contoural

Practical Advice in Document Retention
Real Strategies that Work

Abstract: This article covers key areas in document retention, including:

- Getting employees to follow the program
- Why Aggressive Deletion Does Not Work
- Moving from Paper-centric to Electronic Records Program
- Do You Need to Save Voicemails?
- Creating Multi-national Record Retention Schedules
- Hiring a Records Manager

Getting Employees to Follow the Program

Much of the conversation around eDiscovery discusses the perils of poorly executed Legal Hold processes. Yes, companies do get in trouble for not saving the right documents at the right time during litigation. But let's face it, most inside counsel experience more stress over a far different issue: their employees save nearly everything forever, driving up the cost and risks of discovery. Unmanaged, employees save emails, files and other types of electronically stored information literally everywhere.

Companies do attempt to discourage this behavior, often with little success. Some believe that this packrat mentality is ingrained in employees and unavoidable. Can employees really be made to change their ways?

Yes, but companies need to be smart about it. Good change management programs can be very effective in significantly increasing compliance with document retention, while avoiding "underground" archiving, or employees engaging in rogue retention. Here are some keys to good document retention *and deletion* change management:

Create Retention Policies That Recognize Business Value – Many organizations base their record retention schedules purely on regulatory compliance, an approach ignores that some documents have significant business value. Good record retention policies incorporate retention based on business value along with regulatory compliance. Not all documents have business value, only some of them. The key for workable policies is to provide some level of balance in how much and how long documents are kept.

Give Employees an Option, But Make Continued Retention Manual – Capture your documents in an archive that automatically deletes documents after a prescribed period of time. Give employees the option of saving some important documents longer than the stated retention period, but require them to manually override the deletion period. Some will do that for some documents. Most, knowing that they can retrieve older documents at some point in time will

forget. The result will be that most documents are deleted by the system, without the employees engaging in underground archiving. Use employees' inactivity to your benefit.

Sell the Win for Employees – Too often messages on document deletion come across as the Legal department dictating from the top of the proverbial mountain, telling employees how saving less documents is better (for Legal, that is). Employees quickly tune out these messages. Good record deletion strategies do benefit Legal, as well as IT, HR, business units and other departments. Perhaps most important, good retention and deletion systems can also benefit employees themselves. One large company when deploying an email archiving system dictated from the mountain to no avail. But when they changed their messaging, discussing how email captured in the email archive was easier for employees to search their messages, and how they archive could restore all email even if the employee's desktop computer crashed (not possible previously), the employees tuned in and got on board with the program. There is a win for everyone, not just Legal. Your messaging should reflect that.

Measure, Train, and Monitor – First measure. Assess how much compliance there is with the current retention policy, and the amount of underground archiving. Next, train employees on compliant retention and deletion. Include in this training some of the messaging discussed previously. Be clear, prescriptive and function-specific. Once the program is launched, then measure again. If your training worked, good, if not, modify the training. Also implement ongoing monitoring. Make sure the right documents are being saved, and any given employee is not saving too much beyond the policy. While it is very difficult to monitor everyone, the 80/20 rules applies here. For example, we have found identifying the worst 5% of group file share storage "hogs," and then reaching out to them specifically to clean up and comply with the policy can sometimes reduce overall file system storage by as much as 40%. It is nearly impossible to monitor everyone all of the time, but taking a closer look at the worst offenders can have disproportionate beneficial results.

One last note: some inside counsel will never be happy, believing that these types of change management programs permit employees to save too much. My response: give up perfect and go for good.

