Solving the Email Challenge

Effectively Managing Emails as Documents of Record

White Paper

MDY Advanced Technologies, Inc.

Galina Datskovsky, PhD, CEO
Mark Moerdler, PhD, President

© 2003 MDY Advanced Technologies, Inc.

Table of Contents

List of Tables

© 2003 MDY Advanced Technologies, Inc.

Introduction

> *"Every type of organization needs to consider, more than ever before, the potential damage that can be caused by casual Email that is not properly managed. Email should be regarded as, and considered no different than, a signed hard copy correspondence.*
>
> *The organization must know what Emails have been sent or received, as well as their contents. Without a centralized structured environment for managing this information, the organization assumes great risk."*
>
> Maurene Caplan Grey, Gartner Group

Organizations are increasingly worried about managing their documents of record, whether they are physical documents, electronic files or emails. Government agencies, lawyers, and the court systems are specifically targeting emails (both sent and received) as the key source of information regarding the actions of, and the reasons behind the actions of, organizations and individuals. The following real-world examples serve to illustrate this point:

- **Department of Justice v. Microsoft:** On more than one occasion, the testimonies of key Microsoft employees were refuted with their own emails.
- **Arthur Andersen:** Arthur Andersen was found guilty of obstruction of justice for destruction of Enron related documents in the fall of 2001. Andersen was fined $500,000 and five years probation. The damages to Andersen's reputation led to both a loss of clients and employees, and finally to their demise as a standalone company.
- **Fen-Phen Weight Loss Class Action Suit:** In the American Home Products Fen-Phen class action litigation, an internal email was found by the Plaintiff's lawyers and was perceived as sufficiently problematic, and it forced American Home Products to settle the lawsuit for $3.75 Billion.

In fact, recent case law is proving that attorney-client communications, especially emails, are open to discovery and may not be protected under attorney-client privileges:

- In the Enron shareholder-fraud class action suit, Vinson & Elkins' emails are discoverable.[1]
- In another Enron related case, the New York City Bankruptcy court issued subpoenas to over 45 US, UK and European law firms for thousands of documents, including emails.[2]

[1] "The Rising Heat on Enron's Lawyers," BusinessWeek Online, December 26, 2002 by Mike France.
[2] See Richard Tromans' "Magic Circle in Enron Files Threat" in Legal Week December 9, 2002. http://www.legalweek.net/ViewItem.asp?id=10564

© 2003 MDY Advanced Technologies, Inc.

- The Manhattan district attorney's office and the SEC are using recently discovered emails between Tyco International Ltd.'s employees and its outside counsel. These emails reveal that the law firm knew of improprieties at Tyco.[3]

The obvious question is: what should an organization do with its emails in order to assure that these documents of record are available as required by law? Before discussing how to solve the challenge of properly managing emails as documents of record, it is necessary to define records management.

What is Records Management?

> *Records Management is a set of standards and procedures that an organization follows to ensure that all of its Documents of Record are managed in accordance with legal, regulatory and business requirements.*

This translates into several key requirements:

- **Search:** The originals or copies of Documents of Record are available when requested.
- **Retention:** Documents are retained as long as required by law, statute, or regulatory requirements. In some instances, business rules require documents to be retained for longer periods of time.
- **Destruction:** Documents are destroyed as required by business requirements, but not prior to any legal requirements.
- **Hold:** If legal action, an audit or regulatory review is pending, then all related documents are not destroyed until after the legal action or review is completed.
- **Unedited Original**: With electronic documents and emails, one must demonstrate that the complete, original document of record has not been edited or changed.

Are Emails Documents of Record?

From the inception of email, the courts have argued over whether an email is similar in legal status to a signed document (or record) or to a telephone conversation. This is an incredibly important distinction, since a signed document has long-term legal status unto itself, while a conversation is considered transitory in nature, requires much more stringent proofs[4] of validity and is subject to privacy laws (wire tapping).

Starting with the Watergate[5] hearings, most courts have accepted email as legal records akin to signed documents. This position has only strengthened over time.

[3] See "WSJ: Tyco Lawyers had Early Concerns." December 27, 2002, Reuters. http://story.news.yahoo.com/news?tmpl=story&u=/nm/20021227/bs_nm/manufacturing_tyco_report_dc_2
[4] An overheard conversation is hearsay and not admissible in many instances in court.
[5] Even as far back as the Watergate investigations, emails were part of the discovery process.

© 2003 MDY Advanced Technologies, Inc.

