Fedora and the
Preservation of University Records Project

1.5 Requirements for Trustworthy Recordkeeping Systems and the Preservation of Electronic Records in a University Setting

Version
1.0

Date
September 2006

Digital Collections and Archives, Tufts University
Manuscripts & Archives, Yale University

An Electronic Record Research Grant funded by the
National Historical Publications and Records Commission

Digital Collections and Archives
Tisch Library Building
Tufts University
Medford, Massachusetts 02155
http://dca.tufts.edu

Manuscripts and Archives
Yale University Library
Yale University
P.O. Box 208240
New Haven, Connecticut 06520-8240
http:// www.library.yale.edu/mssa/

© Tufts University and Yale University, 2006

Co-Principle Investigators
Kevin Glick, Yale University
Eliot Wilczek, Tufts University

Project Analyst
Robert Dockins, Tufts University

This document is available online at
http://dl.tufts.edu/view_pdf.jsp?urn=tufts:central:dca:UA069:UA069.004.001.00005
(September 2006)

Fedora and the Preservation of University Records Project Website at
http://dca.tufts.edu/features/nhprc/index.html

Funded by the
National Historical Publications and Records Commission
Grant Number 2004-083

Fedora and the Preservation of University Records Project

TABLE OF CONTENTS

I. INTRODUCTION

This report presents the results of an effort to illustrate trustworthy electronic recordkeeping and preservation at a college or university. It describes the necessary features, behaviors, and qualities of recordkeeping systems and preservation activities which may take place in recordkeeping systems or separate preservation systems. These requirements are articulated as two separate sets of functional requirements, one for recordkeeping and another for preservation.

Although the focus of this research project was aimed primarily at preservation, the project team felt it was necessary to establish a set of recordkeeping system functional requirements. Before designing new recordkeeping systems or evaluating existing systems for active records creation and management, it is necessary to define what types of functionality such a system should possess in order to facilitate preservation, whether that be undertaken inside the recordkeeping system or after transfer of the records to a separate preservation system.

This is not the first set of recordkeeping system functional requirements. In fact, these requirements are primarily a synthesis of recordkeeping requirements written by other groups in the 1990s and early 2000s into a single set that is appropriate for a university setting. There have been a number of significant efforts to define recordkeeping functional requirements, including national and international standards creating bodies. However, the project team believed it necessary to create a new set of recordkeeping requirements, because, "no one list [of functional requirements] has been endorsed by the [university archival] profession."[1] There are a number of reasons for this lack of profession-wide acceptance. The existing literature does not agree on terminology. The sets of requirements differ, in some cases significantly. The field of digital preservation had not reached full maturity during this period (some might argue that the field still has not yet reached full maturity). Many issues remained unexplored as each project began. The recordkeeping functional requirements literature from the period focused on specific aspects of digital perseveration, like records management software specifications, warrant, or policy development. This was all very important work, but each did not always consider the full scope of digital preservation or build upon the work of its predecessors. In addition, the majority of this work has been undertaken primarily by government recordkeeping professionals with the creation and maintenance of the government records in mind. This set is aimed at university records. This work addresses current needs of the college and university recordkeeping by leveraging the expertise from all the most significant projects over the last fifteen years.

A description of the necessary attributes of the activity of preservation in a college or university is necessary in order to preserve electronic records and ensure their continued accessibility and authenticity over time as the creating technologies become obsolete. In addition such a set of requirements is necessary in order to evaluate existing recordkeeping or preservation systems or to plan and/or build new systems capable of facilitating long-term preservation of authentic electronic records. Unlike the situation for recordkeeping, there has not been an extensive body of literature specifically on the functional requirements for preservation of electronic records. There is no single set of preservation requirements; no international standard. However, the project team found that many of the requirements necessary for long-term preservation are

[1] Philip Bantin, "Functional Requirements for Recordkeeping Systems – Evolution of the IU Functional Requirements," 2002 <http://www.indiana.edu/~libarch/ER/nhprcfinalfuncreq.doc>.

included in the existing recordkeeping requirements literature. This is because some of the same activities necessary to keep records accessible in active recordkeeping systems are also necessary to preserve records over the long term. As a result, many of the functional requirements of preservation activities have been gleaned from recordkeeping requirements literature.

The project team developed the separate sets of functional requirements for recordkeeping and preservation because recordkeeping and preservation environments are separately administered respectively by Producers and archivists (preservers) at both Tufts and Yale. Thus the project team is biased to presume that a Producer will create, acquire, use, and manage records in a recordkeeping system to suit its current business needs. While the central purpose of a recordkeeping system is to support the business needs of its Producer, the central purpose of preservation activities is to preserve records. In a pure records lifecycle model environment, an Archive will later ingest some records from a recordkeeping system into a separate preservation system (Archive) that the preserver administers, undertaking preservation activities in this system. In such a situation, the Producer would be responsible for meeting the recordkeeping requirements and the Archive would be responsible for meeting the preservation requirements. However, it may also be possible that this may be a continuous process where records do not move from a recordkeeping system to a separate preservation system administered by completely separate juridical entities. In this case, preservation activities will need to take place in the recordkeeping system if the electronic records are to persist over the long term. In this case, the recordkeeper is also acting as the preserver and should meet both the recordkeeping and the preservation requirements. This document should also apply in such situations.

The purpose of this report is not to serve as a records management or preservation application software specification. These functional requirements describe the entire recordkeeping system, not only the application. Thus it is best utilized by those who would benefit from a more holistic view of recordkeeping and preservation, like resource allocators and administrators responsible for those that buy, build, or manage recordkeeping or preservation systems, as well as archivists and records managers.

II. FORM OF THE REQUIREMENTS

The requirements for a recordkeeping system described in Section IV, or for preservation described in Section V, are for either the *Application* itself or for the *Natural or Juridical People, Institution, Procedure*, or *Infrastructure*. No requirements are expressed as requirements for *Recordkeeping System*. As *Records Controls* themselves impose requirements on records systems, the document does not include requirements for any *Controls*.

Each requirement includes only one of the six records system components. While some requirements may pertain in some way to multiple components, every requirement in this report only contains the most relevant component.

The requirements in this report are organized into two different chapters, one for recordkeeping system requirements and the other for records preservation requirements. The recordkeeping chapter is organized into six sections based loosely on the framework presented in the Records management and controls section of ISO 15489-1: *Information and documentation—Records management.*[2]:

1. Record Retention and Disposition
2. Records Capture and Registration
3. Classification
4. Storage and Handling
5. Access
6. Design and Performance

These six sections are further broken down into a total of fourty subsections that the Tufts-Yale project team created from the existing requirements. There was no attention paid to possible subsection topics that might exist if there were no recordkeeping requirements identified on that subject in the existing literature. Because of the strength of the existing literature, the project team did not make any effort to create requirements not found in the literature.

The records preservation requirements chapter is organized into seven sections, with the requirements grouped according to the six functional entities of the OAIS Reference Model, in addition to Common Services:

1. Common Services
2. Ingest
3. Archival Storage
4. Data Management
5. Administration

[2] ISO 15489-1: 2001, *Information and documentation – Records management – Part 1: General.* During this process the project team also gave careful consideration to mapping the recordkeeping requirements to *Trusted Digital Repositories: Attributes and Responsibilities*, but ultimately decided that the Records management processes and controls section of ISO 15489-1 was a better fit for the requirements. Organizing the requirements according to ISO 15489 gave the project team an existing conceptual framework upon which it could shape the requirements. It appears that that there is no consensus or preferred framework for recordkeeping system requirements in the way the OAIS Reference Model appears to play that role in describing a framework for preservation requirements.

6. Preservation Planning
7. Access

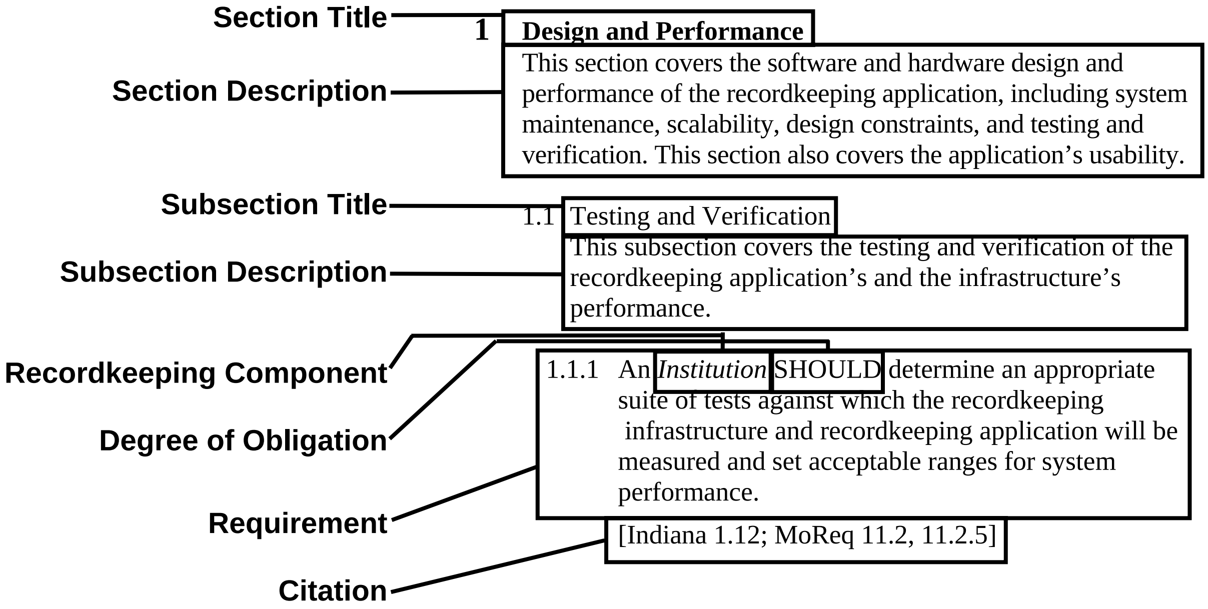
These seven sections are broken down into thirty-four subsections using the corresponding sub-functions of the OAIS model. In the case of the preservation requirements, the project team gave attention to subsection topics for which the requirements literature did not identify functional requirements in any obvious way. Because of the limited nature of the existing literature, the project team attempted to augment requirements found in the literature by creating its own requirements.[3] This was done only in cases where an analysis of the existing literature did not yield requirements the project team deemed necessary for preservation.

As stated above, every section has a number of different subsections. All of the requirements are nested within these subsections. The section and subsections have brief descriptions. These descriptions are not requirements; rather they are explanations defining the nature and scope of each section and subsection.

Each requirement will have a sequential number, the text of the requirement itself, and a citation to one or more of the research projects listed at the beginning of both requirement chapters. The text of the requirement itself will contain one of the five Records Components (Application, Infrastructure, Institution, Natural or Juridical People, or Procedures), a degree of obligation (MUST, MUST NOT, SHOULD, SHOULD NOT, or MAY), and then a description of the actual requirement. (See Figure 1)

[3] A primary reason for this need to identify additional requirements stems from the fact that the OAIS framework covers all the components of preservation, while much of the existing literature was focused on Application (software) specifications.

Figure 1
Example Requirement



1 Design and Performance

This section covers the software and hardware design and performance of the recordkeeping application, including system maintenance, scalability, design constraints, and testing and verification. This section also covers the application's usability.

1.1 Testing and Verification

This subsection covers the testing and verification of the recordkeeping application's and the infrastructure's performance.

1.1.1 An *Institution* SHOULD determine an appropriate suite of tests against which the recordkeeping infrastructure and recordkeeping application will be measured and set acceptable ranges for system performance.

[Indiana 1.12; MoReq 11.2, 11.2.5]

III. Degrees of Obligation for each Requirement

To ensure clarity and accuracy, this report adheres to the RFC 2119 standard for defining requirement levels.[4] It is important to understand the precise meanings of each of these keywords, particularly because each does not necessarily represent the most commonly accepted meaning of the word. In this document each recordkeeping requirement is qualified by one of five modal auxiliary verbs used to express different degrees of obligation. These different verbs are: MUST, MUST NOT, SHOULD, SHOULD NOT, and MAY. The use of each keyword is described below:

MUST. This word means that the definition is mandatory, or an absolute requirement of this specification. If this requirement is not fulfilled, the system can not be considered to be a trustworthy recordkeeping system.

MUST NOT. This phrase means that the definition is an absolute prohibition of the specification.

SHOULD. This word means that there may be valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. Such a requirement is highly desirable. If the requirement is not fulfilled, the level of trust in the recordkeeping system will be diminished.

SHOULD NOT. This phrase mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

MAY. This word means that an item may be desirable, but truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation that does not include a particular option MUST be prepared to interoperate with another implementation that does include the option, though perhaps with reduced functionality. In the same vein an implementation that does include a particular option MUST be prepared to interoperate with another implementation that does not include the option (except, of course, for the feature the option provides.)

[4] Scott Bradner, *RFC 2119: Key words for use in RFCs to Indicate Requirement Levels*, Network Working Group <http://www.ietf.org/rfc/rfc2119.txt?number=2119>.

IV. RECORDKEEPING SYSTEM REQUIREMENTS

This chapter of the report describes the features, behaviors, and qualities of a trustworthy recordkeeping system at a college or university. It describes these features, behaviors, and qualities as requirements in ten sections. The large majority of these requirements are synthesized from existing research into the requirements for recordkeeping systems conducted by a number of organizations and research projects over the last two decades. The requirements documents examined include:

- Indiana University, *Requirements for Electronic Records Management Systems (ERMS)*, Bloomington, IL: 2002 <http://www.indiana.edu/~libarch/ER/requirementsforrk.doc>.
  In this document referred to as: Indiana

- University of Pittsburgh, *Functional Requirements for Evidence in Recordkeeping*, Pittsburgh, PA: 1996 <http://web.archive.org/web/20001024112939/www.sis.pitt.edu/~nhprc/prog1.html>.
  In this document referred to as: Pitt

- Alan Kowlowitz and Kristine L. Kelly, *Functional Requirements to Ensure the Creation, Maintenance, and Preservation of Electronic Records*, Albany, NY: Center for Technology in Government, State Univeristy of New York, 1998 <http://www.ctg.albany.edu/publications/reports/functional/functional.pdf>.
  In this document referred to as: CTG

- IDA Programme of the European Commission, *Model Requirements for the Management of Electronic Records*, 2001 < http://ec.europa.eu/idabc/servlets/Doc?id=16847>.
  In this document referred to as: MoReq

- Public Records Office, *Functional Requirements for Electronic Records Management Systems*, Surrey, UK: 2002 <http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/pdf/requirementsfinal.pdf>.
  In this document referred to as: PRO

- InterPARES I Project, “Requirements for Assessing and Maintaining the Authenticity of Electronic Records,” *in The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project,* San Miniato, Italy: Archilab, 2005 <http://www.interpares.org/book/interpares_book_k_app02.pdf>
  In this document referred to as: InterPARES

- U.S. Department of Defense, *Design Criteria Standard for Electronic Records Management Software Applications* (DoD 5015.2-STD), Arlington, VA: 2002 <http://www.dtic.mil/whs/directives/corres/pdf/50152std_061902/p50152s.pdf>
  In this document referred to as: DoD

- International Organization for Standardization, *ISO 15489-I: Information and*

documentation—Records management
In this document referred to as: ISO

- San Diego Super Computer Center at the University of California, San Diego, *Preserving the Electronic Records Stored in a Records Management Application* (PERM Project), San Diego, CA: 2002 <http://www.sdsc.edu/PERM/Final-Report-December-20-2002.pdf>
  In this document referred to as: PERM

  Health Insurance Portability and Accountability Act, 45 C.F.R. § 160, 162, 164 (2005) <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title45/45cfrv1_02.tpl>.
  In this document referred to as: HIPAA

This report articulates a set of requirements based on a synthesis of these reports appropriate for a college and university setting and within the framework of the following assumptions below.

