are," says Rubin. "And they need to know not only where they are, they need to know the relative ease of retrievability. They need to understand relevance and the production costs and the formats. They really need to have what I would call a treasure map of where their records are."

But can a single IT solution give companies a map to their buried treasure — and ensure compliance with the new amendments in the case of litigation?

"We don't really see any silver bullets out there from a technology perspective," says Mike Kinnaman, vice president of marketing at Attenex, an e-discovery company that helps enterprises improve the efficiency of processing and reviewing electronic documents. "There isn't an end-to-end solution that someone can just drop in."

But you can — and should — get your IT and compliance people and your attorneys all speaking and working together to find out where your data resides, what's accessible, what's inaccessible, and make sure you have a readiness plan, which means, says Whetstone, having "best practices and procedures in place when the duty to preserve is triggered, so that you know you can quickly lock down [data]."

Good News for IT Vendors?

"Technology got us into this mess and technology will get us out of this," says Whetstone. "There are new tools, Stratify happens to be one, that allow lawyers, reviewers, companies to better understand their data universes, better manage them in real time, better organize and pre-organize these data universes, so that when a litigation threat arises, when the duty to preserve triggers and there is a need to go get the data, they'll be able to look at their data across business units by subject matter and be able to then focus their review and leverage technology's ability to cluster like documents together.

"As a result of that, reviewers will be able to far more rapidly review the documents and communicate their conclusions with one another and ultimately to the courts or investigative bodies," he says. "That's very powerful. And it's going to drive down the labor costs, because it's just not sustainable to have dozens or hundreds of litigators at \$200, \$300, \$400 pouring through massive volumes of electronic data as if they are looking at stacks of paper on their desks. So there's going to have to be a need to leverage technology."

That's good news for a lot of IT vendors — many of whom have been hawking their various data management, data retention, data indexing and e-discovery wares in advance of the new rules.

Late this summer, Symantec announced it had added support for new federal regulations (among other services) for its Enterprise Vault Discovery Accelerator e-discovery solution (see [Symantec Speaks Legalese](#)).

USOE DATA RETENTION PLAN

More recently, Iron Mountain announced a new retention management solution called Retention Center, which "will allow organizations to manage, monitor and audit systems and repositories that contain records and information to meet compliance and litigation requirements."

And the list goes on, with e-discovery companies such as Attenex and Stratify talking up their solutions' ability to help companies sift through large collections of unstructured content, such as e-mail and MS Office documents, and quickly zoom in on the most relevant information needed, and data management software provider CommVault positioning its Unified Data Management approach as a way for customers to "establish and document end-to-end processes for data discovery and preservation," according to David West, vice president of marketing and business development at CommVault.

The new rules also "bode well for the information classification folks like Kazeon and Index Engines that can index corporate content," says Babineau.

Is Any of This Good News for Enterprises?

For enterprises that do act in good faith, there is a "safe harbor" provision, Civil Rule 37, "that protects a party from sanctions for failing to provide electronically stored information lost because of the routine operation of the party's computer system."

While that is definitely good news, it is not a "Get out of Jail Free" card, says Whetstone. "In other words, it will not work for lawyers or companies to continue to delete or overwrite consistent with their standard document retention or management policy after the duty to preserve arises," he says. "If you have a 30-day recycling policy in place with respect to e-mail, when the duty to preserve arises, or when you're served with a complaint and you have to lock down data, you can't hide behind Rule 37 and say, oh, the data was lost in good faith because the system kept overwriting data for the next 30 days and someone forgot to turn that off. That's not going to work very well."

The bottom line: "It's hard to say that these types of things are great, because they require organizations to change a little bit, but it's just about standard operating procedures and policies and then buying the technology to support them, as opposed to forcing companies to go down a specific path and buy specific things," says Babineau. "There's enough guidance, but it's not specific enough to be a burden."

Mike Kinnaman, vice president of marketing at Attenex, agrees. "The good news about these amendments is they're taking the best practices that already exist and making them more widespread," he says. "It really comes down to understanding where all the data is and then the bigger piece is using a document retention policy. If you do those two things, then the courts are going to look upon you favorably."

For more storage features, visit [Enterprise Storage Forum Special Reports](#)