

INFORMATION REQUIREMENTS

CLEARINGHOUSE

303-721-7500 -- sales@irch.com

Law, Records and Information Management Questions and Answers

by Donald S. Skupsky, JD, CRM, FAI

Thank you, Andre, and good afternoon to all of you. Good morning to those on the west coast. It's a pleasure having you to the seminar. This is our fourth in the series, we did three in 2015. They are all on our website, and this will be the first of three or four this year. We're glad to have you aboard.

Decided to do questions and answers for this session as opposed to me predetermining what the subjects would be, so with no further ado let's move on with that. What I found is that there are a number of issues that organizations have been dealing with, and they fall into the domain of electronic imaging ... We had a number of questions like ... I've given you the count, just so you know these are actually legitimate questions. The retention of accounting records with some very specific issues. The three-year presumption was raised again, I'll go over that and explain one minor change. Retention program implementation compliance, a variety issues in that area.

What I've tried to do in each of these areas is consolidate the questions and give a consistent answer, so my answers actually respond to numerous questions all at the same time. Privacy versus records retention, how do you reconcile any differences. We get into litigation protection, and then information, governance versus information management. Let me move on with all of this, and ... Oops. [00:02:00] Slight little problem. I'm going to pause my sharing for a second and get that resolved. There we go. Okay. I had reviewed the questions with you, and now let's move on to the next part of the presentation.

Electronic imaging and reproduction. It's amazing that after all these years, there are still questions related to this issue, and we'll be very happy to deal with the areas that I'm about to discuss plus others if you have additional questions. I can't cover the entire subject, but I'll cover some key issues. What I'm going to look at is, will the courts accept electronic images? When are paper records required or preferred as part of litigation, and probably expand that to government investigation also. When can you destroy paper after the reproduction, and when should you destroy it? Should you have an option in all of that? Have there been any changes to ESIGN? Some of you may or may not know what ESIGN is; rather than explaining it now, I'll explain it in just a few minutes.

When you get into the core acceptance of electronic information, I want to reiterate what I've been saying for decades. Electronic images are 100% admissible in the United States courts, there are no exceptions. Why is this an important issue? Because people have been looking for the test case, people have been requesting what is the basis for this. The answer is, there is no problem. There has not been a failure in the [inaudible 00:03:57] of electronic imaging, [00:04:00] when there's reasonable images presented. If there's a failure in the system, that's a totally different question.

Original records can then be destroyed after reproduction, and I add quality control. We do know after you do the reproduction, you do not have to have the original records under numerous laws, and I'll cite the number of

those in a second, that you may destroy the original after reproduction. What I'm seeing is a number of organizations are failing in their inspection of quality control. Often they are buying the scanner, they're scanning it into their system, and away they go. If you do not record quality images, you have not preserved the records, and you are subject to all sorts of fines, penalties, and whatever other issues may be subjected upon your organization. Please be aware that if you have not implemented good quality control in your organization, now's the time to do it, before you get yourselves into trouble.

If the original records continue to exist, then the other party can request them. This is true in all cases. Regulatory agencies can look at it. Here you've developed this very efficient electronic imaging system, and then all of a sudden the other party will cause you to go through your paper record system, maybe even pull back boxes from the record center. It's very important you destroy the original records after reproduction. There was one question on exceptions, and I'll address that shortly.

Reproduction may continue after litigation begins. You can continue to make images, even if you're involved in litigation; but [00:06:00] the relevant originals cannot be destroyed. The rules change. There's a hold placed on those originals, destruction of the originals while litigation is in progress is destruction of evidence. On one level you're not doing anything terrible because you're preserving the record; on the other hand, it looks bad. You're destroying records. Don't do that, you'll get yourself into trouble.

Now we'll get into the court acceptance of electronic imaging. As we've talked about, there are reasons why this occurs. Let me go through some of those with you. I'm having a little problem with my technology, and I'm not sure why. Let me stop this for a second and let me check out what my problem might be. [00:08:00] Sorry, we've had a little glitch in our technology, but we're fine now. The full set of slides will be available to you on our website shortly after the presentation, so please go there and you'll be able to get that information. I apologize for that.