1. **Retention and Disposition**

This section covers the act of executing the disposition of records according to a records retention schedule. This usually means the act of removing records and their metadata from the recordkeeping application for either destruction or for transfer to a preservation application. The work also includes reviewing records before carrying out their disposition and the application of legal holds on records that are involved in a legal action, audit, or review. This section does not cover the creation and assigning of records retention schedules. See Subsection 3.2.

1.1. Execution

This subsection covers the execution of a record's disposition, which usually means either destruction or transfer to a semi-active, inactive, or preservation application.

1.1.1. An *Institution* SHOULD dispose of records that no longer have operational value, either by permitting (arranging for) their destruction, or by transferring (arranging for) their transfer to a preservation repository.
[ISO, 4.3.9, MoReq 5]

1.1.2. *Procedures* MUST articulate the management of records disposition, in particular the destruction or transfer of records to a preservation system.
[MoReq 5.2.10, 5.3.1; ISO 9.9]

1.1.3. *Procedures* MUST allow for the confidential destruction of all copies and instances of records scheduled for destruction.
[MoReq 5.3.9; PRO A.4.74, B.3.26; DoD c2.2.10.6; ISO 9.9]

1.1.4. An *Application* MUST confidentially destroy records scheduled for destruction in a manner that does not allow their recovery.
[Pitt 10; MoReq 5.2.13, 5.3.14, 9.3.2; PRO A.4.67-68; DoD c2.2.6.63; ISO 9.9.a; HIPAA 45CFR164.310]

1.1.5. An *Application* SHOULD be able to retain metadata about records that it destroys.
[Pitt 10C; MoReq 5.2.15-16; DoD c2.2.6.6.4]

1.1.6. An *Application* MUST be able to transfer records scheduled for long-term retention to a preservation system in a trustworthy manner.
[MoReq 5.3.3, 5.3.5, 5.3.7; ISO 9.9.c]

1.1.7. An *Application* SHOULD be able to retain metadata about records that it transfers to a preservation system.
[DoD c2.2.6.5.4]

1.1.8. An *Application* MAY track the actual time of disposition for a record based on the retention schedule assigned to that record.
[PRO A.4.29, A.4.35-36, A.4.49]

1.1.9. An *Application* SHOULD be able to export records to a preservation system.
[PRO A.4.50, A.4.58; PERM non dod 1]

1.1.10. An *Application* MUST, if it can export records to a preservation system, export records in a manner that preserves their recordness.
[PRO A.4.50-52; InterPARES A.8; DoD c2.2.6.5.3; PERM non dod 1]

1.2. Compliance with Schedules

This subsection covers the need for the disposition of records to be executed in compliance with appropriate retention schedules.

1.2.1. An *Institution* MUST base the disposition of its records and audit trails on appropriate, authorized, and approved records retention schedules.
[Indiana 1.4.2, 1.8, 1.8.1-2; MoReq 3.4.6; PRO A.1.46; ISO 7.1, 9.9]

1.2.2. An *Application* SHOULD be able to manage a variety of retention period configurations and disposition instructions.
[DoD c2.2.2.2, c2.2.2.4, c2.2.2.4.1-3, c2.2.2.5]

1.2.3. An *Application* MUST be able to adjust the scheduled disposition of a record if the content of the retention schedule that governs the record changes.
[DoD c2.2.2.6, c2.2.2.7]

1.3. Review

This subsection covers the review of records before executing their disposition as prescribed by their assigned retention schedule.

1.3.1. *Procedures* MUST articulate steps for reviewing records before their scheduled disposition is executed.
[MoReq 5.1.10, 5.2; ISO 9.9]

1.3.2. An *Application* SHOULD alert people of and present to them for review records, including vital records, that have a pending disposition.
[Indiana 1.8.4; MoReq 5.1.10, 5.2.1, 5.2.3-4, 5.2.7-8, 9.3.7; PRO A.4.32, A.4.45-46, A.4.64]

1.4. Legal Holds

This subsection covers managing the process of suspending the execution of a record's disposition that is a part of any ongoing or reasonably expected legal action or proceedings, litigation, audit, investigation, or review.

1.4.1. An *Institution* MUST be aware of ongoing and reasonably expected legal action or proceedings, litigation, audit, investigation, or review that involves or may involve its records and identify any records so affected.
[Indiana 1.8.5; ISO 9.9]

1.4.2. *Procedures* MUST allow for the interruption of the scheduled disposition of records with legal holds that are or are expected to be involved in legal action or proceedings, litigation, audit, investigation, or review.
[Indiana 1.8.5; PRO A.4.25-26, A.4.38; DoD c2.2.6.4.1; ISO 9.9]

1.4.3. *Procedures* MUST allow for the appropriate lifting of legal holds on records and the resumption of their scheduled disposition.
[PRO A.4.27; DoD c2.2.6.4.3]

2. Records Capture and Registration

This section covers the creation and capture of records through recordkeeping systems in a manner that preserves the records integrity and essential elements of form or recordness. It covers the requirements to create records that document activities. It discusses the creation and capture of a variety of standard document types, complex documents, metadata, and relationships between records, along with the process of assigning unique identifiers and normalization during the creation and capture process.

2.1. Generate Records

This subsection covers the need to create required records to successfully conduct business activities

2.1.1. An *Institution* MUST document its activities by creating or capturing records when those activities commit the institution to action, render the institution accountable, or document an action, decision, or decision-making process.
[ISO 9.1]

2.1.2. An *Institution* SHOULD generate records that document all of its defined functions and activities.
[Indiana 1.2.1; ISO 7.1.a, 7.2.1, 8.2.5]

2.1.3. An *Institution* SHOULD ensure its recordkeeping applications are able to capture all of its records.
[MoReq 6.1.1; PRO A.2.1, A.2.4, A.2.6]

2.1.4. *Procedures* SHOULD include quality control mechanics to ensure that accurate records are created.
[Indiana 1.7; Pitt 7a]

2.1.5. *Juridical People* MUST have clearly defined responsibilities for creating and capturing records.
[ISO 6.3]

2.1.6. *Natural People* SHOULD only create records using documented recordkeeping applications and recordkeeping procedures.

[Pitt 3a]

2.1.7. *Natural People* MUST create and receive records as part of their daily work, and should do so in accordance with established policies, procedures, and standards.
[ISO 2.3.2]

2.1.8. An *Application* MUST enable the creation, reception, and keeping of records necessary to support business activities.
[ISO 2.3.1]

2.2. Create and Capture Integrity

This subsection covers the creation and capture of records in a recordkeeping system in a manner that preserves their integrity.

2.2.1. An *Application* MUST create and capture records in a manner that maintains the integrity and identity of the records.
[Pitt 7a1; InterPARES B.1]

2.2.2. An *Application* SHOULD verify the integrity of the records it creates and captures.
[MoReq 6.2.1]

2.2.3. *Procedures* MUST articulate steps that maintain an unbroken custody of records during capture.
[InterPARES B.1.a]

2.3. Create and Capture Recordness

This subsection covers the creation and capture of the essential aspects of records in a recordkeeping system.

2.3.1. An *Application* MUST be able to create and capture a record’s context, structure, and content that together documents the institution’s decisions, actions, or communications.
[Pitt 7b, 7b1-4; MoReq 6.1.2; PRO A.2.8]

2.3.2. *Procedures* MUST provide for the creation and capture of records in a manner that allows them to correctly reflect the decisions, actions, or communications it documents.
[Pitt 7c, 7c1-3; InterPARES A.1.a.i-v, A.1.b.i-iv, A.5]

2.4. Support of Format Types

This subsection covers the creation and capture of records of various formats.

2.4.1. An *Institution* MUST have recordkeeping applications that together are able to create and capture all of the record formats the institution generates in the course of its business.

[MoReq 6.1.1]

2.4.2. An *Application* SHOULD be able to create and capture records with a variety of format types and structures.
[Indiana 1.2.10; MoReq 6.1, 6.3, 6.3.1-2]

2.5. Create and Capture Complex Documents
This subsection covers the creation and capture of complex records.

2.5.1. An *Application* MUST, if it is used to manage complex records, be able to create and capture records in a manner that captures the structural integrity of its component parts.
[MoReq 6.1.13, 6.3.1, 6.3.2; PRO A.2.5, A.2.8; ISO 7.2.1.a]

2.5.2. An *Application* MAY allow for the creation and capture of complex records, a single compound record, or as a series of linked simple records.
[Indiana 1.2.7; MoReq 6.3.6]

2.6. Create and Capture Relationships Between Records
This subsection covers the capture of the relationships between records.

2.6.1. An *Application* MUST be able to capture the relationships between records.
[PRO A.8.17]

2.7. Create and Capture Information About Records
This section covers the creation and capture of metadata associated with records a recordkeeping system creates and captures.

2.7.1. An *Application* SHOULD be capable of automatically extracting metadata from the records it creates and captures.
[Indiana 1.6.1; MoReq 6.1.6, 6.1.14]

2.7.2. An *Application* MUST allow people to manually enter metadata that cannot be automatically extracted from the records created and captured by the recordkeeping application.
[Indiana 1.6.3; MoReq 6.1.9; PRO A.2.38]

2.7.3. *Procedures* MUST provide for the creation of necessary metadata during the creation and capture process that did not exist before creation or capture.
[MoReq 6.1.9; PRO A.2.38]

2.7.4. An *Application* SHOULD be able to technically validate the metadata it creates or captures.
[Indiana 1.6.4; MoReq 6.1.1]

2.7.5. *Procedures* SHOULD provide for the intellectual validation of the metadata (data content standard of the metadata is met) the recordkeeping system creates or captures during the creation or capture process.
[Indiana 1.6.4; MoReq 6.1.1]

2.7.6. An *Application* SHOULD be able to create and capture descriptive, contextual, and technical metadata.
[PERM 12]

2.7.7. *Procedures* SHOULD provide for the creation and capture of descriptive, contextual, and technical metadata.
[Indiana 1.2.3; Pitt 8a; MoReq 6.1.2, 6.1.3; ISO 7.2.1.b]

2.7.8. An *Application* MUST create and capture records and their metadata in a manner that allows them to be persistently linked.
[Indiana 1.2.3; MoReq 6.1.3; ISO 7.1.c]

2.7.9. An *Application* MUST assign unique identifiers to the records it creates and captures.
[Indiana 1.2.5; MoReq 7.1.5]

2.8. System Interaction

This subsection covers the ability of a recordkeeping application to communicate and integrate with other recordkeeping and various record creating applications.

2.8.1. An *Application* SHOULD be capable of communication with all of the Institution's other recordkeeping and record creating applications.
[Indiana 1.6.2; MoReq 6.2.1; PRO A.2.2]

2.8.2. An *Application* SHOULD provide an application programming interface to enable integration with other business applications.
[PRO A.2.3]

2.9. Normalization

This subsection covers capture of standard format versions of records in a recordkeeping system captured in other formats. This section does not cover migration, which is covered in Section 7, Preservation. This deals specifically with normalization during the capture process.

2.9.1. An *Application* SHOULD be able to capture a standard format version of records it captures in its native format.
[PRO A.2.12]

2.9.2. An *Application* MUST persistently link the format versions of the same records together.

[PRO A.2.12]

3. **Classification**

This section covers the development and management of classification schemes, which include records retention schedules, in recordkeeping systems. It also covers the assigning of records to classes within a classification scheme or multiple schemes and the institutional context of these schemes. Although assigning a record to a scheme assigns meaning and prescribes actions to that record, the execution of those actions is not covered in this section.

3.1. Manage Scheme

This subsection covers the creation, management, and modification of classification scheme(s) within a recordkeeping system. A classification scheme is a logical system used to arrange records. Usually, classes are related component parts that compose a scheme. This section does not cover the act of classifying records.

3.1.1. An *Application* MUST allow the creation and defining of a classification scheme.
[MoReq 3.1.5; PRO A.1.3, A.4.1; ISO 9.3.A; DoD c2.2.1.1]

3.1.2. An *Application* MAY allow the creation and defining of multiple classification schemes.
[MoReq 3.1.8; PRO A.1.10]

3.1.3. An *Application* MAY allow the creation and defining of a vital records classification scheme.
[DoD c2.2.6.7]

3.1.4. An *Application* MUST allow the changing, amending, deleting and adding to a classification scheme.
[Indiana 1.8.7; MoReq 3.1.6, 3.4.1; PRO A.1.4, A.1.6, A.1.8, A.4.4, A.4.6]

3.1.5. An *Application* MUST ensure that classification names are unique.
[PRO A.1.18]

3.1.6. An *Application* SHOULD allow the closing of classes within a scheme so that no new records can be added to a closed class.
[PRO A.1.7, A.1.41]

3.1.7. An *Application* MUST NOT allow the deletion of classes that contain records.
[PRO A.1.9]

3.1.8. An *Application* SHOULD NOT impose any practical limits on the number of classes or class levels that exits within a scheme.
[MoReq 3.1.3, 3.2.9; PRO A.1.28]

3.1.9. An *Application* SHOULD report its classes, schemes, and records in a logical, usable fashion.

[MoReq 3.2.10; ISO 9.3.6]

3.2. Retention Schedules

This subsection covers the management and modification of retention schedules along with the act of assigning record(s) to a retention schedule(s). Retention schedules prescribe a record's required length of retention and its disposition. Retention schedules are a type of classification scheme. This subsection does not cover the execution of a record's disposition, see subsection 1.1.