Why Aggressive Deletion Does Not Work

Most inside counsel don't like e-mail. They believe it is evil. To be more specific, inside counsel worry that if an organization faces litigation, the e-mail they discover is much more likely to be hurtful than helpful. The fear is that employees send either irresponsible or poorly stated e-mails that taken out of context can come back to haunt. The plaintiff's bar on the other hand likes e-mail. One class action plaintiff's litigator likes to brag about the success he has had in "mining" e-mail. "Give me enough e-mail, and I'm sure I'll find something bad." Even if employees are writing responsible messages, with so much e-mail (the average employee sends and receives more than 160 messages per day) the cost for discovering this accumulated mass of e-mail for a single large case can sink a corporate litigation budget. Yes,

sometimes help you; they can be exculpatory, providing the only evidence of no wrong doing. Overall, however, most inside counsel simply do not like e-mail.

Therefore it is not surprising that many companies are taking active steps to delete e-mail early before it can do harm. The most common deletion technique is “aggressively” deleting any e-mails older than sixty or ninety days directly from the employees e-mail boxes on the e-mail server. Be careful. Although well-intentioned, we have found that these aggressive e-mail deletion strategies backfire, driving employees to save e-mails in places that keep them safe from being deleted but make them harder and more expensive to find during discovery. I’ve coined the term for this “underground archiving.” Employees who see their older e-mails disappearing from their mailbox often save these messages in other places. They print them out. They will save offline copies of e-mail in standalone “PST” or “NSF” files (depending on your type of e-mail system) and then save these files on desktops, laptops, centralized file servers, USB drives, etc.

Some IT organizations have taken to disabling the ability to save e-mail in these offline files. So what do employees do? They step up this messaging arms race and send copies of e-mail home. One employee of a large financial services firm came up to me after a seminar and explained how every e-mail he sent and received at work he sent copies of these messages to his home account, and then burned these messages on CD ROMS every three months, in clear violation of his employer’s retention and privacy policies. Discoverable? Absolutely. Note: many savvy plaintiffs’ counsel regularly demand the defendant search for relevant documents on employees’ home computer systems.

Another ploy is employees will simply blind carbon copy e-mail messages to a Google Mail or Yahoo! account. Google currently offers users 7GB of free e-mail storage. And yes, these accounts are also discoverable. The truth is that of the many organizations we have reviewed that have aggressive e-mail deletion policies, nearly all had some or a substantial amount of underground archiving, and despite their intentions, actually had a significant amount of saved e-mail in the nooks and crannies of their IT infrastructure.

So, if aggressive deletion does not work, are we therefore cursed with ever-accumulating e-mail? Of course not. You can get rid of e-mail, you just need to be smart about it. Today many companies are deploying “smart” archiving strategies that provide a reasonable, controlled and safer way of saving e-mail in one centralized place, typically utilizing a centralized, automated e-mail archive. These organizations typically introduce the process with liberal archiving policies and choose solutions which make archiving emails easier (for the user), thus improving compliance and largely avoiding or diffusing underground archiving. Once the archive is available, IT then disables the e-mail system from allowing the creation of offline “PST/NSF” files. These steps are followed up with centralized, automated deletion after a year or two (based on the employee’s role).We have found that organizations that take this approach typically save more e-mail initially, but are much more effective at getting rid of older e-mail, especially since e-mail can be accessed and deleted from the central archive, and not

in the elusive “PST” file. The focus turns from deleting already created messages to training employees to be more responsible in their email usage.

This involves reversing traditional thinking to achieve the same result. Inside counsel need to suspend their dislike of e-mail, and allow the organization to save more of it so it can be stored in the central archive. Once there, it is much easier to delete the medium and older age email, as well as discover what remains. Companies with smart archiving strategies typically have much, much less e-mail than those with “aggressive” deletion. That is a good thing.

This example also illustrates a larger lesson in compliance. While employee behavior can be encouraged, modified and monitored, any strategy that attempts to swim too long against a strong current of employee will and desire is likely to fail. If your program is not getting the results you want, take a step back and see if there is a smarter way to approach it.

Moving from Paper-centric to Electronic Records Program

Today we live in a world dominated by electronic information. According to ARMA more than 90% of all records created or received by organizations are in electronic media. Yet many corporate record retention programs are based on an older, paper-centric paradigm. For the most part, paper-based record retention processes do not really work for electronic documents. If you are like many companies that are transitioning your record retention program, you need to be careful to do it the right way.

