



Issues in Record Definition and Declaration

David C. Mills, Esq., CRM
Senior ECM SME
dmills@armedia.com
<http://www.armedia.com>
2/02/2010

Table of Contents

Overview.....	1
What is a Record?	1
Definitions	1
Records.....	1
Characteristics of Records	2
Non-records.....	3
“Declaration”	4
Issues Inherent in Declaration.....	4
Over-declaration.....	5
Under-declaration	7
Solutions	8
Comprehensive Records Programs.....	8
Senior Management Support of Records Management.....	8
Education and Training	9
Limiting or Removing the Record Owners Discretion	9
Conclusion.....	10
About Armedia.....	11



Overview

One of the most difficult problems in records management is the recognition of a “record.” Often the definition is misunderstood, and therefore misapplied, resulting in misclassification of items¹ as records. Because records are vital assets of an organization, misclassification can result in losses of intellectual capital, financial assets, and historical data.

This paper addresses these issues. First it defines what “records” and “non-records” are and describes their characteristics. It then describes how items become records through declaration. Next, it explores issues that surround the misclassification of records through improper declaration. Finally, it suggests solutions to these issues.

What is a Record?

Definitions

Records

Although the definition of “record” varies by locale, jurisdiction, industry, organization and the context in which it is used, the most widely accepted definition for the term is contained in ISO 15489, the international standard for Records Management practices. ISO 15489-1 defines a record as

“...information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.”²

The European Commission has also adopted this standard in its *Model Requirements for the Management of Electronic Records, version 2* (MoReq2).³ However, in contrast to ISO 15489, MoReq2 explicitly states that it applies to both electronic and physical records.

The U.S. National Archives and Records Administration (NARA), and therefore the U.S. government, is required by the Federal Records Act to use a slightly different and more explicit definition:

“records” includes all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.⁴

This definition covers nearly every piece of documentation created or used, regardless of media type, to conduct the business of the U.S federal government. However, there are exceptions in how this definition is interpreted, such when certain records types contain specific information. An example of this difference in interpretation can be found in the Privacy Act, 5 USC 552a⁵, which specifically targets the use of records containing personal information. Nevertheless, all of these interpretations share the common element of providing documentary evidence of an organization’s business transactions, as stated in the ISO 15489 definition.

Characteristics of Records

Regardless of the definition variations and interpretations, the underlying hallmarks of a record are the same. A record requires authenticity, reliability, integrity, and usability.⁶

1. Authenticity: the record is a “true” item – an accurate representation of a transaction or activity, as purported by its creator at the time of creation
2. Reliability: the record can be relied upon to be a trusted source of the information it contains
3. Integrity: the record has not been and cannot be altered. It is complete in form and data
4. Usability: the record can be repeatedly retrieved throughout its lifecycle and used as an authoritative source of the information contained within it.

If an item fails any of these criteria, it is not a record.

Non-records

Non-records are items, regardless of media type, that do not contribute, describe and provide evidence of the activities of an organization. An example of a non-record is an e-mail from one co-worker to another about lunch. Other examples of non-records include: documents that can be altered and have not been finalized, such as document drafts; museum and archival showpieces; voicemails, instant messages, or junk emails that have no connection to the organization's activities; and employees' personal documents, such as letters, notes and emails, stored in an organization's filing cabinets, desk drawers or computer network.⁷

It should also be noted that the criteria and eligibility to become a record is dependent entirely upon the content and context of the item, not the form or medium of the item. For example, many organizations classify all emails as records, and protect them as such through classification and archiving. This common desire is misguided. The decision that all e-mails are records results in needlessly saving thousands of emails that do not meet the definition of a record. Managing this unnecessarily consumes much of an organization's valuable IT and personnel resources.

Instead, organizations should evaluate items for their content and context, and protect them as records only if the definition and criteria for a record are met. The remaining items are non-records and can be destroyed. An example of proper examination of an email is one sent from one employee to another that contains an invitation to a party. Without further information and context, this e-mail is clearly not a record. However, if the two employees worked for an event planning company, the potential record state of the email becomes less clear. Does the invitation in the e-mail refer to a personal event not associated with the business transactions of the company? Or is the invitation a sample sent for review and approval purposes, thus becoming a documentary evidence of a business transaction? This act of discriminating between records and non-records is called "declaration."

“Declaration”

Declaration is the act of determining whether an item is a record. The declarer, usually the record owner or creator, examines the content of the item and performs a two-step analysis:

1. Does the content and context of the item meet the definition of a “record,” as defined by an organization?
2. Does the content meet the four characteristics (authenticity, reliability, integrity and usability) common to all records?

