



Records Management Networking Forum

Minutes from the meeting 25th November 2008

At The offices of
Charles Russell
New Fetter Lane

This document is private & confidential. Therefore, all information contained within this document is provided in confidence. It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without the express written permission of Legal RM and shall be held in safe custody.

Version 1.0
Date: 28th November 2008
Prepared by: Keith Dacey
E-mail: keith@legal-rm.com

© Copyright Legal RM 2008. All rights reserved

Records Management Networking Forum

Minutes from the meeting 25th November 2008

Overview

The Legal RM Records Management Networking Forum is a quarterly held event designed to allow professionals from leading professional services and law firms meet two main objectives:

.... **provide a platform to network & discuss pressing legislative & operational issues**

.... **build a community based on common interests & concerns**

Legal RM are proud to have hosted this event in conjunction with Charles Russell and would like to thank them for their warm welcome.

Forum Discussion: Management of Electronic Records

The discussion was facilitated by Keith Dacey of Legal RM, who raised issues in the form of a bullet pointed Powerpoint which is available through this site. The discussion ranged widely across all aspects of the management of electronic records, and included IT representatives as well as records managers from law firms and other professional organisations.

How many people in the room are involved in an electronic RM project at the moment?

(6 hands)

Guidance and standards appear not to apply to the legal sector, more a risk management exercise for individual firms. Little help from Law Society. US case law and legislation much more well known than any UK equivalents.

How do you manage email storage?

- Is limiting the size of inboxes the right answer? Possibly, some firms currently attempt this. Often overridden by fee earners with clout. There are problems with large attachments which are not handled well by document management systems and can rapidly erode any inbox limit.
- Not allowing the same email to be stored in to the EDRMS more than once. Functionality now exists, but the jury is still out on bulk profiling methods.
- How can you enforce policy when fee earners refuse to comply? Must be driven from the top. Not an IT infrastructure issue but a genuine risk to the firm.
- Review policies and educate end users
- All work related e-mails need to be assigned a matter number, if an email does not have a matter number then it is questionable as to whether it is necessary to retain it, and probably better to delete it.
- Is Exchange responsible for proliferation of information, we only need to keep one final version?
- It appears that the use of e-mail has bypassed Exchanges capability to deal with it. It is important to see exchange as a production environment, in the same way as the document management system and not a long term storage or Records Management equivalent. We look forward to developments from Microsoft to address the shortcomings in the current Exchange application.

Is Instant Messaging a valid form of legal communication when it is hard to capture the information?

- Microsoft have developed a corporate IM application. No one at the forum currently uses this, or has plans to. IM has a bad reputation and needs to be shown to be a valuable transactional tool.

Retention and Risk Management Policies

There was a general discussion around retention of electronic documents and the associated risks.

- How do you destroy Electronic Information, who does the responsibility lie with? Very difficult to destroy. Often Forensically recoverable. Many recursions of backups. Case law in the US suggests that 'best efforts' rule applies and endless and expensive searching of backups is no longer valid if proper procedures can be shown.
- Ethical walls within a DM system, who really has them and are they fully operational? A policy is needed to secure emailed documents. This was a significant split among the members. Those that did have security around documents admitted that 'save as' bypassed this security and control was lost altogether once a document was e-mailed.
- To mitigate risks of security breaches there should just be one point of entry to electronic documents. Good RM practice dictates that a single record copy should be retained.
- You have to prove that policies have been adhered to, if the retention policy states that the information should have been destroyed and the documents made undiscoverable this will prove sufficient (see comment on backups above).
- Legacy Data – information which is not catalogued can't be destroyed as you don't know what it is. There was much support for disposing of this data immediately, but it is hard to translate these good intentions into action.
- A record can be maintained of destruction dates
- Historic documents should not be offered out. Varying views expressed from the floor. There are organisations such as National Archive and British Records Society who will take historic documents on loan, catalogue them and make them available for research. Does this breach client confidentiality? Some thought so. If client cannot be located, then need to retain documents and not publish them.

Practical Issues

Clients have a right to know how long their records are going to be retained. This should be agreed 'upfront' on the creation of a file. Some clients will specify minimum retention requirements, others will expect eternal preservation. Need to balance the risks before agreeing to terms. Possibility of returning papers rather than destroying them can be limited by the need to only return the clients property.

Paper records should be 'thinned' out before they are archived and fee earners should be encouraged to adhere to this. How are you able to do this if emails are still being printed and filed?

Best Evidence – Print and delete policies.

Test case – Batt v Rowe

A printed email is NOT best Evidence (Case notes available)

- Print and Delete is dangerous as you are removing an email from its original context. It cannot be a proper record. Metadata and audit trail is lost.

Who does responsibility lie with for RM in an electronic context?

The clue is in the job title. There has to be a Records Management input to these decisions. The IT department can not be aware of all issues surrounding all the systems they implement and maintain. what responsibility do archivists have, where does the responsibility start?

Overall responsibility lies with the IT department as they support and implement the systems which support the process. Management of electronic records should, on a practical level be almost automatic. It should be possible to construct a rules based approach which limits the need for human intervention and thought. The construction of these rules(based on Client, work type, document type etc) should be a collaboration between Records Managers, Risk Managers and the IT department.

It would be simpler if the rules were clear, but there is a distinct lack of guidance and regulation. The technology is clearly outstripping our ability to control and manage its output.

The meeting closed at 6.30 and the discussion continued over dinner at a nearby restaurant.

About LEGAL RM

Legal RM have over 30 years experience working with professional services and law firms in the field of risk management and compliance. Partnering with industry leading technology organisations and information providers, Legal RM are able to offer unparalleled products and services to assist firms in key areas such as Anti-Money Laundering, Records Management, Conflicts Management and Information Barriers.

For more information, please contact:

Legal RM
+44 (0)207 193 4090
info@legal-rm.com