The reason for the legal acceptance of electronic imaging is a number of laws. The first one I've cited here is the Uniform Photographic Copies of Business and Public Records as Evidence Act. I'm not giving you the exact citation, you can go Google it and read the text of the law. Except in the US federal government, it's called the Uniform Business Records Act. This is a mistaken name, just a freak of history. Previously many years ago, the United States federal government had two uniform laws in one section of law. One was the Uniform Business Records Act, the other is the Uniform Photographic Copies of Business and Public Records as Evidence Act. They deleted the Uniform Business Records Act, leaving the UPA, and left the name, which was the previous act. They made a mistake in legislative drafting, but that's what they call it.

There are the Uniform Rules of Evidence that are just about in all states and the United States federal government, and there's provisions there that allows reproductions to be admissible into evidence, explains some of the requirements. You would need a process or system, and a showing that the process or system produces an accurate result. Each of the states cite it a little bit differently, so again, you can search under the Uniform Rules of Evidence.

We also have the Uniform Electronic Transaction Act, referred to as UETA. UETA, yeah, was adopted in 1999. [00:10:00] The United States federal government did not enact the UETA, it enacted instead a law called ESIGN. I'll explain that in a second. The UETA basically gives you permission to use electronic records whenever records are required, and to use electronic signatures in place of analog signatures. The Uniform Records Retention Act is only in eight states. I'm going to refer to it again a little bit later in the presentation, but there's on paragraph

that relates to electronic imaging where, in those eight states that have adopted it, if the law requires that you keep records the preservation of reproductions will constitute compliance.

Unfortunately, we have no source, we have many sources, and there are of course other state laws and court rulings on reproductions that support reproductions. I just want you to know there is no question, and therefore you can confidently use electronic imaging. I just caution you, please use, develop inspection and quality control.

The reproduction of original paper after reproduction. Some people have asked me to identify what paper you cannot destroy after reproduction. The answer is, where the original records are required by law. Where is that? There's a few scattered statutes out there that refer to original paper records or original records. Very few and far between. No recent statutes use those types of language, with a few minor exceptions. Basically these are old laws, 30, 40 years old, that happen to still be on [00:12:00] the books. Anytime you encounter a law that says you shall keep records, you may keep those records in any form.

Records with intrinsic value, such as stock certificates, bonds, cash, negotiable instruments, those types of things. Those are obviously to be kept in original form. Cash, you don't go to a copier machine with a dollar bill and then pass out copies to your friends who take it to the local nightclub. A check made out to cash, make copies and take a copy to the bank once a week. No, that doesn't work very well, and that'll end you up in the pokey, so please don't do things like that. Most of us realize the original stock certificates are important, although today we rarely touch stock certificates.

Documents with the original signatures or handwriting that may be significant. The most prominent in this class is wills, where somebody will have a handwritten will and as part of that will it's important to be able to do handwriting recognition. There may be other types of documents that have been written out by hand that become exceedingly important. By the way, this is not historical value. If you have handwritten documents from 200 years ago obviously they have some historical value, but you have no requirement unless you're in the government domain to keep something like that. In the private sector, you will not have requirement to keep those types of historical records. There are occasionally documents where the original writing becomes important. [00:14:00]

Last but not least are promissory notes. Yesterday I did a quick search to see what still might be on the books, and I did find federal mortgages, Fannie Mae mortgages and HUD loans, that require original loan documents. Please do check for your specific requirements. Years ago student loans used to fall in this category, and they changed the law approximately ten years ago to allow banks and other financial institutions to keep reproductions instead of the original. Typically, those who have to keep the original have a requirement to stamp the original and return it to the borrower, but this applies to financial institutions and probably doesn't apply to you.