If the content satisfies both criteria, the item is a record and, thereafter, should be maintained and protected by an organization as a record. If the item does not satisfy either criterion, it is not a record. Even if the item satisfies one criterion, but fails another, it is still not a record, as fulfillment of both criteria is necessary to deem the item a “record”. If the item fails the analysis, records management best practices instruct that an organization can and should destroy the non-record after its possible temporary usefulness.

Once the item is declared a record, it should be placed in a restricted, secure storage device, such as a file cabinet or vault for physical records, or an electronic records management system (ERMS) for electronic records. These methods will safeguard the record and keep it unalterable during its lifecycle. Appropriate policies and rules for legal and business maintenance, retention, and disposition can then be applied to the record.

Issues Inherent in Declaration

Declaration is one of the most problematic stages of records management. There are a number of reasons for this: the time-consuming nature of reviewing the content and determining its status; the potential lack of adequate training of record owners and creators on the definition and characteristics of a record; the effort and expense required to create records policies and expectations where they do not exist; the effort required to enforce compliance with established records policies and standards; the wide discretion record

creators have in determining record status; and, at times, the willful disregard for the steps in records declaration. Each of these factors can play a role in either over-declaring or under-declaring records.

Over-declaration

Over-declaration occurs when, through a lack of organizational or personal preparation and commitment, excessive amounts of non-records are declared. The heart of over-declaration is the improper use of discretion given to the records owner in declaring an item a record. Some factors that contribute to the improper use of discretion include historical or past institutional practices, inadequate or non-existent records management training, or improper, uninformed direction from organizational leaders.

One major issue that can cause the improper exercise of discretion is that the act of declaration can be time-consuming and costly. Because of this, the record owner, his/her superiors, or his/her organization will often perform an impromptu and flawed cost/benefit analysis. The results of this analysis may indicate that the costs and time consumed by the declaration of individual items outweigh the liabilities that could accompany an organization's failure to properly declare items as records and follow its records retention and disposition policies. Therefore, a discretionary decision is made to treat and keep all items as records.

Another issue in over-declaration is over-cautiousness by record declarers and organizations. This often results from a record owner believing that a portion of a "record" could be useful or needed in the future. Therefore, through the improper exercise of discretion, the record owner or organization decides to retain both records and non-records, mistakenly assuming they are protecting all of the intellectual assets of the organization. In Armedia's experience, this approach to over-declaration occurs in every type of organization, but most often in organizations handling sensitive or classified information, such as law firms and insurance companies in the private sector. It is also thought to commonly occur in defense and intelligence related agencies, as well as other entities in the public sector.

A third issue centers on liability. It is common for organizations that over-declare to either have no retention schedule and policy or disregard one that is in place. Therefore, records and non-records that could be disposed legitimately remain in storage. The failure to follow

current and legally defensible retention and disposition policies and destroy non-records and eligible legitimate records can result information that is potentially harmful to the organization being made public through a lawsuit's discovery process. Examples of specific types of records an organization may wish to legitimately discard at the end of their lifecycle (according to a valid retention schedule) include: trade secret material; frank and potentially damaging communications between individuals in an organization; and personal employee information, such as health, salary or benefit records. If the records and non-records are available, relevant, and not protected by a privilege, the records and non-records are potentially discoverable in a lawsuit. The revelation of harmful records and non-records during a suit could contribute to an employee or organization suffering financial losses, through fines and judgments, and damaged reputations.

A fourth concern is that the storage requirements for records material. Over-declaration can increase an organization's costs and space requirements associated with records storage. Physical records consume a great deal of floor space for shelves or file cabinets. For example, a 4 drawer lateral file cabinet required 15.7 square feet in order to be used properly and safely. This consumption of space renders those areas unavailable for more productive or profitable purposes. In addition, it forces organizations to purchase more records equipment and supplies, some of which can be very expensive. For example, lateral file cabinets can cost up to \$1,000.00 a piece. For electronic records, it requires an organization to purchase more servers and hard drives for storage, enlarges the record storage footprint, increases electrical costs for this additional equipment, and may require additional IT personnel to manage the collection and potential upgrades to its records management software to scale up to the additional amount of records and non-records.

A final, and very often overlooked, issue relates to the potential inaccessibility of the proper records. When an organization over-declares, it unnecessarily increases the volume of records it needs to track and manage. It also compounds the challenges of searching for and accessing legitimate records, as search and sorting algorithms are applied against both legitimate and illegitimate records. In addition, it can be difficult to distinguish between legitimate and illegitimate records. However, many organizations, both public and private, fail to consider these factors as they amass the records through over-declaration. One consequence of this failure is that legitimate records may not be found or easily retrieved, potentially causing very large expenditures of resources to find the records later in their lifecycle.