Focus on content, not boxes – Move away from a record = paper = “count boxes” mentality . A file folder is not a record – the content of the file folder is the record. Move the organization away from managing physical assets and focus on content, regardless of media.
Consensus Across More Stakeholders – Paper-based programs may be more “facilities” oriented – only dealing with storage of physical assets. The move to electronic record/content management requires buy-in from cross functional teams, including IT, Legal, Compliance (for data security issues around PCI, PII, PHI, etc.), et al. This wider scope can make electronic record retention programs more challenging, yet at the same time impact more areas of the business and provide a greater value to the organization.

Invest and Save – Paper-centric programs look primarily at physical storage costs primarily (onsite office space vs. offsite storage). Combination electronic and paper programs need to consider broader set of factors for electronic documents, including investment in archiving tools, data storage, etc. These programs typically have higher investment costs, but also have greater return on investment.

Identify the Copy of Record – Electronic documents tend to have many more copies of the same document throughout the organization than paper records, exacerbated by e-mails that are cc’ed to what appears to be most of the English-speaking world. More care needs to be taken to identify which groups or individuals are responsible for saving the official copy of an

electronic record (sometimes called the copy of record) and also communicating to everyone else that their copies (considered convenience copies) need not be saved. Don't have multiple people save the same record.

Get Rid of the Paper – It is literally one hundred times cheaper to store a document in an electronic medium than in paper. More than 70% of paper records are copies of electronic documents. Save it once electronically, and then don't save it in paper. Good electronic retention programs can reduce the ongoing paper storage by 80% or more.

Avoid Fauxpliance – One common approach for upgrading a record retention program is to send an automated e-mail to employees every week or month having them confirm that they are manually following the records retention schedule for their e-mail and other electronic documents. This approach sounds easy, except it doesn't work. Even well-meaning employees will click yes, intending to do it later and never do it. Our surveys have found that reminder-based programs with no real archiving have very low actual compliance. We call this fauxpliance (faux + compliance). Electronic records require archiving systems that are integrated with employee's day-to-day work streams.

Get the Right Skills -- Perhaps the biggest challenge in transitioning may be your own staffing. In the words of Pogo, "We have seen the enemy and he is us." A generation of records managers grew up believing that effective records management is based on a manual, "let's manage the boxes" mentality. Adopting to today's world of electronic information may not only require new skills, but also reexamining old ways of doing things.

Do You Need to Save Voicemails?

Are voicemails business records that need to be saved? This is a question I often get at my seminars. The short answer: 1) Occasionally yes, 2) but for most organizations no, 3) it depends in part on your record retention policy, 4) but don't attach them to e-mail unless you are willing to endure the consequences. Perhaps a more coherent explanation is in order. Voicemails are ubiquitous, and the question arises whether any of them can or should be considered business records, and if so, how long should they be saved. At Contoural we define a business record as a document or electronically stored information containing content reflecting the organization's business operations or decisions. Does a voicemail recording qualify as a business record under this definition? For the majority of organizations, the answer is no. Typically a voicemail in itself does not record decisions or operations. A good litmus test is whether a voicemail or other document type is acceptable as the sole record supporting a decision. Applying this test, would a voicemail approving the purchase of new equipment, for example, suffice as the sole record of authorization? For most companies the voicemail in itself is not sufficient and the decision to buy something would need to be recorded in an e-mail or purchase requisition. Therefore one could argue that the voicemail is not a business record.

(Or to be technically correct, in this example a voicemail is considered a non-business, transitory record, which does not need to be saved.)