There's a few others, for example in county in particular, stamped engineering drawings with the signature or initials of the engineer become critical. Original records that have color on them, like engineering drawings or wiring drawings, have no meaning if they're in black and white after being scanned. If you're not scanning in color it becomes important, therefore you might have to keep the original paper. Then there will be a class of things which I'll call optional, which are documents of high value. Some organizations will establish a plateau where contracts, for example, over ten million dollars or a certain dollar amount will be kept in a fireproof safe in original form. That's not a legal requirement, but they feel safer, there's so much money involved and it's not a huge amount of documents. You can make decisions [00:16:00] like that, but please document where you draw the line, what the decisions are, and make sure that's available into the future in case there's questions.

Now the question of ESIGN. It stands for Electronic Signatures in Global Networks. It was in fact adopted in 1999, the same year as UETA was approved as a uniform law, but it was adopted before UETA. How it differs is that it was adopted by the US federal government and many other countries. It's an international provision between countries. It's similar to UETA, except it's related to electronic signatures and documents in international commerce. The main purpose was to establish unified form standards between countries as we get into electronic trade, electronic document management between countries, an exchange of invoices and purchase orders and other types of contracts, and establish the validity of electronic forms of those records.

The United States version of course allows electronic imaging and allows electronic records, and certainly can be viewed as allowing this within the federal domain also. It's not just a private sector provision, but it would defer to UETA provisions if there are conflicts. The United States federal government realized UETA would soon be adopted, its words were similar in goal, but [00:18:00] the exact wording was different. If there ever turns out to be conflicts between ESIGN and UETA, UETA will prevail. It's one of the few times in the history of legislation that the federal government has deferred conflicting legislation to the states. In most cases, if the federal government has a law and the state has a law and they conflict, the federal government will claim that their law is superior to the state's and try to enforce it. In this case, they deferred to the states.

Okay, let's go to a whole different area, and we're going to talk about accounting records and applying retention to accounting records. Some people ask straight out, "How long should we keep accounting records?" Four, five, six years? I would add seven, eight years, there's all sorts of answers. A very important question came in related to the handling of net operating losses. I tend not to talk about it. I am aware of it, and I've dealt with it in a few projects where it's come up as being an important issue. Again, a rehash of tax holds and how best to do that, what are good practices. Let's go over what are the retention requirements for county tax.

Five states in the United States have a specific six-year legal requirement for tax accounting records. By the way, I call them accounting tax records, tax accounting records, because these provisions are from departments of revenue. They are requirements related to records. Of course the US federal government has the Internal Revenue Service, Canada has Revenue Canada. [00:20:00] The objective is for them to have records supporting the tax return. What records are those? That's all your accounting records. It's accounting records that support your tax return, so I refer to them as accounting tax records.

These five states have a six-year requirement from the end of the fiscal year, and it's an absolutely requirement. IRS and the states all have limitations of assessments, and we call these limitations of action. They're actually a special form of limitation of action, because they are related to the tax return in particular, and auditing, when a revenue department can audit. It's from the due date of the return or the filing. Why do they have both of them? The filing could be extended later in the year. It's a general provision is three years. IRS and the states, just about every state has a three-years provision like this, must audit you within three years. That means start the audit, not complete it, as long as they start it. They can of course continue it, and [inaudible 00:21:19] basically will be in a position to look at all your records during that period of time. If they fail to start the audit within that three-year period of time, they are forever barred.

How should we have the list from a retention standpoint? Well, the year you file the tax return is after the fiscal year. We don't know if you're going to file it in March or get an extension, so we typically count that as one year. Then we add three more, or four. If you're not doing business in the five states listed on top, I didn't give you those [00:22:00] lists, I would be happy to provide those on request, you would actually have a four-year period you have to be concerned about.

Then there is a second provision that allows the departments of revenue to audit you six years after you file the tax return, or when the return is due, whichever is later, if you understate your gross income by 25% or more. What does that mean? That you earn, let's say, a million dollars, and you only report that you earned 500 thousand. This is not your taxable income, it's not your net income, it is your gross income. All the money you received, all the money you put in the bank. You know what that is, IRS knows what that is. If you're a publicly held company, you want to brag about it to let everybody know what your revenues were. Nobody does that. Nobody's going to understate their gross income by 25% or more, so this provision is mostly to catch people like drug dealers, who are not reporting their income properly. That's how they got Al Capone, historically.