Virtually every legal action today includes requests for all related emails as a standard practice. In many cases, the only legal proof has been within emails.[6]

Basic Management of Emails as a Record

Given the general issues of records management defined in the previous section, how does one apply records management to all emails (both incoming and outgoing)?

Legal Requirements

There is an enormous amount of legal precedent that an email has a legal status comparable to any other form of written correspondence - it must be managed with the same integrity, authentication and retention schedule as an equivalent paper document. This also means that the lifecycle of the email must be managed based on legal requirements, not at the whim of the sender or recipient of the email.

> *"[Organizations] shall treat email messages the same as any other record, and these shall be subject to all requirements of this Standard"*
>
> The DoD 5015.2 Standard for Records Management[7]

Furthermore, there must be an easy method for applying ***Hold*** to an email. Given today's litigious environment and the volume of regulatory requirements, one must consider and adequately prepare for possible litigation or regulatory review.

A regulatory review could be anything from an SEC investigation to a Human Resources issue. Most organizations do not realize that an employment issue ranging from employee rights, discrimination, sexual harassment or unfair hiring or firing will bring on regulatory review, and may necessitate supplying a wide range of documents as evidence, including emails.

In fact, most government and quasi-government agencies with regulatory or oversight responsibility have either implemented standards or are in the process of implementing standards. These include:

- The Security and Exchange Commission (e.g., SEC Rule 17A[8]) establishes records retention policies for brokers, dealers and Exchange members.
- The Government Paperwork Elimination Act (GPEA) "requires Federal agencies, by October 21, 2003, to allow individuals or entities that deal with the agencies

[6] In the recent $1.1 Billion case arising out of Enron in which Chase Manhattan bank is suing 11 insurance companies for surety bonds (*J.P. Morgan Chase Bank v. Liberty Mutual Insurance Co.*, 01 Civ. 11523). A judge has allowed the jury to see Chase emails that the judge has characterized as potentially "explosive"[6] and could decide the results of the case.

[7] Design Criteria Standard for Electronic Records Management Software, DoD 5015.2-STD.

[8] 17 CFR 240.17-a.

© 2003 MDY Advanced Technologies, Inc.

the option to submit information or transact with the agency electronically, when practicable, and to maintain records electronically, when practicable. The Act specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages Federal government use of a range of electronic signature alternatives." [9]

- The Electronic Signatures in Global and National Commerce Act (E-Signature Act of October 2000) says, "An electronic contract, signature or record is legally equivalent to a hard-copy contract, signature or record."[10]

- The recent Sarbanes – Oxley legislation[11] has long-range ramifications for both public and private companies and established criminal penalties for destruction, alteration or falsification of a record.

- The FDA has set a standard for electronic drug submission, CFR 21 Part 11,[12] which mandates that all electronic documents, including email, be managed as documents of record.

- After Operation Desert Storm, the U.S. Department of Defense developed the DoD 5015.2[13] standards to certify electronic records management software applications. This standard has become the national (and in many cases, international) benchmark.[14]

How and When Should Emails be Retained?

An email record (and its attachments) must be maintained in its original electronic format.[15] A printed copy of an email has lower status than its original electronic version, and a printed copy must be verifiable and proven authentic. For example, a Microsoft Outlook email must be maintained as an Outlook email with all headers, time stamps

[9] Statement of the Office of Management and Budget - http://www.whitehouse.gov/omb/fedreg/gpea2.html .
[10] Sean Doherty, "The E-Signature Act Makes Online Transactions Legally Binding," Network Computing December 10, 2001 http://www.networkcomputing.com/1225/1225ws1.html
[11] The Public Company Accounting Reform and Investor Protection Act of 2002 generally know as Sarbanes – Oxley was signed into law July 30,2002. http://www.aicpa.org/info/sarbanes_oxley_summary.htm
[12] http://www.fda.gov/ora/compliance_ref/part11/
[13] For further information on DoD 5015.2, a copy of the standard, and a list of the certified products one can look at http://jitc.fhu.disa.mil/recmgt/index.htm .
[14] Other standards, such as the United Kingdom's Public Records Office (PRO) Standard (http://www.pro.gov.uk/recordsmanagement), contain many of the same requirements as those included in DoD 5015.2. The PRO standard is based on the requirements as outlined in the "Modernizing Government" white paper written in 1999 which set a target that all UK government organizations manage their records electronically by 2004.
[15] DoD 5015.2-STD C2.2.6.8.8. **"**RMAs shall provide the capability for filed e-mail records to be retrieved back into a compatible e-mail application for viewing, forwarding, replying, and any other action within the capability of the e-mail application."