3.2.1. An *Application* MUST be able to assign a retention schedule to a record.
[Indiana 1.8.3; MoReq 5.1.4; PRO A.4.14; ISO 8.1.f]

3.2.2. An *Application* MUST be able to reassign a retention schedule to a record.
[PRO A.4.21]

3.2.3. An *Institution* MUST associate retention schedules with dispositions and retention periods and the reasons and sources for these determinations.
[Pitt 1b; MoReq 5.1.3, 5.1.11, 5.17, 5.10; PRO A.4.7, A.4.9, A.4.10, A.4.12; ISO 8.1.f, 9.2.c.1-3]

3.2.4. An *Institution* MUST be able to change the dispositions and retention periods of the retention schedules.
[Indiana 1.8.7; MoReq 5.1.15-16; PRO A.4.6, A.4.1]

3.2.5. An *Institution* MUST assign retention schedules to all of its records.
[Indiana 1.8.6]

3.3. Naming

This subsection covers the naming of a classification scheme and its classes within a recordkeeping system.

3.3.1. An *Application* SHOULD support a naming scheme for classification taxonomies.
[MoReq 3.1.4]

3.3.2. An *Application* MAY support user-defined naming schemes for classification taxonomies.
[MoReq 3.1.4]

3.3.3. An *Application* MAY support the use of controlled vocabulary terms to support the creation of naming schemes.
[MoReq 3.2.6, 3.2.8; PRO A.1.24; ISO 9.5.3]

3.3.4. An *Application* MAY use one of two strategies for creating naming schemes: a structured alpha/numeric system or a human understandable textual system.
[MoReq 3.2.2; PRO A.1.14-15]

3.3.5. An *Application* MAY support the mandatory use of a naming scheme.
[PRO A.1.20, A.1.36]

3.4. Assign Classification

This subsection covers the assigning of a record(s) to a class(es) within a classification scheme in a recordkeeping system. Although assigning a record to a scheme assigns meaning and prescribes actions to that record, the execution of those actions is not covered in this subsection. See subsection 1.1.

3.4.1. An *Institution* MUST classify records, assigning them to a pre-established class in a classification scheme.
[ISO 4.2.1-4.2.2]

3.4.2. An *Application* MUST assign all of the records it maintains to a class or multiple classes of a classification scheme.
[Indiana 1.8.3, 1.2.4; MoReq 6.1.1; PRO A.2.19, A.2.21, A.4.55]

3.4.3. An *Application* MUST be able to assign a classification to a particular record that overrides the classification of the group of records that individual record is assigned to.
[MoReq 5.1.14]

3.4.4. An *Application* MUST be able to reassign a record to a different class.
[MoReq 3.4.2, 5.1.16; PRO A.1.47, A.2.50, A.4.21]

3.4.5. An *Application* MAY support the use of controlled vocabulary terms to support the classification of records.
[PRO A.1.37]

3.4.6. An *Application* MAY support records being classified as vital records.
[MoReq 4.3.6]

3.5. Institution and Context

This subsection covers the institutional context into which a classification scheme within a recordkeeping system should fit.

3.5.1. An *Institution* SHOULD ensure that its recordkeeping applications are compatible with the institution's classification scheme(s).
[Indiana 1.3.1; MoReq 3.1.1]

3.5.2. An *Institution* SHOULD ensure its classification scheme(s) reflect its business processes.
[ISO 8.2.2.b, 9.5.2]

4. **Storage and Handling**

This section covers the institution's identification and management of records in recordkeeping systems which includes location tracking, versioning management, and unique identifier management. This section also discusses the integration of the recordkeeping systems into the business process and workflow of the institution. This section also covers the tracking of a record during its maintenance in a recordkeeping system. This section covers the management of versions of records while they are maintained in a recordkeeping system. This section covers the unique identification of a record, the maintenance of its logical relationships and the identification of its custodian(s) during its maintenance in a recordkeeping system. This section covers the preservation of the context, content, structure, and functionality of records in a recordkeeping system.

4.1. Maintain Integrity
This subsection covers the creation and capture of records in a recordkeeping system in a manner that maintains their integrity.

4.1.1. An *Application* MUST enforce data integrity at all times.
[MoReq 3.4.12; PRO A.9.2; ISO 8.3.6]

4.1.2. An *Application* MUST be able to maintain a record’s fixity.
[PRO A.2.14, A.2.18; InterPARES B.1.C; DoD c2.2.3.8]

4.2. Maintain Recordness
This subsection covers the preservation of a record’s recordness during its maintenance in a recordkeeping system.

4.2.1. An *Institution* MUST maintain records in a manner that allows them to correctly reflect the decision, action, or communication it documents.
[ISO 7.2.1]

4.2.2. An *Application* MUST maintain a record’s content, structure, and context that document the institution’s decisions, actions, and communications.
[Pitt 7]

4.2.3. *Procedures* MUST maintain the context, structure, and content of records throughout all recordkeeping activities.
[Pitt 9; PERM non dod5, 2]

4.2.4. *Procedures* MUST maintain the chain of custody of records throughout all recordkeeping activities.
[InterPARES B.1]

4.2.5. *Procedures* MUST maintain the logical boundaries and the relationships between records throughout all recordkeeping activities.
[Pitt 9b1, 9b2]

4.3. Location Tracking
This subsection covers the tracking of a record during its maintenance in a

recordkeeping system.

4.3.1. An *Application* MUST be able to track the location of records in a recordkeeping system.
[MoReq 4.4.1]

4.3.2. An *Application* MUST track a record's unique identifier, current location, time of movements, the person responsible for the movements, and the custodian of the record.
[MoReq 4.4.3; ISO 9.8.3]

4.3.3. *Procedures* MUST articulate steps that govern the receipt, removal, and movement of hardware and media that store electronic records.
[HIPAA 45CFR164.310]

4.4. Versioning

This subsection covers the management of versions of records while they are maintained in a recordkeeping system.

4.4.1. An *Application* SHOULD support versioning of the records it manages.
[Indiana 1.2.9]

4.4.2. An *Application* MUST, if it supports versioning, manage the relationship between the versions of the same record in a recordkeeping system.
[Indiana 1.2.8; DoD c2.2.3.18, c2.2.3.20]

4.4.3. An *Application* SHOULD, if it supports versioning, be able to identify the authoritative version of a record in a recordkeeping system that has multiple versions.
[InterPARES A.7]

4.4.4. An *Application* MUST, if it supports versioning, document the version changes of a record since its creation.
[InterPARES B.3]

4.5. Additional Records Attributes

This subsection covers the ability of a recordkeeping application to interoperate with other record creating and keeping applications while it maintains records.

4.5.1. An *Application* MUST uniquely identify the records it maintains.
[Pitt 6c; MoReq 7.1; PRO A.9.3; DoD c2.2.1.4, c2.2.4.1; PERM 15]

4.5.2. An *Application* MUST maintain the logical relationships between records in a recordkeeping system.
[MoReq 3.4.11; PRO A.2.24; DoD c2.2.3.17]

4.5.3. An *Application* MUST maintain the logical relationships between multiple versions of the same record.
[DoD c2.2.3.19]

4.5.4. An *Application* SHOULD identify the responsible custodian(s) of the records it maintains.
[PRO A.5.41]

4.6. Respond to Data Failure

This subsection covers the planning for and response to disasters that have an impact on the creation, capture, management, and use of records in a recordkeeping system.

4.6.1. *Institution* SHOULD create backup and failure mode procedures for its records and vital records.
[Indiana 1.9, 1.9.4; Pitt 2d; MoReq 4.3.7; InterPARES A.3; ISO 8.3.3]

4.6.2. *Procedures* SHOULD provide for the automated backup of the institution's records, metadata, audit trails, and configuration settings.
[MoReq 4.3, 4.3.1, 9.1.2-3; PRO A.9.11, A.9.17; DoD c2.2.9.1]

4.6.3. An *Application* MUST NOT hinder automated backup of the institution's records.
[DoD c2.2.9.1, MoReq 4.3.1]

4.6.4. *Procedures* SHOULD articulate the actions needed to be undertaken during primary system failure.
[Pitt 2d; MoReq 4.3.5; HIPAA 45CFR164.308]

4.6.5. *Infrastructure* SHOULD allow for backups to be stored at geographically distant locations.
[PRO A.9.12; DoD c2.2.9.2]

4.6.6. An *Application* SHOULD provide facilities for restoring data from backup data and returning the data stores to a consistent state.
[Pitt 4d; MoReq 11.3.5, 4.3.3, 4.3.4; PRO A.9.14-16; DoD c2.2.9.3, c2.2.2.9.3.1-2, c2.2.9.4-5; HIPAA 45CFR164.308]

4.6.7. *Institutions* SHOULD test and review backup and failure mode procedures.
[HIPAA 45CFR164.308, 45CFR164.310]

4.7. Intrusion Detection and Response

This subsection covers the detection and response to unauthorized access to and tampering of records in a recordkeeping system.

4.7.1. An *Institution* SHOULD create and maintain policies and procedures to detect, contain, and correct security violations.

[HIPAA 45CFR164.308, 45CFR164.310, 45CFR164.312]

4.7.2. *Procedures* MUST provide a reasonable guarantee that records are protected from tampering.
[Pitt 9a; PRO A.2.15; ISO 7.1.1, 8.2.2.c; HIPAA 45CFR164.306]

4.7.3. *Procedures* MUST prescribe periodic software security updates.
[HIPAA 45CFR164.308]

4.7.4. An *Institution* SHOULD perform a periodic review of its security procedures.
[InterPARES B.1.b; HIPAA 45CFR164.308]

4.7.5. An *Application* SHOULD be able to facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of records, or possible compromise of sensitive information.
[DoD c2.2.8.3.2]

4.7.6. An *Institution* SHOULD create and maintain policies and procedures to perform regular reviews of audit logs and log-in attempts.
[HIPAA 45CFR164.308]

5. Access

This section covers the institution's management of users' rights to view and/or receive records, including the development, management, and review of records and user security profiles and the management of access controls and authentication of users. This section also covers the recordkeeping system enabling users to search and discover records along with the system disseminating meaningful and functional records to users, including the management of searching mechanisms and query techniques. In addition it covers services to allow browsing and the proper rendering of complex records, a record's recordness, and redacted records.

5.1. Define Access Controls

This subsection covers the definition of access controls, or the assigning responsibility for the creation, modification, annotation, relocation, and destruction of records on the basis of a person's authority and capacity to carry out an administrative activity.

5.1.1. An *Institution* MUST explicitly assign responsibility for the creation, modification, annotation, relocation, and destruction of records on the basis of a person's authority and capacity to carry out an administrative activity.
[Indiana 1.7.2, InterPARES A.2]

5.1.2. An *Application* MUST confer exclusive capabilities upon people to exercise the responsibility for creation, modification, annotation, relocation, and destruction of records as defined by an institution.
[Indiana 1.4.1; DoD c2.2.5.2, C2.2.7.4; ISO 8.3.6; HIPAA 45CFR164.308;

InterPARES A.2]

5.1.3. An *Application* SHOULD manage the security level of the records it maintains.
[MoReq 9.3.3, 9.3.5]

5.1.4. An *Application* MUST NOT allow unauthorized changes to the records it maintains.
[Indiana 1.7.1; MoReq 3.2.1, 4.5.4, 6.1.4; PRO A.2.41; DoD c2.2.5.4; ISO 9.7.d]

5.1.5. An *Application* MUST NOT allow unauthorized creation of records.
[Pitt 8]

5.1.6. An *Application* MAY tailor its user interface to the user's appropriate access level.
[PRO A.8.9]

5.1.7. *Infrastructure* MUST NOT allow unauthorized access to the workstations and hardware that contain or provide access to records.
[HIPAA 45CFR164.310]

5.1.8. An *Institution* SHOULD demonstrate it has created and maintains a reasonable access criteria and it has successfully implemented the criteria.
[InterPARES A.2; ISO 8.3.6]

5.2. Management of Access Controls

This section covers the institution's management of users' rights to view and/or receive records. This includes the development, management, and review of records and user security profiles. It also includes the management of access controls and authentication of users.

5.2.1. An *Institution* MUST develop and implement access control rules for its records.
[MoReq 4.6.5; ISO 9.7; PERM 25; HIPAA 45CFR 164.308, 45CFR 164.312]

5.2.2. *Procedures* MUST insure that only authorized users gain access to records.
[MoReq 4.1.1; PRO A.5.25, A.5.42, A.5.46-50]

5.2.3. An *Institution* MAY designate people as custodians of records and the custodians are responsible for implementing the access control rules governing their records.
[PRO A.5.41, A.5.43-44; ISO 9.7.e]

5.2.4. An *Application* MUST limit search results to the records the user has rights to access.
[MoReq 4.1.10, 4.1.12, 8.1.28; PRO A.3.18, A.5.51-52, B.3.18]

5.3. Security Profiles and Authentication

This subsection covers the creation, management, assigning, reviewing, and modifying of security profiles for records in a recordkeeping system.

5.3.1. An *Institution* MUST create and modify records security profiles.
[ISO 4.3.5]

5.3.2. An *Application* MUST allow records security profiles to be created and modified.
[MoReq 9.3.5; PRO A.5.36]

5.3.3. An *Application* MUST allow record security profiles to be assigned to records.
[MoReq 4.6.1; PRO A.2.26, A.5.5, A.5.26, A.5.27; ISO 9.7.2]

5.3.4. An *Application* SHOULD allow time sensitive records profiles that are valid for a limited time period to be assigned to records and should automatically be switched to another records security profile when their valid time period expires.
[PRO A.5.38-39]

5.3.5. An *Application* MUST allow user security profiles to be created and modified.
[MoReq 9.1.8; PRO A.5.11, A.5.17-18, A.5.20-22]

5.3.6. An *Application* MUST assign or reassign user security profiles to people.
[MoReq 4.1.2, 4.1.5, 4.6.7, 9.1.7; PRO A.5.5, A.5.10, A.5.13, A.5.16, A.5.24; DoD c2.2.7.3]

5.3.7. *Infrastructure* SHOULD provide services for secure authentication.
[PRO A.5, A.5.1, A.5.11; DoD c2.2.7.1; HIPAA 45CFR164.312]

5.3.8. An *Application* MUST authenticate users before providing services.
[PRO A.5, A.5.1, A.5.11; DoD c2.2.7.1; HIPAA 45CFR164.312]

5.3.9. *Procedures* SHOULD allow for the periodic review of access control rules, records security profiles, and user security profiles.
[MoReq 4.6.12; PRO A.5.40; ISO 9.7; HIPAA 45CFR164.308]

5.3.10. *Procedures* SHOULD allow for the modification of access control rules, records security profiles, and user security profiles based on the findings of a review.
[HIPAA 45CFR164.308]

5.4. Searching

This subsection covers the capabilities of a recordkeeping system to search the records it maintains.