Fraud, willful evasion, tax evasion, they can audit you forever, but only in this case will the Internal Revenue Service or the departments of revenue be responsible for the balance of proof. They have to prove you're guilty, as opposed to all other tax dealings and all other tax returns and things like that, where you are pleading guilty in advance. You're guilty until proven innocent. In the case of fraud, you are [00:24:00] innocent until proven guilty. That's a hard thing for IRS or any of those to prove, especially with good corporations who are properly maintaining their accounting records. IRS and the states also recognize capital gains, loss, depreciation, and that's going to be an active plus period, so active plus six typically is what we're using. The active period is while the tax event is current, so while you own the property, while you're depreciating, things like that, plus the normal tax period. That's also recognized.

We have this special issue called net operating loss, and it's particularly important in areas like petroleum, where you drill a well, it's very expensive in year one, and year two through 30 you hope it produces. You want to write off those expenses in future years when you have revenue that matches it. How is a net operating loss created? An organization has a loss from the business activity, as I said, example an oil company drills a well, they have a loss, it's expense. This loss is not fully offset by profits or gains in the tax year. Let's say the well cost a million dollars to drill, you got revenues of 50 thousand, you still have a net operating loss of 950 thousand dollars for that year related specifically to that well. You also have to consider some of your other revenue, what's happened, so we do look not just at a particular entity or particular [00:26:00] operation, but we're looking at losses versus revenues.

You can offset a certain part during the year, and some of it, the rest of the loss, can be carried forward. You can carry forward, in my example, which is just a very general example, it probably is not realistic, but it does point out a number. 950 thousand dollars of loss can be carried forward to future years, and you can write it off each year against some of your other gains. If you get 500 thousand dollars in revenue the next year, you can write off 500 thousand dollars of that loss, or however those particular rules work. Sometimes there's limitations on that.

What is the record-keeping implications of all of that? I had to rewrite this section three times so I can explain it. IRS can audit the tax year when the original loss occurs. It can always go back, and go back to that original year, the year you drilled the well, and audit the loss that you said you incurred during that year. If you recognize a loss carry-forward, you carry forward that loss, in any year you're subject to a tax audit. In what years would you be subject to a tax audit? We just looked at it, they can go normally three years to audit you. IRS can only change the loss carry-forward during the audit period, which is typically the last three years, but it can redetermine the original lost amount.

For example, I said the loss was 950 thousand. They said, "Wait a [00:28:00] second, you had these other revenues, you didn't write this off properly. Your loss was actually 100 thousand, and six years ago you took that loss of 100 thousand, so today you can't write off any more loss." That's the way IRS would handle it. They

cannot change the amounts you've written off four years ago, six years ago, etc., but they can say the original loss was wrong, and here's the new number. They could look at what you wrote off, and then say what you're allowed to write off in returns subject to tax audit. Unfortunately, you need all the records of the tax year of the original loss until the loss is carried forward and is written off, plus the normal retention period. You need to be able to show what that original loss was, what your incomes were, what your revenues, what the losses were. Talking with an accountant the other day, that means you have to keep all your records. If you have a net operating loss, please be aware this is an exception to the rule.

Here's a summary. Six years for general accounting, active plus six for capital accounting, property investments, etc, where the active period is you keep those records until the property is sold or scrapped or depreciation ends. If it's an asset, like a stock, until you sell it. That's the active period, plus six more years. Then if you are dealing with this net operating loss issue, you have a couple choices, and let me try to explain them. One is active plus three. What does that mean? You keep the [00:30:00] original records while it's active plus three more years, or six, whichever is longer. Let me put that in perspective. If you have the original loss in the year 2000 and you've written it off by 2005, you don't need, then, the records of the original loss after 2006. You would have gone six years from when that occurred.

Of course, you may have some other property issues for capital property that you may want to keep records of the property depreciation, depletion, and things like that, but you don't need those original records. You still have to keep those records totally at least six years, because that's your normal retention, and you may have to keep capital property records active plus six. If there are the general accounting records could be destroyed after the six, and of course in 2016 you don't need the net operating loss records from 2000 if the loss has been written off years ago, more than three years ago. I know it's a little complicated, but please check with your tax attorneys on that, or tax advisers.