There are some exceptions to this, which tend to be regulatory-driven and industry specific. Under SEC 17a-4 Broker Dealer regulations voicemail recordings from customers wishing to buy and sell securities are considered records. Under some statutes certain voicemails from state and local governments are considered records. Again, these tend to be exceptions. Companies actually have some leeway in declaring what is a record and what is not, and in which media records should be saved. A good record retention policy and schedule should clearly spell out whether an organization classifies voicemails as records. If the answer is no, make sure the policy clearly states this. The policy should address exceptions. If an employee does receive a voicemail containing content that may require retention as a business record the policy should require the content be documented in a medium that does support record keeping, such as e-mail. Common sense and consistency are important here.

While companies may be able to classify voicemails as not being business records, this does not mean they should be ignored. Regardless whether you declare them or not as business records, voicemails are clearly a type of electronically stored information and discoverable under regulatory inquiry or litigation. (See *In Re: Seroquel Products Liability Litigation, 244 F.R.D. 650 (M.D. Fl. 2007)* where the defendant's failure to produce any voicemails was one of multiple failures that led to the court sanctioning the company.) Often discovery requests will include voicemails.

The worst problems arise when voicemails accumulate in combination voicemail and e-mail systems called unified messaging systems. These unified messaging systems record voicemails and then send them to the recipients in ".wav" audio files attached to e-mails. Employees often hold onto and accumulate these e-mails containing voicemails.
When either regulatory inquiry or litigation discovery strikes companies may find themselves in a possession of quite a few voicemail messages. Unlike text which can be searched, voicemails need to be reviewed by a human. We are aware of one company that had to review more than 10,000 voicemails for a single matter. There are some e-discovery technologies that transcribe voicemails to text, and this text is analyzed for relevance. However, exclusively reviewing messages in this manner may not be defensible. Because of this potential liability around discovery, many organizations have turned off this voicemail to e-mail capability in their unified messaging systems.

Deal with these voicemail issues early through a combination of policies and processes. Good policies delineate business records from non-record documents. Good processes discourage ongoing accumulation of non-record documents, including voicemails.

Creating Multi-national Record Retention Schedules

Creating a record retention schedule and executing a records program for multinational companies operating in many countries can be overwhelming. Each country has its own record retention regulations, and different records are created and stored in different countries. These multinational policies and schedules are one of the most challenging aspects of building a program, but if companies follow some basic guidelines they can be successful.

Create a Global Policy But Allow for Local Exceptions – Some companies create a separate record retention policy and schedule for each country or region they operate in. I think this is a mistake, as it becomes exceedingly difficult to administer multiple policies across the enterprise. We have found it much more effective to create a single, global retention policy. Often the business need for retaining a record is enterprise-wide, and this business need may trump the aggregate of local requirements. On the other hand, there are country-specific exceptions requiring some records to be stored longer, and other records to be destroyed earlier than the global policy. Instead of creating separate schedules for each country, allow local exceptions to the global policy. This keeps it simpler. Initially it may appear a global policy will require many exceptions, but we found most global schedules end up with many fewer exceptions than anticipated.

Consider High Watermark Retention Periods – If an engineer creates a safety procedure document in San Jose, and shares this record with an engineering group in Dublin, who then share it with the team in India, which country's regulatory retention requirements should apply? It's difficult to determine because electronic information often literally travels around the globe. Favoring clarity and compliance, I think the best approach is often to adopt a "high water mark" retention period, adopting the longest retention requirement. This will often be the United States. Trying to pin down where a document lives is difficult and can easily lead to non-compliance.

Engage Foreign Business Units – The biggest mistake U.S.-based companies make in developing record retention programs is creating a policy with only input from their U.S. business units, and then adopting this policy for the rest of the world without consulting the international groups. These international groups often then feel that the policy was foisted upon them and start listing reasons why the policy cannot or should not be implemented in their country. Often the root issue here is not compliance with local regulations, but rather that these groups were not engaged and consulting. Good early engagement can go a long way, and many of the "this policy won't work over here" objections tend to melt away when these groups felt heard.