5.4.1. An *Application* MUST ensure all of its records and metadata are discoverable.
[Indiana 1.10.2-3; MoReq 8.1.4-5, 8.1.7; PRO A.3.4, A.3.6, A.3.8, A.3.17; PERM 18]

5.4.2. An *Application* SHOULD provide an integrated search interface.
[MoReq 8.1.2; PRO A.3.7]

5.4.3. An *Application* SHOULD support external search engines in addition to any integrated search interface.
[PRO A.3.19]

5.4.4. An *Application* MUST, if it has an integrated search interface, present search results.
[PRO A.3.15; DoD c2.2.6.8.5]

5.4.5. An *Application* MUST be able to render all records returned in a search results list.
[MoReq 8.2.1; PRO A.3.20; DoD c2.2.6.8.10]

5.4.6. An *Application* SHOULD provide capabilities to manage a search results list including, but not limited to, order, number of hits per page, filter results files, and save search results.
[MoReq 8.1.17, 8.1.24-25; DoD c2.2.6.8.5]

5.4.7. An *Application* MUST support searching by records' identifiers.
[MoReq 8.1.16, 8.1.23]

5.4.8. An *Application* SHOULD be able to save and reuse queries.
[MoReq 8.1.20; PRO A.3.11-12]

5.5. Query Techniques

This subsection covers the querying techniques a recordkeeping system employs to search the records it maintains.

5.5.1. An *Application* SHOULD support the full text search of the records and metadata it maintains.
[MoReq 8.1.8; DoD c3.2.9]

5.5.2. An *Application* SHOULD support searching metadata fields containing controlled vocabulary terms managed by thesauri.
[MoReq 8.1.10; PRO A.3.5; DoD c3.2.9]

5.5.3. An *Application* SHOULD support searching multiple metadata fields and/or full text of records.
[MoReq 8.1.6; PRO A.3.9; DoD c2.2.6.8.2]

5.5.4. An *Application* SHOULD support the use of Boolean and/or relational search operators such as "and" "or" "not" "less than" "greater than" "equal to."
[MoReq 9.1.8; PRO A.3.13; DoD c2.2.6.8.4]

5.5.5. An *Application* SHOULD support wild card and/or pattern matching searches.
[MoReq 8.1.11; PRO A.3.13; DoD c2.2.6.8.3]

5.5.6. An *Application* SHOULD support the iterative refinement of a search by adding search conditions to a previously run search—i.e. narrow a search.
[MoReq 8.1.21]

5.5.7. An *Application* MAY support word proximity searching.
[MoReq 8.1.12]

5.5.8. An *Application* MAY support searching null values.
[DoD c2.2.6.8.6]

5.5.9. An *Application* MAY support searching time intervals.
[MoReq 8.1.22]

5.6. Rendering Complex Objects

This subsection covers the ability of a recordkeeping system to deliver a record it maintains to a user in a manner that fully maintains the record's context, structure, and content.

5.6.1. An *Application* MUST render all of the components of a record and its metadata in a logical manner.
[Indiana 1.10.4; MoReq 8.2.3; PRO A.3.21]

5.6.2. An *Application* MUST be able to render records together with their associated metadata.
[MoReq 8.1.15; PRO A.3.24; DoD c2.2.3.21; PERM 23]

5.6.3. An *Application* MUST be able to render records on to appropriate output mediums which should at least include graphical display and printer output.
[MoReq 8.2, 8.3, 8.4.1; Pro A.3.25-26, A.3.28-29; PERM 3, 10, 14, 16, 17, 24, non DoD 2]

5.6.4. An *Application* SHOULD be able to render records into an open export format.
[PRO A.3.31]

5.6.5. An *Application* SHOULD be able to render records independently of their creating environments.
[MoReq 8.2.2; PRO A.3.22; DoD c3.2.14]

5.6.6. An *Application* SHOULD be able to render a record simultaneously for multiple users.
[PRO A.3.23; DoD c2.2.7.5]

5.6.7. An *Application* SHOULD be able to render all versions of a record.
[DoD c2.2.6.8.9]

5.7. Rendering Recordness

This subsection covers the ability of a recordkeeping system to deliver a record it maintains to a user in a manner that fully maintains the record's context, structure, and content.

5.7.1. An *Application* MUST render a record's content.
[Pitt 11, 12; MoReq 8.2.3; PRO A.3.21; PERM 2]

5.7.2. An *Application* MUST render a record's structure.
[Pitt 12, 12b, 12b1; PRO A.3.21; PERM 2]

5.7.3. An *Application* MUST render a record's context.
[Pitt 12, 12b1, 12c; ISO 7.25; PERM 2]

5.7.4. An *Application* MUST render a record's functionality.
[Pitt 11b; DoD c2.2.5.3]

5.8. Availability

This subsection covers the availability of needed records in a recordkeeping system.

5.8.1. An *Application* MUST ensure that records needed for their primary business functions are available.
[Indiana 1.10, 1.10.1; Pitt 12a; ISO 8.3.6]

5.8.2. An *Application* SHOULD ensure that records needed for secondary use are available.
[Indiana 1.10, 1.10.1; Pitt 12a]

5.8.3. An *Application* MUST ensure that its records are available in a timely manner.
[Indiana 1.10.1; Pitt 12a; ISO 8.3.6]

5.9. Browsing

This subsection covers the ability of a recordkeeping application to provide users the capability to browse records.

5.9.1. An *Application* SHOULD support the browsing of its classification schemes, including any hierarchical structure in which the records are managed.
[MoReq 8.1.13, 8.1.27, 3.1.7; PRO A.3.3; DoD c2.2.1.6]

5.10. Redaction

This section covers the management and execution of redacting records and the delivery of redacted versions of records to users.

5.10.1. *Procedures* SHOULD provide for the redaction of restricted content from records delivered to users that do not have the right to see the restricted output.
[Pitt 13; MoReq 9.3.10; PRO A.2.56]

5.10.2. An *Application* SHOULD be able to create redacted versions of textual, audio, and moving image records.
[MoReq 9.3.10]

5.10.3. An *Application* MUST NOT, if it can redact records, alter the content of a record while creating a redacted version of that record.
[Pitt 13a; PRO A.2.56]

6. **Design and Performance**

This section covers the software and hardware design and performance of the recordkeeping application, including system maintenance, scalability, design constraints, and testing and verification. This section also covers the application’s usability.

6.1. Testing and Verification

This subsection covers the testing and verification of a recordkeeping application’s and the infrastructure’s performance.

6.1.1. An *Institution* SHOULD determine an appropriate suite of tests against which the recordkeeping infrastructure and recordkeeping application will be measured and set acceptable ranges for system performance.
[Indiana 1.12; MoReq 11.2, 11.2.5]

6.1.2. *Procedures* SHOULD include provisions for regular execution of application and infrastructure tests.
[Indiana 1.12; PRO A.9.22]

6.1.3. *Infrastructure* SHOULD reliably pass all tests and perform within stated acceptable ranges.
[Indiana 1.12; Moreq 11.2]

6.1.4. An *Application* SHOULD reliably pass all tests and perform within stated acceptable ranges.
[Indiana 1.13; PRO A.9.22; MoReq 11.2, 11.2.1-4]

6.1.5. An *Application* SHOULD undergo formal verification and be provably correct.
[Pitt 4b, 4c]

6.2. System Maintenance

This subsection covers the maintenance of the recordkeeping application and infrastructure.

6.2.1. *Procedures* SHOULD contain provisions for all routine maintenance tasks which fall in line with industry best practices.
[Pitt 2c; CTG System]

6.2.2. An *Application* MUST allow convenient access to and the ability to modify any configuration parameters.
[MoReq 11.2.7, 9.1.1]

6.2.3. *Infrastructure* SHOULD provide the ability to monitor available storage capacity.
[MoReq 9.14; PRO A.9.21]

6.2.4. An *Institution* SHOULD determine the acceptable ranges for downtime and minimum numbers of simultaneous users.
[MoReq 11.3; DoD c3.1.3]

6.2.5. *Infrastructure* SHOULD be capable of fulfilling downtime and simultaneous user requirements laid out by the institution.
[MoReq 11.3]

6.3. User Interface

This subsection covers the user interfaces of a recordkeeping application.

6.3.1. An *Application* SHOULD provide a user interface which is easy to use.
[MoReq 11.1; PRO A.8.11; DoD c2.2.5.1]

6.3.2. An *Application* SHOULD follow generally accepted user interface guidelines by providing a consistent look and feel.
[PRO 8.1-3]

6.3.3. An *Application* MAY provide a remote login facility.
[MoReq A.9.7]

6.3.4. An *Application* SHOULD facilitate use by persons with disabilities by including accessibility features.
[PRO A.8.16]

6.3.5. An *Application* SHOULD provide meaningful error messages in the event of an error, and attempt to guide the user to an appropriate resolution.
[PRO A.8.7-8]

6.4. Scalability

This subsection covers scalability issues concerning the recordkeeping system.

6.4.1. An *Application* SHOULD be able to both scale up to large organizations, and scale down for smaller organizations.
[MoReq 11.2.6, 11.2.8]

6.4.2. *Institutions* SHOULD estimate its medium and long-term scalability requirements and determine acceptable ranges for various scalability metrics.
[PRO A.9.23]

6.4.3. An *Application* SHOULD be capable of fulfilling its institution's scalability requirements, and of operating within acceptable ranges.
[PRO A.9.23]

6.4.4. An *Application* SHOULD NOT impose any practical limit on the number of records which can be managed by the application.
[MoReq 6.3.5; PRO A.2.20]

6.4.5. An *Application* SHOULD provide the ability to synchronize multiple instances of all underlying data stores.
[DoD c2.2.3.24]

6.4.6. An *Application* SHOULD, when it offers remote or distributed services, use efficient network protocols which minimize the amount of data exchange required.
[PRO A.9.20]

6.5. Sustainability

This subsection covers the design constraints that affect sustainability of the recordkeeping application.

6.5.1. An *Application* SHOULD be designed around a flexible architecture which can evolve as the institution's needs change.
[PRO A.9.1]

6.5.2. An *Application* MAY support a distributed repository with multi-site service.
[PRO A.9.18]

6.5.3. An *Application* SHOULD provide at least one version of backward compatibility.
[DoD c2.1.4]

V. REQUIREMENTS FOR THE PRESERVATION OF UNIVERSITY ELECTRONIC RECORDS

This chapter describes the features, behaviors, and qualities that are necessary in order to preserve and ensure the continued accessibility and authenticity over time of electronic records at a college or university, written as requirements. Preservation is the whole of the activities and processes involved in the technical stabilization and physical and intellectual protection of resources through time. Those sources are:

- Indiana University, *Requirements for Electronic Records Management Systems (ERMS)*, Bloomington, IL: 2002 <http://www.indiana.edu/~libarch/ER/requirementsforrk.doc>.
  In this document referred to as: Indiana

- University of Pittsburgh, *Functional Requirements for Evidence in Recordkeeping*, Pittsburgh, PA: 1996 <http://web.archive.org/web/20001024112939/www.sis.pitt.edu/~nhprc/prog1.html>.
  In this document referred to as: Pitt

- Alan Kowlowitz and Kristine L. Kelly, *Functional Requirements to Ensure the Creation, Maintenance, and Preservation of Electronic Records*, Albany, NY: Center for Technology in Government, State Univeristy of New York, 1998 <http://www.ctg.albany.edu/publications/reports/functional/functional.pdf>.
  In this document referred to as: CTG

- IDA Programme of the European Commission, *Model Requirements for the Management of Electronic Records*, 2001 < http://ec.europa.eu/idabc/servlets/Doc?id=16847>.
  In this document referred to as: MoReq

- Public Records Office, *Functional Requirements for Electronic Records Management Systems*, Surrey, UK: 2002 <http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/pdf/requirementsfinal.pdf>.
  In this document referred to as: PRO

- InterPARES I Project, "Requirements for Assessing and Maintaining the Authenticity of Electronic Records," *in The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*, San Miniato, Italy: Archilab, 2005 <http://www.interpares.org/book/interpares_book_k_app02.pdf>
  In this document referred to as: InterPARES

- U.S. Department of Defense, *Design Criteria Standard for Electronic Records Management Software Applications* (DoD 5015.2-STD), Arlington, VA: 2002 <http://www.dtic.mil/whs/directives/corres/pdf/50152std_061902/p50152s.pdf>
  In this document referred to as: DoD

- International Organization for Standardization, *ISO 15489-I: Information and*

documentation—Records management
In this document referred to as: ISO

- San Diego Super Computer Center at the University of California, San Diego, *Preserving the Electronic Records Stored in a Records Management Application* (PERM Project), San Diego, CA: 2002 <http://www.sdsc.edu/PERM/Final-Report-December-20-2002.pdf>
  In this document referred to as: PERM

  Health Insurance Portability and Accountability Act, 45 C.F.R. § 160, 162, 164 (2005) <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title45/45cfrv1_02.tpl>.
  In this document referred to as: HIPAA

  A small number of additional requirements have been identified as a result of this research project and are attributed to The Fedora and the Preservation of University Electronic Records Project.
  In this document referred to as: Tufts-Yale

In addition, the project team surveyed the preservation system requirements literature and selected what it believes to be the seven most applicable to the university archives community. This literature is much less standardized than the recordkeeping system requirements literature, consisting mostly of more general research best practices statements. In the last two years, the situation has improved because of the landmark work completed by the National Archives and Records Administration's Electronic Records Archives Program Management Office. This grand and detailed statement of responsibilities must be considered the most significant work of its kind. The full list of the preservation system requirements documents includes:

- National Archives and Records Administration Electronic Records Archives Program Management Office, *Electronic Records Archives Requirements Document* (RD), Version 2.0, prepared by Integrated Computer Engineering (ICE), College Park, MD: 2003 <http://www.archives.gov/era/about/requirements.csv>.
  In this document referred to as: NARA

- *ISO 14721:2003: Space data and information transfer systems—Open archival information system—Reference model* (Geneva: International Organization for Standardization, 2003).
  In this document referred to as: ISO

- Research Libraries Group, *Trusted Digital Repositories: Attributes and Responsibilities,* Mountain View, CA: RLG, 2002 <http://www.rlg.org/legacy/longterm/repositories.pdf#search=%22Trusted%20Digital%20Repositories%3A%20Attributes%20and%20Responsibilities%22>
  In this document referred to as: TDR

- Research Library Group and National Archives and Records Administration, *An Audit*

Checklist for the Certification of Trusted Digital Repositories, Draft for Public Comment, Mountain View, CA: RLG, 2005 <http://www.rlg.org/en/pdfs/rlgnara-repositorieschecklist.pdf>.
In this document referred to as: CTDR

- van Diessen, Dr. R.J., *Preservation Requirements in a Deposit System: IBM/KB Long Term Preservation Study*, The Hague: IBM and Koninklijke Bibliotheek, 2002 <http://www.kb.nl/hrd/dd/dd_onderzoek/reports/3-preservation.pdf>.
  In this document referred to as: KB

- Yale University Library, *Requirements Document for the Rescue Repository*, New Haven, CT: Yale, 2004 <http://www.library.yale.edu/iac/documents/RescueRepositoryRequirements.pdf#search=%22Requirements%20Document%20for%20the%20Rescue%20Repository%22>.
  In this document referred to as: Yale

1. Common Services

This section covers information technology services that are necessary to support the preservation system, but not necessarily unique to that system, including operating systems, networking, and security. It is most likely that most common services would be offered by central information technology units or contractors. While the service activities these requirements call for would not be unique or unusual for IT units or contractors, the activities may be more be a more extensive and expensive undertaking than IT units or contractors normally carry out.[5]

1.1. Operating System Services

This subsection covers the core services needed to operate and administer the application platform, and provide an interface between application software and the platform.