© 2003 MDY Advanced Technologies, Inc.

and attachments. This means that the email document must remain in a format that can be viewed within its native email application.

Outgoing email is a provably original document at the moment it is sent.[16] Therefore, an outgoing email must be captured as part of the send process at the very moment it is sent. This assures that it is the original, and that it has not been edited or altered in any manner prior to filing it as a record.

Why not just Print it all Out?

Some organizations and / or individuals print their emails and place the printed copies in their physical records. This solution does not deal with the legal issues related to managing the "original." There are several additional problems with a printed copy of an email:

- A printed version does not carry the same weight as the unedited electronic original.
- Printing out every email is a very labor-intensive process, which is rarely, if ever, consistently maintained.
- The cost of storing all printed emails would be enormous.

Why Not Just Keep Everything Forever?

Some organizations believe that the solution is to maintain all records, especially email, forever. This is based on a misunderstanding of the legal and regulatory requirements. Every document has a legal retention period associated with it (e.g., human resource records must be maintained for various numbers of years after an employee leaves the organization, unless legal action is pending). By keeping documents beyond their retention period, the organization opens itself up to numerous document discovery problems.

- **Cost of Discovery:** If an organization maintains copies of all emails forever and a legal action occurs in which specific emails are requested, then the organization will need to search all of its emails and supply only those that relate to the specific topic.[17] For example, an organization with 3000 DLT tape backups of their emails estimated the cost of finding and printing the required emails was in the millions of dollars.

[16] As stated earlier an email whether in an inbox, outbox or other folder can be edited without an audit trail that it was changed.

[17] Simply supplying the backup tapes is not recommended since it could supply non-relevant, but damaging, information. Furthermore, it is critical that one's own attorneys know exactly which documents are relevant. In the Justice Department v Microsoft case, the Justice Department was able to refute testimony by showing emails of which Microsoft's own lawyers were not cognizant.

© 2003 MDY Advanced Technologies, Inc.

- **Discovery of Damaging Documents the Organization Need Not Have Kept:** Kept forever, email records that could have been legitimately disposed of according to their retention schedule, would remain discoverable and create potential liability to an organization.

- **Cost of Litigation:** In *Murphy Oil USA Inc. v. Fluor Daniel Inc.*, the court stated, "Fluor's e-mail retention policy provided that backup tapes were recycled after 45 days. If Fluor had followed this policy, the email issue would be moot." As a result of Fluor's records retention, both parties in the action spent substantial time and money arguing over the discoverability of email messages that should have been destroyed.[18]

A Gartner Group research note published in December 2002 strongly states: "Retaining everything forever is unwise and costly, as is deleting it after 30 days. An all-or-nothing approach will not work and enterprises must have a good understanding of the legal and technical issues involved."[19] No solution can solve the records-related legal and technical issues better than a dedicated records management system.

Why Email Systems are Inadequate as a Records System

Since the emails and their attachments need to be maintained in their original format, many ask: "Why not leave the emails in the email system?"

Storing email records in one's email system creates numerous problems, including:

- **Search**: Email records must be easily found. To find all instances of an email, it must be searched for and found in each individual's email account.

- **Hold:** All email systems allow users to delete emails at any time and virtually destroy audit trails, even when a Hold requirement is in effect.[20]

- **Authenticity of Email Content:** Most email systems allow the user to move or copy an email into an electronic file (e.g., .msg file for Outlook), which can then be edited using a regular word processor. The modified email can then replace the original email without audit trails or easily identified marks to indicate that the email has been edited. Therefore, email systems do not meet electronic records requirements.

[18] Michele C.S. Lange, "Sarbanes-Oxley Has Major Impact on Electronic Evidence", The National Law Journal, Jan 2, 2003.
[19] A group of Gartner analysts, "Waves of Information Disruption Due in 2003," December 3, 2002.
[20] This is one of the many issues that arose in the Enron / Andersen document destruction case.

© 2003 MDY Advanced Technologies, Inc.

What about Other Solutions?