The other choice, though, I think is a little simpler. Just place a audit hold on the loss year until the loss is written off. Just place a hold on it, and then when the hold is removed it just gravitates to its normal retention. Just keep normal accounting procedures, normal general accounting, normal capital accounting, and then just put [00:32:00] a hold on the years where you have a net operating loss. When the loss is fully recognized and three years go by, you can remove that hold. That's probably the simplest way of handling it, and of course, I want to say accounting management reports, keep those for a maximum of three years. There's no requirement to keep year-to-date accounting reports and things like that.

Three-year presumption, an update. For those who have not followed the three-year presumption, it basically says that records that are required by law to be kept, so that you find the records that the law says you shall keep, where there's no retention period stated, there are no retention periods, the records can be safely destroyed after three years. That's a three-year presumption, I take credit for it, I invented it, and it's based upon two ... or actually, three big issues.

Number one is certain specific laws. If you recall, I did want to return to the Uniform Preservation of Private Business Records Act. In four states it's called the Uniform Records Retention Act, and those four states are in red. Basically what it says is unless expressed provision is made by law for the period during which they must be preserved or for the conditions upon which they may be destroyed, business records of persons by the laws of this state are required to be kept or preserved, may be destroyed after the expiration of three years. [inaudible 00:33:48] making of such records without constituting an offense under such laws. What does that mean? If the law of the state requires you to keep records, but there is no requirement, there's no [00:34:00] express

provision in the law, that indicated how long it must be preserved, they may be safely destroyed after three years. That is the law in these eight states.

The four in red are under the Uniform Records Retention Act. When I was chair of Regulatory Affairs for ARMA we changed a few words, and actually ARMA chapters got with their state legislature, got those enacted in those four states. I had the privilege of testifying in Colorado, and prior to that, under the older law, there were four states that had previously adopted it. Obviously not all the states, but this sets a position of at least eight states says this type of approach is correct.

Then we have the US Federal Paperwork Reduction Act. I've written extensively about that. One person a week ago pointed out that the citation that I'm about to talk about was actually slightly changed, and here's the current citation change, if you want to look it up. Basically a United States federal regulation with a retention period of three years, actually, it should be three years or more, is not enforceable unless the retention period is proved by the Office of Management and Budget. That was true about 20 years ago, it's true today. When an agency develops a regulation but does not state a retention period, OMB will not approve it and it's not enforceable. You don't have to follow it. Even though the regulation actually got published, it is unenforceable.

The wording in that section [00:36:00] says, "Unless the agency is able to demonstrate when it submits it to OMB that such character of the collection of information is necessary to satisfy statutory requirements, etc., OMB will not approve a collection of information requiring respondents to retain records other than those listed for more than three years." OMB won't approve any requirement longer than three years without substantiation, and the areas where they create an exception are actually areas where we do have laws that establish retention periods, so I'm not really concerned about those exceptions.

Collection of information. When you have a record-keeping requirement and you are required to keep records, you are doing it for the betterment of the agency, the agency can then go and audit you. The agency is forcing you to collect the information on their behalf, so it does fall in. Now, if the agency does not request a retention period, it cannot be over three years, because of the Paperwork Reduction Act. What do you do if it's not a federal regulation, or you're not in the eight states? You keep records for a reasonable period of time. We now have enough information that three years is reasonable. There's no information that says it's not, and in particular three-year presumption was a big deal back then when I first discovered it and let it be known that there was such an idea, because prior to that attorneys would read laws which stated [00:38:00] you shall keep records, so no permission to destroy it, and therefore they require those records to be kept forever.

Their analysis was incorrect. If you had a requirement to keep records, you don't need permission to destroy it. However, if there's a requirement to keep records for longer periods of time, you have requirement to comply and then you may destroy it immediately after.