1.1.1. The *Application* SHOULD function on well-supported operating systems and other core infrastructural software.
[CTDR D1.1]

1.1.2. The *Infrastructure* SHOULD provide tools to support system level testing.
[NARA 26.1]

1.1.3. The *Application* SHOULD generate notices to users.
[NARA 23.6]

1.1.4. The *Application* SHOULD support logging of all system events.
[NARA 24.1]

1.1.5. The *Application* SHOULD comply with relevant *de facto* and *de jure* operating systems standards.
[MoReq 11.4]

1.1.6. The *Institution* SHOULD have a process to stay current with the latest operating system security fixes.
[CTDR D1.10]

1.2. Network Services

This subsection covers the capabilities and mechanisms to support distributed applications requiring data access and applications interoperability in heterogeneous networked environments.

1.2.1. The *Infrastructure* SHOULD provide for networked access to records.
[NARA 19]

1.2.2. The networking *Infrastructure* SHOULD be appropriate to the access services

[5] See 3.1 Maintain Guide. The existing requirements literature on digital preservation is particularly sparse on these services, particularly when such services seem necessary for any computer application to operate effectively.

provided and the designated community.
[CTDR D2.1]

1.2.3. If data storage is outsourced or administered externally, there MUST be sufficient network *Infrastructure* to support this service.
[MoReq 11.6]

1.2.4. A network *Application* MUST be able to provide metadata necessary for preservation.
[MoReq 12.1.22]

1.2.5. The networking *Infrastructure* MUST support the security requirements of the Institution.
[ERA 13.6]

1.2.6. The networking *Infrastructure* SHOULD meet or exceed specified performance reliability requirements
[ERA 31.1–31.4]

1.3. Security Services

This subsection covers the capabilities and mechanisms to protect the records in the system. This includes intrusion detection and response and authentication of users. It does not cover all of the security requirements that are covered in the recordkeeping requirements.

1.3.1. An *Application* MUST enable the use of user security profiles.
[MoReq 9.1.8; PRO A.5.11, A.5.17-18, A.5.20-22]

1.3.2. An *Application* MUST enable the use of record security profiles.
[Indiana 1.2.8; DoD c2.2.3.18–c2.2.3.20; NARA 15.2.1]

1.3.3. *Procedures* MUST provide a reasonable guarantee that records are protected from tampering.
[Pitt 9a; PRO A.2.15; ISO 7.1.1, 8.2.2.c; HIPAA 45CFR164.306; NARA 13–14]

1.3.4. *Procedures* MUST prescribe periodic software security updates.
[HIPAA 45CFR164.308]

1.3.5. An *Application* MUST confer exclusive capabilities upon authorized people to exercise the responsibility for creation, modification, annotation, relocation, and destruction of records as defined by an institution.
[Indiana 1.4.1; DoD c2.2.5.2, c2.2.7.4; ISO 8.3.6; HIPAA 45CFR164.308; InterPARES A.2]

1.3.6. An *Application* SHOULD manage the security level(s) of the records it

maintains.
[MoReq 9.3.3, 9.3.5]

1.3.7. *Infrastructure* SHOULD provide services for secure authentication.
[PRO A.5, A.5.1, A.5.11; DoD c2.2.7.1; HIPAA 45CFR164.312]

1.3.8. An *Application* MUST authenticate users before providing services.
[PRO A.5, A.5.1, A.5.11; DoD c2.2.7.1; HIPAA 45CFR164.312; Yale A.4]

1.3.9. An *Application* MUST NOT allow unauthorized changes to the records it maintains.
[Indiana 1.7.1; MoReq 3.2.1, 4.5.4, 6.1.4; PRO A.2.41; DoD c2.2.5.4; ISO 9.7.d; Yale A.4, A.7; NARA 13]

1.3.10. An *Institution* SHOULD undertake a periodic system security analysis of its data systems and identify security risks and needs.
[CTDR D3.1]

1.3.11. An *Institution* SHOULD implement mechanisms to address each of the security needs identified in a system security analysis.
[CTDR D3.2]

1.3.12. *Natural People* MUST have delineated roles, responsibilities, and authorizations.
[CTDR D3.3]

2. **Ingest**
This section includes requirements describing accepting Submission Information Packages from Producers, preparing Archival Information Packages for storage, and ensuring that Archival Information Packages and their supporting Descriptive Information are stored within the Preservation System

2.1. Receive Submission
This subsection includes taking in records transferred from a Producer, a SIP, or an updated SIP produced through some internal processes. This includes accepting all types of records.

2.1.1. An *Institution* MUST confirm that a transfer is authorized.
[NARA 1.2.1; CTDR B1.4]

2.1.2. An *Application* MUST be able to ingest data files in the digital formats in which they were received, as specified by submission agreements.
[NARA 6.1–7.2]

2.1.3. An *Application* SHOULD be capable of accepting transfers via physical media.
[NARA 16.1]

2.1.4. An *Application* SHOULD be capable of accepting transfers electronically.
[NARA 16.2]

2.1.5. An *Application* SHOULD accept electronic records that are composed of more than one digital component.
[NARA 15.2]

2.1.6. An *Application* SHOULD be capable of interacting with all of the institution's recordkeeping applications.
[Indiana 1.6.2; MoReq 6.2.1; PRO A.2.2; NARA 1.10]

2.1.7. An *Application* SHOULD allow Producers to describe the link between record security profiles and records.
[MoReq 4.6.1; PRO A.2.26, A.5.5, A.5.26, A.5.27; ISO 9.7.2; NARA 8.9.5]

2.1.8. An *Institution* SHOULD provide the Producer with progress reports at specific predetermined points throughout the Ingest process.
[CTDR B1.7]

2.1.9. An *Institution* SHOULD mark the formal acceptance of preservation responsibility.
[CTDR B1.9]

2.2. Quality Assurance
This subsection include checking electronic records contained in a transfer, the SIP, in order to verify the success of that transfer.

2.2.1. An *Application* MUST confirm the success of a file transfer (verification of completeness and correctness).
[NARA 16.3; CTDR B1.6]

2.2.2. An *Application* SHOULD be able to technically validate that records components conform to technical file format standards.
[Yale B.4; NARA 5.8]

2.2.3. *Procedures* SHOULD provide for the intellectual validation (data content standard of the metadata is met) of the metadata the records preservation system creates or captures during ingest.
[Indiana 1.6.4; MoReq 6.1.1]

2.2.4. An *Institution* MUST actively produce benchmarks during Ingest in order to monitor the integrity of Archival Information Packages (AIPs).
[CTDRB3.7]

2.2.5. An *Institution* SHOULD confirm that the determinations of the feasibility of

preservation made during the process of appraisal are still valid.
[Tufts-Yale]

2.3. Generate AIP
This subsection includes requirements for transforming a SIP into an AIP that conforms to the data formatting and documentation standards.

2.3.1. An *Application* MUST uniquely identify the records it maintains.
[Pitt 6c; MoReq 7.1; PRO A.9.3; DoD c2.2.1.4, c2.2.4.1; PERM 15; Yale A.5; NARA 1.1.2.1, 19.1.14; CTDR B2.4–B2.5]

2.3.2. An *Application* MUST be able to bind records components together as part of an AIP.
[Tufts-Yale]

2.3.3. An *Institution* MUST define how AIPs are derived from SIPs.
[CTDR B2.1–B2.3]

2.3.4. An *Application* SHOULD facilitate the transformation of record components according to a format transformation plan.
[Tufts-Yale]

2.4. Generate Descriptive Information
This subsection includes extracting metadata from the records and also attaching metadata collected from other sources.

2.4.1. An *Institution* MUST identify the properties of the records it will preserve.
[CTDR B1.1]

2.4.2. An *Application* SHOULD be capable of automatically extracting metadata from the records it captures from a recordkeeping application (including representation information).
[Indiana 1.6.1; MoReq 6.1.6, 6.1.14; Yale B.5; NARA 3.3–3.5; CTDR 3.3, B3.4, B4.1]

2.4.3. An *Application* MUST allow people to manually enter metadata that cannot be automatically extracted from the records captured from a recordkeeping application.
[Indiana 1.6.3; MoReq 6.1.9; PRO A.2.38, PERM 12; NARA 3.3.1.2; CTDR B4.1]

2.4.4. *Procedures* MUST provide for the creation of necessary metadata during the capture process that did not exist before capture (including descriptive, technical, and contextual metadata necessary to document ingest).
[MoReq 6.1.9; PRO A.2.38, PERM 12, Indiana 1.2.3; Pitt 8a; MoReq 6.1.2, 6.1.3; ISO 7.2.1.b; NARA 3.3; CTDR B4.1]

2.4.5. An *Institution* MUST register records with a unique identifier.
[Yale A.5–A.6]

2.4.6. An *Application* MUST be able to technically validate the metadata it creates or captures.
[Indiana 1.6.4; MoReq 6.1.1]

2.4.7. An *Institution* SHOULD use representation information from appropriate community registries.
[CTDR B3.3]

2.4.8. An *Institution* SHOULD generate or acquire preservation metadata.
[CTDR B3.6]

2.5. Coordinate Updates
This subsection includes the transfer of AIPs to Archival Storage and descriptive information to Data Management. This may be the nexus between separate applications for Ingest, Archival Storage, and Data Management.

2.5.1. An *Application* MUST facilitate the transfer of records from Ingest into the record components store.
[Tufts-Yale]

2.5.2. An *Institution* MUST deposit AIPs into its preservation system according to its preservation system rules.
[Tufts-Yale]

2.5.3. An *Institution* MUST update information on preservation actions applied to acquired records.
[Tufts-Yale]

3. Archival Storage

This section includes requirements for the storage, management, and retrieval of Archival Information Packages.

3.1. Receive Data
This subsection includes the storage of AIPs that have successfully completed the Ingest process and now must be stored and maintained by the Archive.

3.1.1. An *Application* MUST generate storage identifiers and document them in the appropriate AIPs.
[Tufts-Yale]

3.1.2. An *Institution* SHOULD gauge anticipated frequency of utilization of AIPs in order to select the most appropriate storage devices or media.

[Tufts-Yale]

3.1.3. An *Application* MUST NOT modify electronic records to accommodate physical storage media.
[NARA 12.2]

3.1.4. An *Application* MAY be capable of adding an "object accession" event to the PDI history.
[Tufts-Yale]

3.2. Manage Storage Hierarchy
This subsection includes administering the record components storage media.

3.2.1. *Procedures* MUST allow for storage media to be maintained in an appropriate physical environment.
[MoReq 11.7.1; ISO 8.3.3; NARA 12.6]

3.2.2. An *Application* SHOULD support high-reliability and redundancy features such as clustering and hot spares.
[Tufts-Yale]

3.2.3. *Infrastructure* MUST be able to support migration to new Storage Hardware Environments.
[Tufts-Yale]

3.2.4. *Procedures* SHOULD describe backup and failure mode activities.
[HIPAA 45CFR164.308, 45CFR164.310; NARA 27.1; CTDR D1.2, D3.5]

3.3. Replace Media
This subsection describes when one of the primary media elements of the records components or administrative metadata store is refreshed or replaced. This can occur preventively or because errors have been detected on the media.

3.3.1. An *Application* MAY provide the automated capability to move electronic records to different media to accommodate new technology.
[NARA 12.1]

3.3.2. *Procedures* MUST allow for the migration of records from one storage media to another in a manner that preserves the recordness of the records.
[Indiana 1.9.1; MoReq 4.4; NARA 12.1, 28.2.4, 28.2.5; CTDR D1.7]

3.3.3. An *Instituion* SHOULD test new media for manufacturing defects before replacing media.
[Tufts-Yale]

3.3.4. An *Application* MAY automatically update PDI for all records affected by a

media replacement with a “media refresh” event.
[Tufts-Yale]

3.4. Error Checking

The AIPs for each record contain fixity information about records components (perhaps in the form of cryptographic checksums, message authentication codes, integrity check-values, modification detection codes, or message integrity codes). This subsection describes the periodic calculation of these fixity information values from the records components and the verification against the existing fixity information values.

3.4.1. *Procedures* SHOULD allow for periodic checks for media deterioration or loss.
[MoReq 11.7.2, 9.1.5; NARA 12.6–12; CTDR D1.5]

3.4.2. An *Institution* MUST actively monitor the integrity of AIPs.
[CTDR B3.7]

3.5. Disaster Recovery

Disaster preparation is listed more than once in these requirements, both here as part of the Archival Storage activity and later (See 4.1.1) as part of the Administration activity. This section refers to requirements necessary to ensure that records components are stored reliably. In 4.1.1 Disaster Preparation describes the development and maintenance of policies and procedures regarding disaster preparation.

3.5.1. An *Application* MUST NOT hinder automated backup of the institution’s records.
[Yale-Tufts]

3.5.2. *Procedures* SHOULD require backups to be stored at geographically distant locations.
[PRO A.9.12; DoD c2.2.9.2; Yale C.2; NARA 10.1.4]

3.5.3. An *Application* MUST provide facilities for restoring data from backup data and returning the data stores to a state prior to disaster.
[Pitt 4d; MoReq 11.3.5, 4.3.3, 4.3.4; PRO A.9.14-16; DoD c2.2.9.3, c2.2.2.9.3.1-2, c2.2.9.4-5; HIPAA 45CFR164.308; NARA 10.2.3]

3.5.4. *Infrastructure* SHOULD include tools for recovery of electronic records from failed media.
[NARA 12].

