

How to Protect Your Records by Really Trying

By John Avellanet, Managing Director and Principal of [Cerulean Associates LLC](#)

Reprinted with permission from SMARTERCOMPLIANCE™ 2(2): p 1,4-5 (February 2008)

Records are a double-edged blade. They are the emails, memos, databases, standard operating procedures, reports, presentations and to-do lists that we rely upon to detail deliberations and document decisions .

Records are also the means by which company executives are convicted by the courts and exonerated by inspectors. Records are proof. To ensure compliance and prevent financial loss, you must protect this proof.

Confidentiality Declarations

First and foremost, guidelines need to be established around what type of records can be said to be (and marked as such) “confidential.”

If every record is “confidential,” then no record is confidential. The term has lost its significance.

Therefore, work with your legal department to draw up a list of record categories that automatically classify as “confidential.” Examples include new product concept documents, product formulations, schematics, and reports, memos and presentations on un-launched marketing campaigns.

Likewise, be clear about records that should never be marked confidential—task lists, draft training presentations, corporate-wide policies, and day-to-day, regular internal emails.

By and large, standard operating procedures that do not deal with your intellectual property or trade secrets should not be marked as confidential (see “Saving Intellectual Property,” in February’s [SMARTERCOMPLIANCE™](#), volume 2, issue 2, for details on how to handle intellectual property aspects within standard operating procedures).

Your computer (IT/ICT) department should then use the confidentiality typology to set core, base security on your electronic files.

Confidentiality guidelines should be part of your overall organizational records management policies. Other aspects of your records management infrastructure include:

- Retention guidelines;
- Regular reviews;
- Personnel roles; and

- Litigation response plans.

The key point to remember is that records do not start their retention period (2 years, 7 years, and so on) until the activity they are associated with (such as a project, a manufacturing lot, a clinical trial, etc.) is complete.

For instance, if you are to retain project files for 2 years, when your project ends, you retain those project files for two further years (*i.e.*, a three-year project ending in 2008 would have its records retained through 2010). At that point, determine if you need to retain those records further (perhaps due to a lawsuit or personnel action) or throw them away.

A further example: records, such as batch records, of a Phase I clinical product or API. Those records have a retention period of two years. That two year period starts *after* the clinical trials are over (not after you finished producing it) or *after* you have withdrawn your IND.

Regular Records Reviews

Reviewing records on a predetermined basis—those still in use and those in retention (*i.e.*, archived), is absolutely crucial to being able to use your records as proof.

Consider scheduling a quarterly or annual review period that is company-wide and officially announced. This will help avoid the Arthur Anderson/Enron embarrassment of suddenly announced “reminders” of records retention policies.

Ensure that you review all your emails, draft documents, final reports, and so on with an eye to keeping only those things you need. We often advise our clients that if you find a record that is not required for any legal obligations and is not part of an active project or process, ask yourself two questions:

1. Is the record more than one year old?
2. If it is older than one year, why am I keeping this?

If the answer to number two is “just in case” or starts with “well, but someone might...” then toss the record.

That is a hard moment. Old records bring back memories and earlier achievements. Trying to decide if you should get rid of an old record or keep it just a bit longer is something that all of us struggle with—even former records management executives.

I advise my clients who hesitate to throw records away to do two things:

First, consider that someday, you may have to defend that record to a court or to a skeptical auditor or to an outside investigator who will be looking to twist your reasons. Are you really sure keeping that record is wise? Are you sure that you will remember your reasoning five years from now on the witness stand in a courtroom with jurors and the judge looking at you,

waiting for you to hesitate (and thereby look like you're trying to hide something)? I can tell you from experience – this is not something you want to go through. Toss the record.

If that does not do the trick, then I ask my clients to watch the first five minutes of the 2002 movie, *About Schmidt*. There is a sobering moment when, after watching the main character carefully characterize and sort of all his files (and use the phrase, “Someone might want to...” in reference to all those records), after he retires, we catch a glimpse of all those records – that proof of his successes and efforts – sitting neatly stacked by the dumpster.

Lawsuit Records Response Plan

Eventually, almost every company is taken to court and here is where the concept of records as proof comes to the forefront. Your records will either exonerate you or convict you—and properly managed records are more than likely to help you.

Work with your legal department to craft a “discovery” response plan. This plan forms the basis of how you will manage records during a possible lawsuit (and any appeals). Personnel will need to be trained on the plan, and audits will need to be conducted against the plan to ensure it is being followed.

Do not make the same mistake many companies have and forget to include your IT/ICT department and other support groups in your company's plans. In the past, judges have levied heavy (\$30 million+) penalties against companies who were supposed to be saving electronic documents, only to find out that the IT/ICT departments were never informed or trained.

Response plans to lawsuits are very complicated given the complexities of business today, from outsourced suppliers and departments, electronic and paper records, emails, employees who work at home, and so on. Consider bringing in an outside expert to conduct a workshop on best practices and then help you craft a consistent policy and strategy that gives you the best chance for success. Mistakes in this arena are too costly to “go it alone.”

Final Thoughts

Even if you are never taken to court, the same principles of good records management and protection apply to dealing with auditors and investigators. Managing your records is not an exciting task, but it is a necessary one.

Are you ready?

About the Author

John Avellanet is a former *Fortune 500* subsidiary C-level medical device and biotechnology executive where he created, developed and ran his firm's Records Management and IT

John Avellanet

departments. In 2006, he founded his independent consulting firm, Cerulean Associates LLC (www.ceruleanllc.com) and has since become one of the leading experts on cost-effective compliance and trade secret protection.