Why not Use an Email Archiving System

Archiving systems are not records management systems. In fact, the courts have made it clear that *"… utilizing a system of record keeping which conceals rather than discloses or makes it unduly difficult to locate"* documents may be equivalent to destroying them.[21]

- **Personal Emails:** Archiving systems often store all emails, regardless of their business or personal nature.
- **Retention:** Archiving systems store every email for a fixed period of time, rather than on an individual time- or event-based retention schedule, which is standard for all records.
- **Hold:** A records management system must have a Hold capability to ensure that records are not disposed of before or during a litigation, government investigation, audit or regulatory review.
- **Audit Trail:** When documents of record are destroyed, one must be able to prove that they were stored and destroyed according to the correct retention schedule. Archiving systems don't normally maintain this level of audit trails.

Why Not Use a Document Management System?

Document management systems are designed to manage the electronic document creation and development process and to simplify the sharing of documents. The very features that make a document management system effective are counter to the requirements of an email records management system.[22] A document management system often fails to meet the following requirements:

- **Retention:** Most document management systems have very simplistic retention capabilities (e.g., delete all documents that are 1 year old). Selective handling is very difficult or not available.
- **Hold:** Document management systems lack the ability to place email records under Hold and prevent editing or destruction.
- **Audit Trails:** Once a document is deleted, the audit trail is normally also deleted.

The differences in the various approaches to managing emails as documents of record are summarized in Table 1 on the following page.

[21] Kozlowski v. Sears Roebuck & Co., 73 F.R.D. 73 (D Mass. 1976).
[22] Document Management Systems need to be integrated with a Records Management System in order to meet these needs.

© 2003 MDY Advanced Technologies, Inc.

Table 1. Summary of Approaches to Managing Emails as Documents of Record.

	Email Systems	Email Archiving Systems	Document Management Systems with Integrated Records Management	**Records Management Systems**
Ability to provide optimal retention	None	Low	Low	**High**
Ability to maintain record authenticity	None	Low	Low	**High**
Ability to maintain audit trail	None	Low	High	**High**
Legal Hold Capability	None	None	None (without Records System integration)	**Yes**
Coverage	Broad	Broad	Narrow	**Broad**
Ease of searching and finding	Low	High	High	**High**
Built-in intelligence	Low	Low	Low	**High**
Total cost of ownership (for Records)	Medium	Medium	High	**Low**
Total reduction of risks (operational, regulatory and legal)	None	Limited	Limited	**Significant**

Conclusion

While maintaining only those documents that are relevant, organizations must manage emails as documents of records in order to meet legal and regulatory requirements. To do so, organizations must:

1. Separate relevant email records from non-relevant and personal emails.

2. Store the relevant emails and their attachments as records in their original format.

3. Store the emails outside of the email system as records to prove they are authentic documents of record.

4. Manage the life cycle of email records within a DoD 5015.2 Certified records management system.

© 2003 MDY Advanced Technologies, Inc.

About MDY Advanced Technologies, Inc.

MDY Advanced Technologies, Inc., has been providing state-of-the-art records, document and knowledge management solutions and enterprise-wide system implementation services to large and medium corporations, professional service organizations and government agencies since 1988. FileSurf®, MDY's exclusive records management solution, integrates all physical and electronic files - including emails - into a single, scalable and extensible enterprise-wide system. MDY's unique mix of software plus services gives organizations a single point of accountability in gaining complete control over their information management needs, reducing risk, complying with state and federal regulations, and effectively implementing knowledge management policies, best practices and procedures.

Galina Datskovsky, PhD, CEO

Dr. Galina Datskovsky is the Chief Executive Officer of MDY Advanced Technologies, Inc. Dr. Datskovsky is a pioneer and leader in the fields of records, document and knowledge management and has led MDY for more than 14 years of steady growth. She has guided companies in the legal, insurance, medical, financial and other industries in implementing innovative solutions to improve information flow and information management systems.

Dr. Datskovsky received her Ph.D., M.S., M.A., and B.A. in computer science from Columbia University. She is a Board Member of the Metro New York Chapter of ARMA (Association of Records Managers and Administrators) and is a highly sought-after speaker in regional and national conferences and trade shows.

Mark L. Moerdler, PhD, President

Dr. Mark Moerdler is the President of MDY. Dr. Moerdler directs the design, installation and maintenance of MDY’s records and information management systems for law firms, investment banking firms, real estate management companies, health services organizations and other specialized and sophisticated integrations.

Dr. Moerdler received his Ph.D., M.S., M.A. and B.A. in computer science from Columbia University. He has delivered papers at numerous international conferences and has been published in leading academic journals.

© 2003 MDY Advanced Technologies, Inc.