Be Prepared for Sparse or Ambiguous Local Regulations – Unlike the U.S. and Europe, many countries have either sparse or ambiguous regulations governing document retention. The regulations that do exist often tend to be focused on paper records. Search for Ghana's requirements for saving employee records, for example, can be fruitless because these regulations don't exist. More research does not yield better answers. Organizations need to

create policies even without the underpinning of local requirements. Often U.S. and European-level retention requirements can be used in these situations.

Keep an Close Eye on Data Privacy – One area does require close scrutiny. Data privacy regulations are generally stricter outside the US, especially in Europe, and in France and Germany in particular. While a data privacy policy is separate from a record retention policy, a good record retention policy needs to be data privacy aware. There are restrictions, for example, on when and how employers can surveille employees' archived e-mail in some countries. Many of the aforementioned local exceptions to global policies are around privacy-related issues.

Hiring a Records Retention Manager

Many companies are creating or expanding their in-house records management and e-discovery staffs. One question I often get from clients is what type of skills should they be looking for in candidates. This is an important question as these roles have changed significantly during the past five years.

First, as inferred in this article's title, many companies are combining their records management and e-discovery functions into one group. Records management is fundamentally about keeping and deleting records, and e-discovery is about knowing and producing all the documents you have. A strong records management program will beneficially impact e-discovery, and many e-discovery tools and processes can drive good records management.

What skills should you be looking for in your candidates? There are four main areas to assess:

Records Management – Potential candidates need to understand records management concepts, including understanding the role policies and retention schedules, regulatory issues, classification strategies and auditing. ARMA offers excellent records management certification programs.

e-Discovery Skills – In-house e-discovery staff need to understand all phases of the e-discovery model (EDRM.net is the accepted industry standard), with a strong emphasis on early stages including identification, preservation and collection. Other than a JD, today there are no nationally recognized certification programs for e-discovery, although there may be some announced later this year.

IT Skills – As more than 96% of all documents an organization creates or receives are in electronic format, it is essential that records managers and e-discovery specialists understand and are comfortable working with technology. This should include e-mail archiving systems, e-discovery programs, records management systems as well as storage

and backup technologies. AIIM, a records-oriented IT industry group, offers training programs in these areas.

Project Management – An often overlooked area is project management. In-house staff need to orchestrate and manage complex tasks involving teams, processes and technologies. This is particularly important if the current legal department staff does not have strong project management expertise. I tend to be less concerned about whether someone is a Certified Project Manager (offered through the Project Management Institute). Instead, it is important for candidates to have demonstrated experience in managing large, complex projects. It is unlikely that a company will find candidates with all four or even three of these skills. That's OK. Focus on candidates who have some of these skills and have the athleticism and attitude to learn the others. (We have a template job description we share with clients. E-mail me for a copy.) Compliance, legal and technology are involving quickly. In-house staff in these positions will always have to be learning on the job.

Do not always think you have to go outside your company to fill these positions. In our experience, many companies have been successful in finding the right people from internal candidates – a paralegal, for example, who wants a new challenge, or savvy IT professionals who are interested in e-discovery and retention.

The final consideration is probably most important. Do you want the employee to build or run a program? Builders like the challenge of putting something together, but get bored with ongoing program management. Runners enjoy monitoring and managing program compliance and training, but have less interest in initially creating the processes. These are different mindsets, and be sure you get the right one for your program. Once a program is in place – often with outside help – most of the work is managing the program. All else being equal I tend to lean more towards runners than builders.

About Mark Diamond and Contoural

Mark Diamond is CEO and founder of Contoural. Contoural is the largest independent provider of records & information management and litigation readiness consulting services. The company is a trusted advisor to more than 20% of the Fortune 500, plus numerous mid-sized and public-sector organization. Contoural is independent and sells no products, document storage services or "reactive" e-discovery. Contoural provides assessments, records policy and schedule development, litigation readiness, change management and record management program development services. More information and other articles are available at www.contoural.com.