3.5.5. *Procedures* SHOULD provide for the automated backup of the preserved records and preservation metadata.
[MoReq 4.3, 4.3.1, 9.1.2-3; PRO A.9.11, A.9.17; DoD c2.2.9.1]

3.5.6. *Procedures* SHOULD articulate the actions needed to be undertaken during primary system failure.
[Pitt 2d; MoReq 4.3.5; HIPAA 45CFR164.308]

3.5.7. *Juridical People* SHOULD have clearly defined responsibilities to maintain service continuity and to recover from disasters.
[CTDR D3.6]

3.6. Provide Data

This subsection includes providing record components from storage in order to fulfill a request for a DIP from the Access system. This does not include providing copies of record components for internal functions of the Archive.

3.6.1. An *Application* MUST be able to retrieve all the records components of a record.
[Tufts-Yale]

3.6.2. An *Institution* MUST To gather the information required, from descriptive instruments and other preservation information, to satisfy requests for records and/or information about records.
[Tufts-Yale]

3.6.3. An *Application* MAY automatically update retrieval statistics when providing data.
[Tufts-Yale]

4. **Data Management**

This section includes requirements for populating, maintaining, and accessing data that refers to the operation of an Archive.

4.1. Administer Database

This subsection concerns maintaining the integrity of the Data Management database.

4.1.1. An *Application* MUST maintain any links established between ingested records and their metadata (and demonstrate referential integrity).
[Indiana 1.2.3; MoReq 6.1.3; ISO 7.1.c; CTDR B4.2]

4.1.2. An *Application* MUST be able to maintain a record’s Preservation Description Information, which documents all events which affect the record.
[Tufts-Yale]

4.1.3. An *Institution* MUST ensure that all actions taken which affect records cause a Preservation Description Information event to be generated.
[Tufts-Yale]

4.1.4. An *Application* MUST manage the relationship between the copies of records components in the system.[6]
[Indiana 1.2.8; DoD c2.2.3.18–c2.2.3.20; NARA 15.2.1]

4.1.5. An *Application* MUST manage the relationship between all copies of records components to their corresponding records.
[NARA 7.4]

4.1.6. An *Application* MAY support identification of the authoritative version (master copy or preservation copy) of a record component in the system.
[InterPARES A.7; NARA 18.5.1]

4.1.7. An *Application* MUST document any changes of a record component from the point of ingest.
[InterPARES B.3; NARA 8.1.5]

4.1.8. An *Application* MUST document items removed from the preservation system, including filenames, timestamps, and person identifiers.
[Yale D.3; NARA 15.8.1]

4.1.9. An *Application* MUST be able to track the logical location of its records copies.
[MoReq 4.4.1; NARA 10.2.4, 10.2.6; CTDR B2.4–B2.5, D1.3]

4.1.10. An *Application* MUST track a record’s unique identifier, current location, time of movements, and the natural person responsible for the movements.
[MoReq 4.4.3; ISO 9.8.3; NARA 10.2.6; CTDR B2.4–B2.5]

4.1.11. An *Institution* SHOULD document the security level of the records it maintains.
[MoReq 9.3.3, 9.3.5]

4.1.12. An *Application* MAY provide for management of templates within a template repository.
[NARA 7.2]

4.1.13. An *Application* MAY provide the capability to associate templates with sets of records.
[NARA 7.7.1–7.7.2]

4.1.14. An *Application* MUST allow records security profiles to be stored and

[6] The term “copies” could mean different things in different contexts. In a Fedora repository, different datastreams, surrogates, or derivatives of the same “original” could be considered copies. Record components, the different digital files that combine to form an electronic record, together could also be considered a copy of the record which they are derived from. The reassembly of those digital components would be considered to be a copy of the record from which the components derived.

modified.
[MoReq 9.3.5; PRO A.5.36; NARA 8.9.5, 16.6.2]

4.1.15. An *Application* MUST allow for the linkage between record security profiles and records.
[MoReq 4.6.1; PRO A.2.26, A.5.5, A.5.26, A.5.27; ISO 9.7.2; NARA 8.9.5]

4.1.16. An *Application* SHOULD allow time sensitive records profiles that are valid for a limited time period to be automatically switched to another records security profile when the time period expires.
[PRO A.5.38-39; NARA 13.13.2]

4.1.17. An *Application* MUST allow user security profiles to be stored and modified.
[MoReq 9.1.8; PRO A.5.11, A.5.17-18, A.5.20-22]

4.1.18. An *Application* MUST allow user security profiles to be linked to natural people.
[MoReq 4.1.2, 4.1.5, 4.6.7, 9.1.7; PRO A.5.5, A.5.10, A.5.13, A.5.16, A.5.24; DoD c2.2.7.3]

4.1.19. A *Juridical Person* SHOULD review records before a time-sensitive change is made in the records security profile.
[Tufts-Yale]

4.2. Perform Queries
This subsection includes queries performed by the Archive against records metadata. This might be for a Consumer search, a regular report for Administration, or a maintenance operation.

4.2.1. An *Application* MUST ensure all of its records metadata are discoverable.
[Indiana 1.10.2-3; MoReq 8.1.4-5, 8.1.7; PRO A.3.4, A.3.6, A.3.8, A.3.17; PERM 18; NARA 19]

4.2.2. An *Application* MAY provide integration with external discovery services.
[Tufts-Yale]

4.3. Generate Report
This subsection includes generating reports for internal administrative purposes.

4.3.1. An *Application* MUST report any unauthorized changes to the records it maintains.
[Indiana 1.7.1; MoReq 3.2.1, 4.5.4, 6.1.4; PRO A.2.4.1; DoD c2.2.5.4; ISO 9.7.d; Yale A.4, A.7; NARA 13]

4.3.2. An *Application* SHOULD be able to produce reports for Administration to document any system activity, including failure.

[MoReq 3.4.14; NARA 26.1, 26.3.1, 27.2.4; CTDR B5.2]

4.3.3. An *Application* MUST provide the capability to produce documentation of any reproduction or copy process and its effects, including the dates of the records' reproduction and the name of the responsible person and the impact of the reproduction process on the form of the records components (any changes the records components have undergone).
[InterPARES B.2]

4.4. Receive Database Updates
This subsection describes whenever record metadata is added, modified, or deleted. This can occur when a member of the Archive creates or modifies descriptive metadata, when technical metadata is created or derived from the records, or when supporting records (such as Representation Information (RI), Record Type Records or Producer Records) are updated.

4.4.1. An *Application* MUST enable the addition of new metadata bistreams or the versioning of an existing bitstream as appropriate.
[Tufts-Yale]

4.4.2. An *Application* MUST update an AIP with any new storage identifiers and fixity information.
[Tufts-Yale]

4.4.3. An *Application* MAY automatically update PDI for all affected records with "Metadata Update Event".
[Tufts-Yale]

4.4.4. An *Application* MUST provide the capability to destroy the components of any electronic record.
[NARA 1.5]

5. **Administration**
This section includes requirements for the demonstration of controls over records transfer, maintenance, and reproduction. This refers to auditable documentation proving the existence of such controls but does not include requirements for transfer, maintenance, and reproduction of the records themselves.

5.1. Negotiate Submission Agreement
This subsection includes the actions needed for an Archive and a Producer to generate a Submission Agreement to define the nature and scope of the records to transfer to the preservation system.

5.1.1. An *Institution* MUST specify all appropriate aspects of acquisition, maintenance, preservation, and access issues in written agreements with the Producer.

[CTDR B1.2]

5.1.2. An *Application* MAY automate the implementation of submission agreements.
[NARA 1.6–7]

5.1.3. An *Institution* MUST provide for transfer of custody of records to the Archive.
[NARA 1.3]

5.2. Manage System Configuration
Includes monitoring integrity, reporting Capability and Event Log, and system administration.

5.2.1. An *Institution* SHOULD develop a physical storage media tracking system.
[NARA 11.1]

5.2.2. An *Application* MUST support migration to a new preservation application Hardware Environments.
[Tufts-Yale]

5.2.3. An *Application* SHOULD facilitate the creation, maintenance, and distribution of documentation to support a demonstration of controls over records transfer, maintenance, and reproduction.
[InterPARES B.1; NARA 6; CTDR B3.8]

5.2.4. An *Institution* SHOULD perform a periodic review of its security procedures, including reanalysis of security threats or access management system failures.
[InterPARES B.1.b; HIPAA 45CFR164.308; CTDR B5.2]

5.2.5. An *Application* MUST be able to identify system failures.
[NARA 27.2.1; CTDR B5.2]

5.2.6. An *Application* MAY provide the facility to isolate and resolve failures.
[NARA 27.2.2–27.2.3]

5.2.7. *Procedures* SHOULD contain provisions for all routine maintenance tasks which fall in line with industry best practices.
[Pitt 2c; CTG System; NARA 27; CTDR D1.10]

5.2.8. An *Application* MUST allow convenient access to and the ability to modify any configuration parameters.
[MoReq 11.2.7, 9.1.1; NARA 27.4]

5.2.9. An *Institution* SHOULD identify the necessary hours of Application availability.

[MoReq 11.3; DoD c3.1.3]

5.2.10. *Infrastructure* SHOULD be capable of fulfilling downtime and simultaneous user requirements laid out by the Institution.
[MoReq 11.3]

5.2.11. An *Institution* SHOULD establish a policy to use Representation Information from appropriate international registries.
[CTDR B3.3]

5.2.12. An *Application* MAY provide the capability to monitor the overall system state in a consolidated manner.
[NARA 27.3]

5.2.13. An *Institution* MUST actively monitor the integrity of AIPs.
[CTDR B3.7]

5.2.14. *Infrastructure* SHOULD provide the ability to monitor available storage capacity.
[MoReq 9.14; PRO A.9.21; NARA 27.3.4]

5.2.15. An *Institution* SHOULD determine the maximum number of simultaneous users necessary for the operation of the preservation application.
[MoReq 11.3; DoD c3.1.3]

5.2.16. An *Application* MUST support a stasis mode where no changes are allowed.
[Tufts-Yale]

5.3. Archival Information Update
Includes transformation, and creating copies of records (versions).

5.3.1. An *Institution* MUST ensure that transformations are synchronized across multiple components of records, where appropriate (when content information may be conceived as identical).
[CTDR D1.4]

5.3.2. An *Application* SHOULD provide the capability to transform any ingested data file to a different, more persistent format.
[NARA 8.5-8.6]

5.3.3. An *Application* MUST persistently link the format versions of the same records together.
[PRO A.2.12; NARA 19.8.9]

5.3.4. An *Application* SHOULD automate the synchronization of transformations across multiple copies of records where appropriate.

[CTDR D1.4]

5.4. Physical Access Control
This subsection includes any mechanisms to restrict or allow physical access to elements of the Archive, including doors, locks, guards, etc.

5.4.1. An *Institution* SHOULD create and maintain policies and procedures to detect, contain, and correct security violations.
[HIPAA 45CFR164.308, 45CFR164.310, 45CFR164.312]

5.4.2. *Procedures* MUST provide a reasonable guarantee that records are protected from tampering.
[Pitt 9a; PRO A.2.15; ISO 7.1.1, 8.2.2.c; HIPAA 45CFR164.306]

5.4.3. An *Institution* MUST implement procedures to protect the Archive's facilities and equipment from unauthorized access, tampering, or theft. Such facilities include the physical surroundings of all storage devices and media.
[HIPAA 45CFR164.310]

5.4.4. *Natural People* MUST be authorized to access the Archives' facilities.
[HIPAA 45CFR164.308]

5.4.5. An *Institution* SHOULD implement physical safeguards for all workstations that access electronic records, restricting access to authorized users.
[HIPAA 45CFR164.310]

5.4.6. An *Institution* MUST NOT dispose of records storage media or make it available for re-use without assuring electronic records are removed.
[HIPAA 45CFR164.310]

5.5. Establish Standards and Policies
This subsection concerns the establishment of a variety of standards and policies concerning a variety of issues, including maintain, use rights (institution's management of user's rights).

5.5.1. An *Institution* MUST ensure that all actions taken which affect records cause a Preservation Description Information event to be generated.
[Tufts-Yale]

5.5.2. An *Institution* SHOULD demonstrate it has created and maintains a reasonable access criteria and it has successfully implemented the criteria.
[InterPARES B.1; ISO 8.3.6; NARA 13.2–13.4; CTDR B3.8]

5.5.3. *Procedures* SHOULD exist to redact restricted content from records.
[Pitt 13; MoReq 9.3.10; PRO A.2.56; NARA 20.11.2]

5.5.4. An *Institution* SHOULD establish procedures for the backup and recovery of its records and metadata associated with those records.
[Indiana 1.9, 1.9.4; Pitt 2d; MoReq 4.3.7; InterPARES A.3; ISO 8.3.3; NARA 10.2.3, 14.9; CTDR D1.2, D3.4]

5.5.5. An *Institution* MUST explicitly assign responsibility for the annotation, relocation, and destruction of records on the basis of a person's authority and capacity to carry out the activity (establishing user security profiles).
[Indiana 1.7.2; InterPARES A.2; MoReq 4.6.5, 9.3.5; PRO A.5.36; ISO 9.7; PERM 25; HIPAA 45CFR 164.308, 45CFR164.312; Yale A.5; NARA 13]

5.5.6. An *Institution* SHOULD create policies to manage the security level of the records it maintains.
[MoReq 9.3.3, 9.3.5]

5.5.7. An *Institution* MUST have a policy of not allowing any unauthorized changes to the records it maintains and must have a procedure for documenting any such unauthorized changes.
[Indiana 1.7.1; MoReq 3.2.1, 4.5.4, 6.1.4; PRO A.2.4.1; DoD c2.2.5.4; ISO 9.7.d; Yale A.4, A.7; NARA 13]

5.5.8. An *Institution* SHOULD perform a periodic review of its security procedures, including reanalysis of security threats or access management system failure.
[InterPARES B.1.b; HIPAA 45CFR164.308; CTDR B5.2]

5.5.9. An *Application* MAY provide the capability for Archive staff to create and maintain preservation and access plans, including the ability to alter plans.
[NARA 8.9.1–8.9.6; CTDR B3.10]

5.5.10. An *Application* MAY provide the capability for Archive staff to associate a preservation and access plan with records.
[NARA 8.9.5]

5.5.11. An *Institution* MAY accept all format types in which electronic records are created.
[Tufts-Yale]

5.5.12. *Procedures* MUST be created to guide the Ingest process.
[Tufts-Yale]

5.5.13. An *Institution* MUST have formats standards to guide the terms and conditions of transfer for Ingest.
[Tufts-Yale]

5.5.14. An *Institution* MUST have standards for what metadata it needs to properly document the Ingest process.

[Tufts-Yale]

5.5.15. An *Institution* SHOULD establish policies regarding rendering the functionality of record types.
[Pitt 11b; DoD c2.2.5.3; NARA 8.1.6.5, 20.11.3]

5.5.16. An *Institution* SHOULD establish policies defining the necessary elements of a response to a Consumer request (what is an appropriate response).
[CTDR B5.3]

5.5.17. An *Institution* SHOULD establish policies defining the description necessary to ensure records are discoverable.
[Indiana 1.10.2-3; MoReq 8.1.4-5, 8.1.7; PRO A.3.4, A.3.6, A.3.8, A.3.17; PERM 18; NARA 19]

5.5.18. *Procedures* SHOULD exist for managing record types with templates.
[NARA 7.2]

5.5.19. *Procedures* SHOULD exist for monitoring the available storage.
[Tufts-Yale]

5.5.20. *An Institution* SHOULD establish format transformation policies and plans to implant them.
[Tufts-Yale]

5.6. Audit Submission

This subsection includes verifying that submissions (either SIP or AIP) meet the specifications set out in the Submission Agreement.

