ARMA International TR 28-2015

Secure Management of Private Information

A Technical Report prepared by
ARMA International and registered with ANSI
September 13, 2015

Secure Management of Private Information

ARMA International TR 28-2015

A Technical Report prepared by ARMA International
and registered with ANSI
September 13, 2015

Consulting Editors: Nancy D. Barnes, Ph.D., CRM, CA, and Vicki Wiler
Composition: Cole Design & Production
Cover Art: Cole Design & Production

ARMA International
11880 College Blvd., Suite 450
Overland Park, KS 66210
913.341.3808

978-1-936654-69-7
978-1-936654-70-3 (PDF version)

A4968
V4968 (PDF version)

Table of Contents

Acknowledgments

ARMA International gratefully acknowledges the contributions of time and expertise made by the following individuals. Without their efforts, this publication would not have been possible. Affiliations listed are those on record with ARMA International at the time of printing.

Workgroup Leader:

Dernea Michaux-Davis, CRM, CIPP/US, Kemper Corp, Chicago, IL

Workgroup Members:

Ana Aquino-Pérez, Wisconsin Department of Transportation, Madison, WI

Melinda Augustus, J.D., The Augustus Law Office, Missouri City, TX

Cherri-Ann Beckles, University of the West Indies, Cave Hill, Barbados

Sandra Broady-Rudd, CRM, Wells Fargo, Pardeeville, WI

Raúl Chang Rivas, PMP, CIP, Panama Canal Authority, Panama City, Panama

Sylvia Diaz, CIPP/US, Biogen, Cambridge, MA

Sofia Empel, Ph.D., IGP, CRM, Connolly iHealth Technologies, Wilton, CT

Carol Garnham, CRM, Southern Health-Santé Sud, Southport, Manitoba, Canada

V. Nicole Godin, KPMG LLP, Toronto, Ontario, Canada

Susan Goodman, IGP, CRM, CIP, CIPP/US, CIPM, Kirkland, WA

Sheri Nystedt, IGP, CRM, CIP, Janus Capital Group Inc., Denver, CO

Monette Ramos, AECOM Middle East, Doha, Qatar

Snow Zhu, CRM, CA, CIP, American Civil Liberties Union, New York, NY

Special Contributors:

Thank you to the members of the ARMA International RIM Review Group and Content Editorial Board who graciously contributed to the vetting and review of this technical report.

Thanks, also, to the ARMA International Standards Development Program standards consultant, Nancy D. Barnes, Ph.D., CRM, CA, who served as project manager for the development of this publication, and to Vicki Wiler, ARMA International's director of publications.

Foreword

Publication of this Technical Report has been approved by ARMA International. This document is registered as a Technical Report series of publications according to the *Procedures for the Registration of Technical Reports with ANSI*. This document is not an American National Standard and the material contained herein is not normative in nature.

Comments on the content of this document should be sent to:

ARMA International
Attn: Standards
11880 College Boulevard, Suite 450
Overland Park, Kansas 66210
standards@armaintl.org

With the registration of this publication, ARMA International has 13 titles in its series of ANSI-registered technical reports. Many of the subjects touched upon in this technical report are discussed in-depth in preceding titles. A complete list of ANSI-registered technical reports may be found in Appendix G.

Rationale

The scope of ARMA International's Standards Development Program activities includes the development of systems, rules, reports, and/or procedures for information and records creation, structure, capture, organization/classification, search, access, retrieval, use, transmission, retention, storage, and disposition in paper and electronic formats. Topics related to archives/records and information management such as: information governance, security, disaster recovery, legal/regulatory requirements, process quality improvement, and specific filing equipment, supplies, terminology and applications/technologies are studied, as well. Standards and technical reports may be developed in any of the aforementioned subject areas and may have broad, cross-industry, or unique sector-specific applicability.

This technical report addresses topics related to the secure management of private information. It is designed for instructional use by information management professionals including educators, vendors, and recordkeeping practitioners, as well as others employed in information governance roles defined by ARMA International to embrace privacy, security, information technology, legal, line-of business, and audit stakeholders. It is not industry- or sector-specific.

This publication complements the ARMA International Generally Accepted Recordkeeping Principles®, also known as the Principles. The Principles are recognized as a *de facto* standard; they are used and accepted by information governance professionals worldwide.

▸ 1 Introduction

Management of information is an essential activity for any organization, whether operating as a for-profit, not-for-profit, or government-affiliated entity. Such management can be accomplished by using either a lifecycle or continuum-based approach.

The *lifecycle approach* uses a cradle-to-grave model in which information moves through definable stages from creation/receipt to use, storage, and disposition. Within the disposition stage, information undergoes destruction, transfer, or permanent preservation. Thus, the recordkeeping and archival components are somewhat separate and distinct.

Alternatively, the *continuum-based approach* de-emphasizes these discrete, time-bound stages of the lifecycle. Records are recognized as usable for multiple purposes, and there is a more seamless vantage point from which to view the records/archives elements of information management. The continuum perspective also promotes integration of records management into an organization's business systems and processes.

While organizations in North America more often utilize the lifecycle perspective, other regions of the world espouse the continuum as the ideal model. Despite this duality, information management continues to evolve, thriving in diverse organizations around the globe. And regardless of the approach selected, information management remains, nonetheless, entrenched in sound information governance. Good governance requires that an organization construct a framework that affords a reasonable level of protection to information that is private. This is the basis for the Principle of Protection as described in ARMA International's Generally Accepted Recordkeeping Principles© (Principles). (See the eight Principles at *www.arma.org/principles*.)

1.1 Scope

This publication includes a general discussion of issues related to the secure management of private information. It does not focus on the requirements of specific industries or sectors, but offers general advice for implementation of information privacy controls in the organizational setting.

1.2 Purpose

The purpose of this technical report is to educate information management professionals and related practitioners about information governance-related issues pertaining to the protection of private information, including records. It supplements the records and information management (RIM) literature and answers these questions:

1. How can organizations more effectively comply with privacy laws and regulations (domestic and international) in the management of private information?
2. How can the organization's policies and procedures better effect its ability to handle private information?

While this publication is not all-inclusive, it provides foundational knowledge and offers references in the appendixes and bibliography to many educational resources for further reading.

▸ 2 Definitions

This section contains only those definitions essential for clarification of this technical report.

Unless otherwise noted, definitions are derived from ARMA TR 22-2012, *Glossary of Records and Information Management Terms*, 4th edition.

access
The right, opportunity, or means of finding, viewing, using, or retrieving information.

access control
The management of access to a resource or service based on organizational policy and the permission level assigned to the person requesting access.

active directory (AD)
A central location for network administration and security that is used for authenticating and authorizing all users and computers within a network of Windows® domain type, assigning and enforcing security policies for all computers in a network, and installing or updating software on network computers.

appraisal
The evaluation of a document's worth or its value for retention or archival purposes, based upon its current or predicted future use(s) for administrative, legal, fiscal, research, or historical purposes.

Also referred to as records appraisal.

ARMA International Information Governance Maturity Model
A model providing metrics that organizations can use to develop an information governance program, benchmark an information governance program's maturity, identify and analyze gaps in an information governance program, assess information-related risks, and develop plans for mitigating those risks.

attribute
A characteristic of an element or data that provides additional information about it.

audit trail metadata
Protected metadata documenting record activity, including information about when and by whom a specific record was created, changed, or deleted.