Records retention, let's move on. How often should we review and update the program, how can we stay informed of changes? There's a whole slew of records issues that came up. There were questions about compliance, how do we get people to comply with the program, what should a custodian do before they throw away records, what's their concerns? How do you set up audits, and an interesting question about applying retention in the Cloud. Let me summarize all these areas in a few simple slides.

How do you protect yourself from legal challenge on records retention? I've preached this for decades, the program must be systematically developed. That includes comprehensive legal research, full coverage of the records of the organization. I recognize that you will not be able to identify every record, and this is an ongoing

process, but you should certainly cover the main records of your organization. For example, a retention program in your accounting department is not adequate for the rest of the organization. That's the point of that line. The program must be reviewed at least annually; you may not make changes [00:40:00] annually. If you're following our legal group concept, then even when laws change it's rarely necessary to change the retention period, but the retention period does change periodically, so it's important for you to be looking at it.

The program has to be systematically implemented, then. Nothing sadder than a good retention program sitting on the shelf. Destruction must be performed under the program. You must have audit to confirm compliance, and you must have coercion. I know we hate coercion to make things happen, but records retention is an important policy of the organization. Individuals who don't participate are creating exceptions, inconsistencies. We have seen that these types of inconsistencies can get an organization into trouble and litigation. Why were some records destroyed under the retention program, while records I'm interested in, which are similar in nature, still exist in other departments? Why is that? What is the company trying to do to cover up?

The reality is, you need that coercion, but you certainly need that audit. That audit is critically important to be able to confirm your retention program works the way it's supposed to, and therefore the program and implementation, including the audit information, needs to be documented. I've generally said you need ten years of records of what your program was in compliance. There's no hard and set rule. You don't have to keep all of it, you're just trying to show a long history of compliance with your own program.

Legal holds, many of you are already familiar with this so I'll go through it very quickly. [00:42:00] The most important point is the legal holds operate independently of the retention program. You do not take records subject to legal holds and put it into another category in your retention schedule. The records retain the same quality, same character, in your retention program throughout its life cycle. Instead, what you're going to do is put a hold on certain records as necessary. You identify the records or documents subject pending or imminent litigation, government investigation and audit. You do that, you meet with your attorneys. This is tough for them, but it's worthwhile to set up a formal process, get them to participate, because it works to their benefit, it'll work to your benefit too. Basically to identify which records are subject to hold as soon as possible. Not at the time of destruction, but the time you become aware of the litigation or pending litigation.

You then basically identify those records, you put holds on the relevant records. They are prevented from destruction, even if they could be destroyed under your retention schedule. Let's say the records have a six-year retention. After about three years into that period you have litigation. There are holds on those records. Litigation goes on for four more years. After six years after the creation of those records, or the tax year, those records would normally be candidates for destruction under your retention schedule, but the hold says no, these records cannot be [00:44:00] destroyed because they're being held for litigation. When the hold is removed, litigation is over, you will then be able to destroy records whose time is up. You need to manage the holds. The creation of them, updating, and removal. There are many types of software in the electronic document management domain that makes it possible. Much more difficult in the paper world, but it's important issue to get a handle on.

By the way, destruction of the records is permitted when the holds are removed, assuming the retention period is up. One of the keys, though, to make this all work is the approval of destruction. I'm still finding organizations that are very weak on this particular issue. It comes time to destroy records, and they are following the old, archaic approach, as I describe it, of authorization for destruction. I don't recommend it, as you see, because individuals within the organization must specifically approve the destruction before it is permitted to go ahead.

Now, why were they doing this? Because some records were subject to litigation. Well, if you have a good hold system, all the records subject to litigation are being hold and they are not candidates for destruction. What is going to be found on authorization for destruction? Probably nothing. Nor can an individual go through a stack of 200 pages listing records and figure out what's heads or tails, what's covered by litigation. You can't do this at the time you're about to destroy records. [00:46:00] That's why the hold program is so important, to do it proactively as soon as you hear about litigation, it's pending, it's imminent; not at the time you're about to destroy the records.