Under-declaration

The opposite of over-declaration is under-declaration. It is the act of treating otherwise valid, legitimate records as non-records and disposing of them as such. Its cause is similar to that of over-declaration – the record owner’s improper use of his/her discretionary power in declaring an item a record. For under-declaration, some of the causes are similar to those of over-declaration – faulty interpretations of the definition of records; uniformed or improper instructions from superiors; inadequate training of personnel; and incorrect historical or past institutional practices.

One issue in under-declaration occurs from using the same flawed cost benefit analysis that invites over-declaration. An organization may arrive at the same analytical conclusion – that the costs associated with declaration outweigh the liabilities attached to non-declaration. However, in this instance, the conclusion produces the opposite reaction – an organization and its records owners, again improperly exercising their discretion, determine that declaration should not occur as a matter of course. Therefore, an organization treats none, or only its most obvious items, as records.

Another result of over-declaration is the loss of an organization’s vital intellectual and business record assets and information. It results in gaps in both the business and historical record of an organization’s actions and can cause an organization to incur large costs for the records’ recovery and restoration. An excellent example of this is the loss and eventual discovery of the missing 22 million emails from former President George W. Bush’s Administration. These emails were deleted prematurely from the email system used by the White House. Eventually, copies were found on back-up tapes.⁸ In a Freedom of Information Act lawsuit settlement agreement⁹, the Executive Office of the President (EOP) was forced to comply with the substance of the Federal Records Act and the Presidential Records Act.¹⁰ However, restoration of the records will prove to be far more costly in labor, financial and time expenditures than if care had been taken to review the emails for their records status before deletion.¹¹

Related to the loss of an organization’s intellectual capital and business information issue is the inability of an organization’s employees to draw upon missing information. If records are unavailable to the employees, employees must recreate previously performed work every time they conduct a business transaction. This reduces their productivity and slows their responsiveness to customers and/or

colleagues. In addition, cost of recreating a lost record can be considerable; some estimates put the cost at more than two hundred dollars per record.

A final issue of under-declaration is liability due to the loss of records. In the public sector, organizations and their employees can be fined or sanctioned by the courts for failure to produce records that should have been kept.¹² In the private sector, such unavailability has resulted in massive fines imposed by the courts.¹³

Solutions

There are several tools that can be used to prevent or alleviate the issues related to declaration of records.

Comprehensive Records Programs

A comprehensive records program includes:

- ◆ Policies and procedures governing the lifecycle of an organization's records, which includes an unambiguous statement by an organization of its definition of a record
- ◆ Retention and disposition policies that are applied to records once they are declared
- ◆ Well-defined file plans or taxonomies mapped to the retention schedule to organize the records
- ◆ A software platform to store, organize and track records regardless of their media type

Such a program can alleviate many of the problems associated with record status and declaration. The program provides a framework for the intake and protection of records and ensures that they are maintained for their appropriate time in the information lifecycle.

Senior Management Support of Records Management

Support from the senior leadership is vital to success of a records management program. Through strong support of the program, organizational leaders can convince subordinates to adopt the interpretation of a "record." In addition, the senior leadership can

command the organization to develop and implement a sound enterprise records management program. Such leadership begins with, as stated above, an unambiguous statement by an organization's leadership of its definition of a record, along with lifecycle policies and procedures that are promulgated from the organization's top management. Such policies must also contain "teeth" – punitive measures that triggered to enforce the use of the organization's policies and procedures by employees.

Education and Training

Mistakes by individuals in over and under-declaration often result from misunderstanding the definition and criteria of a record. Education and training can help correct this problem. An education and training program can present the organization's definition and criteria for record, the proper interpretation of that definition and criteria during declaration and the consequences of erroneous declaration by failing to follow the definition and criteria. Additionally, the presence of formal education also displays commitment to the records process to the entire organization.

Limiting or Removing the Record Owners Discretion

By removing a record owner's discretion in the interpretation and application of the record definition, the problems inherent in the process can be eliminated. For physical records, this can be accomplished in several ways. The first is routine reviews of potential records by a designated department records coordinator who is familiar with the records created by that portion of the organization. This review would be accomplished in conjunction with the organization's Records Manager to insure proper interpretation of the organization's standards. This review does not absolve the record owner of his/her responsibilities regarding the proper declaration of records and place the declaration issue in the hands of the coordinator. That would merely increase declaration problems by overburdening the coordinator. Instead, the review represents a "safety check" on the declaration process.