5.6.1. An *Application* SHOULD be able to confirm that a transfer is authorized by a submission agreement.
[NARA 1.2; CTDR B1.4]

5.6.2. *Procedures* MUST stipulate validation of a records transfer against its corresponding submission agreement (terms and conditions of transfer).
[NARA 1.2.1–1.2.1.2; CTDR B1.6]

5.6.3. An *Institution* SHOULD provide feedback to the Producer on the success or failure of the transfer.
[Yale B.4; CTDR B1.7]

5.6.4. An *Institution* SHOULD create and maintain policies and procedures to detect, contain, and correct security violations.
[HIPAA 45CFR164.308, 45CFR164.310, 45CFR164.312; NARA 13]

6. **Preservation Planning**
This section includes evaluating the contents of the archive and periodically recommending archival information updates to migrate current archive holdings, developing recommendations for standards and policies, and monitoring changes in the technology environment and in the Designated Community's service requirements and Knowledge Base. This section also includes requirements for developing format transformation plans.

6.1. Monitor Designated Community
This subsection includes tracking the service requirements of Producers and Consumers as well as the state of the art of information technology.

6.1.1. An *Application* SHOULD enable the Archive to track changes in its service requirements and available product technologies to determine when preservation strategies are no longer viable.
[CTDR B3.9]

6.1.2. An *Institution* SHOULD monitor that consumer requests are responded to (see requirement 7.1.18).
[CTDR B5.5]

6.1.3. An *Institution* MUST periodically monitor the acceptability of chosen preservation strategies to existing Consumers and Producers.
[Tufts-Yale]

6.2. Monitor Technology
This includes monitoring preservation strategies standards and best practices against emerging digital technologies, information standards, and computing platforms.

6.2.1. *Juridical People* SHOULD monitor the state of the art of information technology in order to facilitate preservation planning.
[Tufts-Yale]

6.2.2. An *Application* MAY enable the Archive to track emerging digital technologies, information standards and computing platforms (i.e., hardware and software) to determine when preservation strategies are no longer viable.
[CTDR B3.9]

6.2.3. An *Institution* MUST periodically monitor the viability of chosen preservation strategies.
[CTDR B3.9]

6.3. Develop Preservation Strategies and Standards
This subsection includes requirements for developing recommendations for Archive standards and policies to mitigate issues of hardware and software obsolescence and media decay.

6.3.1. *Juridical People* MUST synthesize information about designated communities, technologies, system performance, inventory, and finances in order to recommend preservation strategies and standards.
[Tufts-Yale]

6.3.2. An *Institution* MUST develop plans for preserving records as long as needed and have a written mission statement that reflects a commitment to long-term preservation.
[Indiana 1.9; MoReq 11.7.4; PERM non dod 4; NARA 8.9; CTDR 3.1]

6.3.3. An *Institution* SHOULD develop strategies for ensuring the accessibility and functionality of records components over time.
[InterPARES A.4; ISO 8.3.5, 9.6]

6.3.4. An *Institution* SHOULD develop preservation action plans specifying the preservation actions to be taken to ensure the accessibility and functionality of templates of records components over time.
[InterPARES A.4; ISO 8.3.5, 9.6; NARA 8.9]

6.3.5. An *Institution* SHOULD develop plans for managing preservation metadata and attaching it to records.
[MoReq 5.3.10, 11.7.7; PERM 5, 6]

6.3.6. An *Institution* SHOULD develop strategies for redaction of restricted content from users.
[Pitt 13; MoReq 9.3.10; PRO A.2.56; NARA 20.11.2]

6.3.7. An *Institution* SHOULD develop strategies for rendering the functionality of types of records.
[Pitt 11b; DoD c2.2.5.3; NARA 8.1.6.5, 20.11.3]

6.3.8. An *Institution* SHOULD develop templates to manage record types.
[NARA 7.2]

6.4. Develop Packaging Designs and Migration Plans
This subsection includes the developing of new information package designs and detailed migration plans and prototypes, to implement Administration policies and directives.

6.4.1. An *Institution* MUST create rules for formulating Submission Information Packages.
[Tufts-Yale]

6.4.2. An *Institution* MUST create rules for formulating Archival Information Packages.
[Tufts-Yale]

6.4.3. An *Institution* MAY define records templates to automate Ingest and processing.
[NARA 7]

7. **Access**
This section includes requirements necessary in order to support Consumers in determining the existence, description, location and availability of records stored in the Archive, as well as applying controls to limit access to specially protected records, generating responses, and delivering the responses to Consumers.

7.1. Coordinate Access Activities
This includes the institution's coordinating of the execution of requests to successful completion.

7.1.1. *Procedures* MUST ensure that only authorized users gain access to records.
[MoReq 4.1.1; PRO A.5.25, A.5.42, A.5.46-50; NARA 13]

7.1.2. An *Application* MUST coordinate the application of user security profiles in order to respond to requests.
[MoReq 4.1.2, 4.1.5, 4.6.7, 9.1.7; PRO A.5.5, A.5.10, A.5.13, A.5.16, A.5.24; DoD c2.2.7.3]

7.1.3. An *Application* MUST ensure all of its records and metadata are discoverable.
[Indiana 1.10.2-3; MoReq 8.1.4-5, 8.1.7; PRO A.3.4, A.3.6, A.3.8, A.3.17; PERM 18; NARA 19]

7.1.4. An *Application* MUST be able to render all records returned in a search results list.
[MoReq 8.2.1; PRO A.3.20; DoD c2.2.6.8.10; NARA 19.8]

7.1.5. An *Application* MUST support searching by records' identifiers.
[MoReq 8.1.16, 8.1.23; NARA 19.1.14]

7.1.6. An *Application* MAY provide an integrated search interface.
[MoReq 8.1.2; PRO A.3.7; NARA 19.1, 21]

7.1.7. An *Application* MAY support resource discovery through external interfaces/mechanisms in addition to any integrated search interface.
[PRO A.3.19]

7.1.8. An *Application* SHOULD limit search results to the records the user has rights to access.
[MoReq 4.1.10, 4.1.12, 8.1.28; PRO A.3.18, A.5.51-52, B.3.18; NARA 19.8.3]

7.1.9. An *Application* SHOULD support the full text search of the records and metadata it maintains.
[MoReq 8.1.8; DoD c3.2.9; NARA 19.1.5–19.1.19

7.1.10. An *Application* SHOULD support searching metadata fields containing controlled vocabulary terms managed by thesauri.
[MoReq 8.1.10; PRO A.3.5; DoD c3.2.9; NARA 19.1.3]

7.1.11. An *Application* SHOULD support searching multiple metadata fields and/or full text of records.
[MoReq 8.1.6; PRO A.3.9; DoD c2.2.6.8.2; NARA 19]

7.1.12. An *Application* SHOULD support the use of Boolean and/or relational search operators such as “and” “or” “not” “less than” “greater than” “equal to.”
[MoReq 9.1.8; PRO A.3.13; DoD c2.2.6.8.4; NARA 19.1.19]

7.1.13. An *Application* SHOULD support wild card and/or pattern matching searches.
[MoReq 8.1.11; PRO A.3.13; DoD c2.2.6.8.3; NARA 19.1.24]

7.1.14. An *Application* SHOULD support the iterative refinement of a search by adding search conditions to a previously run search—i.e. narrow a search.
[MoReq 8.1.21; NARA 19.9]

7.1.15. An *Application* MAY support word proximity searching.
[MoReq 8.1.12; NARA 19.1.20]

7.1.16. An *Application* MAY support searching null values.
[DoD c2.2.6.8.6]

7.1.17. An *Application* MAY support searching time intervals.
[MoReq 8.1.22]

7.1.18. An *Institution* SHOULD track Consumer requests in order to determine if requests are responded to (see requirement 6.1.2).
[CTDR B5.5]

7.2. Generate Dissemination Information Package (DIP)
This section includes the retrieval of an AIP from Archival Storage and Data Management and the formation of a DIP in order to fulfill a dissemination request.

7.2.1. An *Application* MUST render all of the components of a record along with their associated metadata in a logical manner.
[Indiana 1.10.4; MoReq 8.1.15, 8.2.3; PRO A.3.21–A3.24; DoD c2.2.3.21; PERM 23; NARA 20.9, 20.11]

7.2.2. An *Application* MUST be able to render records on to appropriate output

media, which should at least include graphical display and printer output.
[MoReq 8.2, 8.3, 8.4.1; Pro A.3.25-26, A.3.28-29; PERM 3, 10, 14, 16, 17, 24, non dod 2; NARA 26.3.3, 26.4.1]

7.2.3. An *Application* SHOULD be able to render records into an open export format.
[PRO A.3.31; NARA 26.4.3]

7.2.4. An *Application* SHOULD be able to render records independently of their creating environments.
[MoReq 8.2.2; PRO A.3.22; DoD c3.2.14]

7.2.5. An *Application* SHOULD be able to render a record simultaneously for multiple users.
[PRO A.3.23, DoD c2.2.7.5]

7.2.6. An *Application* SHOULD be able to render all versions of a record.
[DoD c2.2.6.8.9]

7.2.7. An *Institution* SHOULD redact restricted content from records delivered to users that do not have the right to see the restricted content.
[Pitt 13; MoReq 9.3.10; PRO A.2.56; NARA 20.11.2]

7.3. Deliver Response
This subsection includes the online and off line delivery of responses (DIPs, result sets, reports, and assistance) to Consumers.

7.3.1. An *Application* MUST, if it has an integrated search interface, present search results.
[PRO A.3.15; DoD c2.2.6.8.5; NARA 19.8]

7.3.2. An *Application* MAY provide capabilities to manage a search results list including, but not limited to, order, number of hits per page, filter results files, and saving search results.
[MoReq 8.1.17, 8.1.24-25; DoD c2.2.6.8.5; NARA 19.8.4–19.12.3]

7.3.3. An *Institution* MUST answer a consumer request with an appropriate response, either a DIP fulfilling the entire request, a response denying the request, or a DIP fulfilling part of the request accompanied by a response clarifying why the request is only partially fulfilled.
[CTDR B5.3]

7.3.4. An *Institution* MUST disseminate DIPs that are authentic copies of their corresponding SIPs.
[CTDR B5.6]

7.3.5. An *Application* MUST render a record’s content.
[Pitt 11, 12; MoReq 8.2.3; PRO A.3.21; PERM 2; NARA 8.1.6.3, 20.11.1]

7.3.6. An *Application* MUST render a record’s structure.
[Pitt 12, 12b, 12b1; PRO A.3.21; PERM 2; NARA 8.1.6.6, 20.11.4]

7.3.7. An *Application* MUST render a record’s context.
[Pitt 12, 12b1, 12c; ISO 7.25; PERM 2]

7.3.8. An *Application* MUST render a record’s functionality.
[Pitt 11b; DoD c2.2.5.3; NARA 8.1.6.5, 20.11.3]

7.3.9. *Procedures* SHOULD provide for the redaction of restricted content from records delivered to users that do not have the right to see the restricted output.
[Pitt 13; MoReq 9.3.10; PRO A.2.56; NARA 20.11.2]

7.3.10. An *Application* MAY be able to create redacted versions of textual, audio, and moving image records.
[MoReq 9.3.10; NARA 18]

7.3.11. An *Application* MUST NOT, if it can redact records, alter the content of a record while creating a redacted version of that record.
[Pitt 13a; PRO A.2.56; NARA 18]

VI. Conclusion

This report presents the results of an effort to illustrate trustworthy electronic recordkeeping and preservation at a college or university. The Requirements for Trustworthy Recordkeeping and Preservation can assist institutions or university archives evaluate existing recordkeeping systems or preservation programs informally, particularly by giving them an outline of issues to address.

One of the strengths of the recordkeeping requirements chapter lies in the fact that it is based on a number of excellent efforts to describe the functional requirements for recordkeeping, from which the project team was able to select those requirements most applicable to university electronic records. The weakness of this section may be that most of the existing documents are focused on very large, complex, centralized recordkeeping environments with vast resources and the ability to purchase, design, create, and support massive recordkeeping applications. This is not the situation at most colleges and universities. Universities are usually not centralized institutions and are often incapable of controlling the recordkeeping environment in the way that is necessary to fulfill the requirements. Also, the resources necessary to administer and maintain such recordkeeping systems are beyond the means of most university archives. The cost of administering a recordkeeping application is enough to cripple the budgets of most archives or records management programs.

As mentioned earlier, the project staff had great difficulty arriving at an appropriate framework for organizing the requirements, particularly the set for recordkeeping. It may be that rather than fixing them in textual, linear document where they are in a fixed, numerical order, the requirement are instead best served by residing in database or other environment that allows users the flexibility to arrange individual requirements to suit their needs. For example, a user may only want to see the mandatory requirements or only the requirements that pertain to applications.