The preferred method to start with is notice of destruction. You provide a list of your records for destruction to those who have to know, department, tax attorneys, whoever. They can request exceptions, but those exceptions are rarely approved because those exceptions are typically, "The records are covered by litigation, we didn't catch that before." Then you modify your procedures for legal holds to do that better. Records being held are not candidates for destruction, and therefore they don't even show up on the list. It's a list of records that can be destroyed with no reason to withhold approval for destruction.

I notice that destruction does not, however, require approval, and therefore destruction proceeds unless somebody raises a red flag. After a while, we hope, some of the people in your organization get tired of these notices, maybe you post them on your intranet if you really must do that, but there's no notice of destruction or no approval. It's recommended when the hold system is put in place, it's working well, you audit it, everything's fine, and the results are the best you can get for a retention program, results are the most consistent retention. An authorization of destruction is the worst choice, even though so many organizations have viewed it as the best choice. Many people who must approve destruction do not approve it, and also it encourages people [00:48:00] not to participate in the hold system because they'll have a second chance when the records are about to be destroyed. Holds should be put on immediately, not later.

Next topic, privacy in records retention. This comes up all the time, especially for a company dealing with an international retention issue. Let me give you a real rough definition, and through the next couple slides I'll do a couple definitions. They're all pretty rough, I'm not saying they're definitive. Just want to convey the ideas. Privacy deals with the protection of personal and personally identifiable information. PII is commonly the abbreviation used. What would that be? That would be, for example, on an invoice, the name of the party, or a sales slip, the name of the party, the address, phone number, credit card number, etc. It would not be, for example, the particular product purchased, the amount paid, and things like that which are not personal.

Our records retention deals with the period of time for keeping records. That's just a very short and dirty explanation of it, it's obviously much more elaborate than that. What's the impact of privacy on records? Privacy laws may limit the period of time to keep records. You may not keep certain types of information longer, because the fear is if you keep it longer you might violate somebody's privacy. In Europe, for example, they have many laws even on employees that say some of the personal information on employees can't be kept longer than five years. [00:50:00] In the area of pharmaceuticals, if there is a drug that is being tested in clinical trials, the individuals participating, their personal information can't be kept longer than five years. Those are periods of time that I've encountered over time. There are certainly others.

Retention laws, however, set the minimum period you must keep the records. You shall keep records six years. You can keep them seven, you can keep them eight, but you can't give them five. It states the period of time you must have the records at least that period of time. Therefore, these two may sometimes conflict. If you're doing an international schedule, in previous webinars I've talked about strategies on international schedules. If in Europe you have requirements you cannot keep records longer than five years and in the United States those

same records you must keep them at least six years, I have no solution to that problem other than in the United States you keep them six years, and in Europe you keep them five years. Therefore, you need to deal with that in your retention schedule.

Alternatively, I have recommended to a number of organizations not to establish one global retention schedule, but instead establish a US or US and Canada based schedule, offer it to the other countries. If they have an add-on let them do it, or an exception, let them do it in those other countries. This, however, creates a huge problem in a global information management system or a global accounting system, and you're going to have to come up with creative solutions on how to deal [00:52:00] with these types of problems.

Next issue, applying retention in the Cloud. With Cloud, obviously it's somewhere on the internet where some service provider is providing you some service, storage, etc. Number one most important thing about applying retention in the Cloud is first apply records retention on earth. Before you get into it, set up your program in a domain where you have complete control, you have your hands around all the records clearly in the paper world, and as you expand into the electronic world. All-important. Then you can deal with the Cloud problem. You need to accept the principle that the retention program should apply to records wherever they reside, regardless of form. If the records are on your [inaudible 00:52:58] or if they're in the Cloud, doesn't matter. The retention applies to those records.

Now, you need to implement retention in the Cloud application, and my recommendation, if you can't or don't, don't put the records in the Cloud. I know this is tough love, and I know your IT people will frown upon it, but why get yourself into a system where you cannot apply the rules of retention that you so diligently worked on and developed for your organization just because it's the Cloud? Don't use the Cloud until the Cloud does what you need it to do. The service provider must therefore provide you with retention capabilities that you can apply to your records. Don't take shortcuts.