A second solution is conversion of the organization's physical items to electronic formats and the use of auto-classification techniques applied to item's captured metadata to determine whether it is a record. The metadata can be collection by the use of: bar code identifiers placed

on items during the conversion process; zonal or document wide Optical Character Recognition (OCR) for text material; and Intelligent Character Recognition (ICR) for handwriting; or forms recognition software. If the item is a record, the metadata populates a records management software platform and is associated with each record imported or migrated to the platform. Once the records are within the platform, they are auto-classified and appropriate retention and disposition policies are applied.

For organizations that use records management software platforms for items that begin lifecycle as electronic files, the process can have even fewer steps. Discretion can be removed by matching metadata attached to the record via a profile completed upon the item's creation or by keywords within the document. This matching process would also allow auto-classification of the records and application of appropriate retention values. Like physical records, electronic records may be subject to periodic review by the record owner's supervisor.

Conclusion

The U.S. government is required by the Federal Records Act to define records:

“records” includes all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.

Although the definition of a record may be clear, it is evident that it is not always followed. This is due in large part to a lack of focus on communicating these standards and the criteria in the declaration of records. When record owners do not apply the organization's standards and guidelines, this improper use of discretion costs organizations time, money and labor to correct. Executive leadership is crucial in eliminating these problems. If senior management demands implementing the approaches suggested in this whitepaper, employee compliance will be appropriately increased, and the risks to an organization are greatly reduced.

Armedia has experience providing Case, Document and Records Management services and solutions to various agencies to include Delta Airlines, United States Mint, Federal Bureau of Investigations, Pentagon Joint Staff, National Science Foundation, and the Department of Housing and Urban Development (HUD).

About Armedia

Armedia is a Veteran owned 8(a)/SDB certified technology firm, headquartered in Atlanta, GA, specializing in enterprise content management and content related solutions. Armedia's mission is to provide world-class solutions for clients to automate the creation, capture, organization and presentation of their intellectual assets. Armedia has offices in Atlanta, GA; Vienna, VA; and Dallas, TX. For more information visit our website at <http://www.armedia.com>.

¹ Throughout this document, the term “item” will refer to a container of information, regardless of media type, that has the potential to be considered a record.

² ISO 15489-1:2001, pg. 3

³ MoReq2 Specification. European Communities, 2008. pg. 17

⁴ 44 U.S.C. 3301.

⁵ 5 USC 552a(4): the term “record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;...”

⁶ Jones, Jim I. The Document Methodology for Enterprise Analysis, 2nd ed. Bloomington, IN, AuthorHouse, 2007. pg. 46.

⁷ See, Saffady, William. Records and Information Management: Fundamentals of Professional Practice. Lenexa, KS, ARMA International, 2004. pg. 7, for a more extensive list of non-records.

⁸ The Associated Press, “Missing Bush-Era E-Mail Is Found.” *The New York Times* December 14, 2009. Web. December 30, 2009.

⁹ CREW v. EOP, et. al. , Case 1:07-cv-01707-HHK, (D.D.C.), filed Sept. 25, 2007 and National Security Archive v. EOP et. al., Case 1:07-cv-01577-HKK (D.D.C.), filed Sept. 5, 2007.

¹⁰ CREW v. EOP. et. al., and National Security Archive v. EOP, Terms of Agreement, Case Nos. 1:07-cv-01707 and 1:07-cv-01577, Dec. 14, 2009, U.S. District Court for the District of Columbia. See also, Federal Records Act of 1950 (as amend), 44 U.S.C. 3301 et. seq., and Presidential Records Act of 1978, [44 U.S.C. § 2201–2207](#)

¹¹ See, e.g., Zubulake v. UBS Warburg LLC1, 2003 U.S. Dist. LEXIS 12643 (S.D.N.Y. July 24, 2003). (Defendants estimated cost of recovering 600 responsive emails from 77 backups was \$165,954.67 with another \$107,694.72 for analysis.) and Gaudin, Sharon, (2007, April 11), Security Breaches Cost \$90 To \$305 Per Lost Record. *InformationWeek*. Retrieved from <http://www.informationweek.com>.

¹² See, e.g. Leonning, Carol D. (2003, July 25) EPA held in contempt by judge. *The Washington Post*. Retrieved from <http://www.washingtonpost.com>. (EPA held in contempt for the destruction of computer hard drives and deletion of emails)

¹³ See Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co. Inc., 2005 WL 67071 (Fla. Cir. Ct. Mar. 1, 2005), rev'd on other grounds, 955 So.2d 1124 (Fla. 4th CA 2007) (Jury found \$1.45 billion in compensatory and punitive damages for being "grossly negligent" in failing to produce emails and email attachments during discovery) and Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (D.N.Y. 2004) (\$29 million in damages, in part for failure to provide emails pertinent to the suit). In both cases, jurors were given adverse inference jury instructions regarding the failure to produce responsive material during discovery.