[00:54:00] If they can't apply retention in a responsible way, the way you do within your organization, my answer is don't use the Cloud, and don't do what IT has done all along. "Let's put the records in the Cloud. Let's develop new systems, and then we'll figure out how to destroy it." We continue to have problems with software solutions, SAP, PeopleSoft, etc, where the vendors develop great products to create, manage information, use it for the betterment of the organization, and some of those vendors did not spend even a moment on how to get rid of it. Now they're confronted by their customers with these problems. The solutions are coming, there are some interim solutions. Don't put it off. Don't develop a new system, [inaudible 00:54:58] put information in the Cloud until you're able to manage it, and managing includes applying retention and destroying it.

You do need to check with the service provider that the destruction or backup practices, what do they follow? What do they do? When you destroy, they must destroy too. The only exception I can think of is if they have a 30-day backup cycle, and you destroy records on the first day of that cycle. It may be 30 days before that last tape is recycled by the service provider, but make sure you understand the policies, what they're following, and that it does conform to your needs, or find a service provider that does, or don't use them. That's my conclusion.

Litigation protection, some people asked me about that. The best protection you can possibly deal with is [00:56:00] to manage your records and information. Know what records and information you have, know where it's stored. That puts you in the best position legally. Develop, and implement of course, a legally defensible retention schedule. Know what you don't have because it's been destroyed. Know that you've destroyed information properly, that you have good procedures, and that you can demonstrate compliance with the program. That's where audit comes into play, becomes particularly important.

The last area I'm going to deal with today is an area where I get a lot of questions, information governance versus records and information management. What is the difference? Is this a new concept, is this an old concept? What gives? I'll give you my perspective. I'm sure some of the information governance gurus may have a slightly different view, but let me give you my 30 ... actually, going on 40 years plus experience in some aspect of records and information management. I'll use Wikipedia's definition, not the definitive source but it popped up first when I was preparing this presentation and doing the Google search.

What is information governance, according to them? It says it okay. "The set of multi-disciplinary structures, policies, procedures, processes, of control." Multi-disciplinary, it not just records management. A whole group of people. IT, legal, the [inaudible 00:57:45], you name it, everybody's involved in all of this. Implemented to manage information at enterprise level. We're not just doing it in a department, we're doing it across the entire organization. Everybody working to deal with all the information [00:58:00] at the highest levels of the organization.

What is records and information? It's "the professional practice of managing the records of an organization through the life cycle, from the time they are created." I would add through maintenance to their eventual disposal. The life cycle of records, we try to manage it and things like that. One level there's similarities. What is that? Well, both seek to manage the information of the organization. Both are trying to manage it with different approaches at sub-levels. Information governance includes more people, all systems, all information, all data at an entire organization. Its goal is to be comprehensive from the beginning.

Records and information management historically is to manage records as it could and it was able to. Include some records, little or no data, because rarely got into the electronic side although we should have, few systems. The program is managed through the records management group, probably legal is involved, and we get some cooperative parts of the organization who participate, but there's not an organizational-wide effort to make this all happen and put it all together. RIM, if it was fully implemented, would be a lot like information governance today. That was a goal, and some people actually met that goal. RIM rarely got the full support of upper management, rarely controlled all the enterprise information, but successfully managed some of the records, leaving [01:00:00] many gaps while, while information governance strives to manage all of it.

In the end, information governance strives to encompass the entire organization and all its information. That has been a goal of RIM professionals all along, but it's been difficult to achieve. Information governance has the support at the highest levels of the organization, with a total plan to manage all information and all data. It is hopefully successful, and of course records and information management is all part of the same thing.

That really covers what I wanted to cover today. I appreciate you coming to today's session. I apologize for the glitch at the beginning, we tried to do the slides slightly differently and it didn't work, and we won't do that again. This presentation will be posted on the internet in probably a week, and on our website. Also, there will be a transcript of it and all the slides will be made available. If you have any need for additional information or just want to discuss more of what we do, you can contact Andre, I've given you his phone number the website. Therefore, that ends today's session. I appreciate you all coming, and we look forward to having you at future sessions. Thank you.