The strength of the records preservation requirements chapter is that it is one of the first efforts to define specific system requirements for each of the sections of the OAIS Reference Model. By distributing the existing literature into the sections and subsections of OAIS, it is easier to judge the status of the digital preservation literature to this point. The project team did not match several subsections of the model with requirements from the existing literature either because they do not exist or because they were hidden in a forest of detailed requirements. In those cases, the project team was forced to include Tufts-Yale requirements for necessary activities. In addition, there were two OAIS subsections the project team entirely skipped because there were no requirements from the existing literature and no obvious requirements came to light for each subsection. These lacunae might be fodder for the current analysis of the OAIS Reference Model, or may say something about the effectiveness of the requirements literature to date. There is still more to be accomplished in this area.

Despite these strengths, the requirements presented here are static; they are still not a true evaluation tool. To be used effectively in an assessment, the Requirements must be customized to fit a particular institutional environment. Institutions will need to identify specific sets of requirements which apply to their circumstances, extract them (by source, degree, or section) and use them in their own contexts. They may also need to add requirements, or further analyze existing requirements. This would transform the requirements into a living document in the Open Source style, in which users would contribute their developments back to the community.[7] Such an effort is beyond the scope of this project and would require an organization to manage the work and provide some sort of tool allowing others to rearrange the requirements and annotate them to suit individual or institutional needs. It is also clear that this is not the final set of functional requirements for electronic recordkeeping and preservation that will be created. MoReq, ISO 15489, CTDR, and the OAIS Reference Model are all currently undergoing revision. Each of these efforts would benefit from a complete understanding of the work of each of the other projects and from a conception of the requirements as dynamic documents to be applied in different ways in different situations.

Archives may be able to leverage the work of other projects to turn the Requirements for Trustworthy Recordkeeping and Preservation into a true evaluation tool. Possible projects that might be of assistance in this effort include the Center for Research Libraries' Digital Repository Certification project or the PLEDGE Project (PoLicy Enforcement in Data Grid Environments), which is developing tools and mechanisms to enable scalable policy expression in digital repositories.[8]

[7] From internal comments by Nancy Y. McGovern on draft trustworthy electronic recordkeeping project report, February 2006.

[8] For more information on the Digital Repository Certification project, see <http://www.rlg.org/en/page.php?Page_ID=580>, for more information on the PLEDGE project, see <http://pledge.mit.edu/>.

APPENDIX A: RECORDKEEPING REQUIREMENTS CROSSWALK

The table below presents the recordkeeping requirements from Section IV along with their corresponding place in the August 2005 draft for public comment version of the requirements and their location in the Trusted Digital Repository framework. The full text of the requirement, along with its appropriate sources, is listed in the "Requirement" column. The "Level" column describes if the corresponding row describes a section of the requirements (denoted by an "S"), a subsection (denoted by an "SS"), or an actual requirement (denoted by an "R").

Final Requirement Number	TDR Requirement Mapping	Aug 2005 Requirement Number	Requirement	Level
X	6.1	1	**Compliance** This section covers the identification of and compliance with laws, regulations, standards, and best practices that govern recordkeeping. This section also deals with an institution's ability to demonstrate its compliance with these laws, regulations, standards, and best practices.	S
x	X	1.1	***Identify Laws, Regulations, Standards, Best Practices, and Professional Ethics*** This subsection covers an institution's identification of the laws, regulations, standards, and best practices that govern its recordkeeping practices.	SS
x	6.1.1	1.1.1	An Institution MUST identify the laws, regulations, standards, best practices and professional ethics that affect its recordkeeping activities. [Pitt 1a, 1a1-3; ISO 5, 5a-e]	R
x	6.1.2	1.1.2	An Institution MUST track changes in the laws, regulations, standards, best practices and professional ethics that affect its recordkeeping activities. [Pitt 1c]	R
x	6.1.3	1.1.3	People MUST understand the laws, regulations, standards, best practices and professional ethics that affect their recordkeeping activities. [ISO 8.2.4]	R
x	X	1.2	***Comply with Laws, Regulations, Standards, Best Practices and Professional Ethics*** This subsection covers an institution's compliance with the laws, regulations, standards, and best practices that govern its recordkeeping practices.	SS
x	6.1.4	1.2.1	An Institution MUST comply with the laws, regulations, standards, best practices and professional ethics that affect its recordkeeping activities. [Indiana 1.l, 1.1.1; Pitt 1; MoReq 11.4, 11.5, 11.5.2-3, 11.5.5; PRO A.10.1, A.10.2; ISO 5, 5a-e, 7.1.h, 8.2.4]	R
x	6.1.5	1.2.2	A Recordkeeping Application MUST NOT include any features that do not comply with the laws, regulations, standards, best practices and professional ethics that affect the recordkeeping activities of the institution that the application serves. [MoReq 11.5.4]	R
x	X	1.3	***Demonstrate Compliance with Laws, Regulations, Standards, Best Practices and Professional Ethics*** This subsection covers the demonstration of its compliance with the laws, regulations, standards, and best practices that govern its recordkeeping practices.	SS
x	6.1.6	1.3.1	An Institution SHOULD be able to demonstrate its compliance with the laws, regulations, standards, best practices and professional ethics that affect its recordkeeping activities. [Pitt 1; ISO 5, 5a-e, 8.2.4]	R

2	1.1	2	**Creation and Capture** This section covers the creation and capture of records through recordkeeping systems. It covers the requirements to create records to document activities. It discusses the creation and capture of a variety of standard document types, complex documents, metadata, and relationships between records, along with the process of assigning unique identifiers and normalization during the creation and capture process.	S
2.1	X	2.1	***Generate Records*** This subsection covers the need to create required records to successfully conduct business activities.	SS
2.1.1			2.1.1. An Institution MUST document its activities by creating or capturing records when those activities commit the institution to action, render the institution accountable, or document an action, decision, or decision-making process. [ISO 9.1]	R
2.1.2	1.1.1	2.1.1	An Institution MUST generate records that document all of its defined functions and activities. [Indiana 1.2.1; ISO 7.1.a, 7.2.1, 8.2.5]	R
2.1.3	1.1.2	2.1.2	An Institution MUST ensure its recordkeeping applications are able to capture all of its records. [MoReq 6.1.1; PRO A.2.1, A.2.4, A.2.6]	R
2.1.4	1.1.3	2.1.3	Procedures SHOULD include quality control mechanics to ensure that accurate records are created. [Indiana 1.7; Pitt 7a]	R
2.1.5	1.1.4	2.1.4	People MUST have clearly defined responsibilities for creating records. [ISO 6.3]	R
2.1.6	1.1.7	2.1.5	People SHOULD only create records using documented recordkeeping applications and recordkeeping procedures. [Pitt 3a]	R
2.1.7	x	x	People MUST create and receive records as part of their daily work, and should do so in accordance with established policies, procedures, and standards. [ISO 2.3.2]	
2.1.8	x	x	An Application MUST enable the creation, reception, and keeping of records necessary to support business activities. [ISO 2.3.1]	
2.2	X	2.2	***Preserve Integrity*** This subsection covers the creation and capture of records in a recordkeeping system in a manner that preserves their integrity.	SS
2.2.1	1.1.8	2.2.1	A Recordkeeping Application MUST create and capture records in a manner that maintains the integrity and identity of the records. [Pitt 7a1; InterPARES B.1]	R
2.2.2	1.1.9	2.2.2	A Recordkeeping Application SHOULD validate the integrity of the records it creates and captures. [MoReq 6.2.1]	R
2.2.3	1.1.10	2.2.3	Procedures MUST articulate steps that maintain an unbroken custody of records during capture. [InterPARES B.1.a]	R
2.3	X	2.3	***Preserve Recordness*** This subsection covers the creation and capture of the essential aspects of a record in a recordkeeping system.	SS
2.3.1	1.1.11	2.3.1	An Application MUST be able to create and capture a record's context, structure, and content that together documents the institution's decisions, actions, or communications. [Pitt 7b, 7b1-4; MoReq 6.1.2; PRO A.2.8]	R
2.3.2	1.1.12	2.3.2	Procedures MUST provide for the creation and capture of records in a manner that allows them to correctly reflect the decisions, actions, or communications it documents. [Pitt 7c, 7c1-3; InterPARES A.1.a.i-v, A.1.b.i-iv, A.5]	R

2.4	4.1	2.4	***Support of Format Types*** This subsection covers the creation and capture of records of various formats.	SS
2.4.1	4.1.1	2.4.1	An Institution MUST have recordkeeping applications that together are able to create and capture all of the record formats the institution generates in the course of its business. [MoReq 6.1.1]	R
2.4.2	4.1.2	2.4.2	A Recordkeeping Application SHOULD be able to create and capture records with a variety of format types and structures. [Indiana 1.2.10; MoReq 6.1, 6.3, 6.3.1-2]	R
2.5	4.2	2.5	***Create and Capture Complex Documents*** This subsection covers the creation and capture of complex records.	SS
2.5.1	4.2.1	2.5.1	A Recordkeeping Application MUST, if it is used to manage complex records, be able to create and capture records in a manner that captures the structural integrity of its component parts. [MoReq 6.1.13, 6.3.1, 6.3.2; PRO A.2.5, A.2.8; ISO 7.2.1.a]	R
2.5.2	4.2.2	2.5.2	A Recordkeeping Application MAY adopt one of the following strategies for creating and capturing complex records: As a single compound record or as a series of linked simple records. [Indiana 1.2.7; MoReq 6.3.6]	R
2.6	4.3	2.6	***Create and Capture Relations between Records*** This subsection covers the creation and capture of the relationships between records.	SS
2.6.1	4.3.1	2.6.1	A Recordkeeping Application MUST be able to capture the relationships between records. [PRO A.8.17]	R
2.7	4.4	2.7	***Create and Capture Metadata*** This section covers the creation and capture of metadata associated with records a recordkeeping system creates and captures.	SS
2.7.1	4.4.1	2.7.1	A Recordkeeping Application SHOULD be capable of automatically extracting metadata for the records it creates and captures. [Indiana 1.6.1; MoReq 6.1.6, 6.1.14]	R
2.7.2	4.4.2	2.7.2	A Recordkeeping Application MUST allow people to manually enter metadata that cannot be automatically extracted from the records created and captured by the recordkeeping application. [Indiana 1.6.3; MoReq 6.1.9; PRO A.2.38]	R
2.7.3	4.4.3	2.7.3	Procedures MUST provide for the creation of necessary metadata during the creation and capture process that did not exist before creation or capture. [MoReq 6.1.9; PRO A.2.38]	R
2.7.4	4.4.4	2.7.4	A Recordkeeping Application MUST be able to technically validate the metadata it creates or captures. [Indiana 1.6.4; MoReq 6.1.1]	R
2.7.5	4.4.5	2.7.5	Procedures SHOULD provide for the intellectual validation of the metadata the recordkeeping system creates or captures during the creation or capture process. [Indiana 1.6.4; MoReq 6.1.1]	R
2.7.6	4.4.6	2.7.6	A Recordkeeping Application MUST be able to create and capture descriptive, technical, and contextual metadata. [PERM 12]	R
2.7.7	4.4.7	2.7.7	Procedures SHOULD provide for the creation and capture of descriptive, contextual, and technical metadata. [Indiana 1.2.3; Pitt 8a; MoReq 6.1.2, 6.1.3; ISO 7.2.1.b]	R
2.7.8	4.4.8	2.7.8	A Recordkeeping Application MUST create and capture records and their metadata in a manner that allows them to be persistently linked. [Indiana 1.2.3; MoReq 6.1.3; ISO 7.1.c]	R
2.8	4.5	2.8	***System Interaction*** This subsection covers the ability of a recordkeeping application to communicate and integrate with other recordkeeping and various record creating applications.	SS
2.8.1	4.5.1	2.8.1	A Recordkeeping Application SHOULD be capable of communication with all of the institution's other recordkeeping and record creating applications. [Indiana 1.6.2; MoReq	R

			6.2.1; PRO A.2.2]	
2.8.2	4.5.2	2.8.2	A Recordkeeping Application SHOULD provide an application programming interface to enable integration with other business applications. [PRO A.2.3]	R
X	X	2.9	***Identifier*** This subsection covers the assigning of unique identifiers to records in a recordkeeping system.	SS
2.7.9	4.4.9	2.9.1	A Recordkeeping Application MUST assign unique identifiers to the records it creates and captures. [Indiana 1.2.5; MoReq 7.1.5]	R
2.9	4.6	2.10	***Normalization*** This subsection covers capture and of standard format versions of records in a recordkeeping system captured in other formats. This section does not cover migration, which is covered in Section 7, Preservation. This deals specifically with normalization during the capture process.	SS
2.9.1	4.6.1	2.10.1	A Recordkeeping Application SHOULD be able to capture a standard format version of records it captures in its native format. [PRO A.2.12]	R
2.9.2	4.6.2	2.10.2	A Recordkeeping Application MUST persistently link the format versions of the same records together. [PRO A.2.12]	R
X Now Storage and Handling in preservation requirements	4.7	3	**Maintenance** This section covers the institution's identification and management of records in recordkeeping systems which includes location tracking, versioning management, and unique identifier management. This section also discusses the integration of the recordkeeping systems into the business process and workflow of the institution.	S
4.2	X	3.1	***Preserve Recordness*** This subsection covers the preservation of a record's recordness during its maintenance in a recordkeeping system. (Now Maintain Recordness)	SS
4.2.1	4.7.1	3.1.1	An Institution MUST maintain records in a manner that allows them to correctly reflect the decisions, action, or communication it documents. [ISO 7.2.1]	R
4.2.2	4.7.2	3.1.2	A Recordkeeping Application MUST maintain a record's content, structure, and context that documents the institution's decisions, actions, and communications. [Pitt 7]	R
4.3	X	3.2	***Location Tracking*** This subsection covers the tracking of a record during its maintenance in a recordkeeping system.	SS
4.3.1	4.7.3	3.2.1	A Recordkeeping Application MUST be able to track the location of records in a recordkeeping system. [MoReq 4.4.1]	R
4.3.2	4.7.4	3.2.2	A Recordkeeping Application MUST track a record's unique identifier, current location, time of movements, the person responsible for the movements, and the custodian of the record. [MoReq 4.4.3; ISO 9.8.3]	R
4.3.3	4.7.5	3.2.3	Procedures MUST articulate steps that govern the receipt, removal, and movement of hardware and media that store electronic records. [HIPAA 45CFR164.310]	R
4.4	X	3.3	***Versioning*** This subsection covers the management of versions of records while they are maintained in a recordkeeping system.	SS
4.4.1	4.7.6	3.3.1	A Recordkeeping Application SHOULD support versioning. [Indiana 1.2.9]	R
4.4.2	4.7.7	3.3.2	A Recordkeeping Application MUST, if it supports versioning, manage the relationship between the versions of the same record in a recordkeeping system. [Indiana 1.2.8; DoD c2.2.3.18, c2.2.3.20]	R

4.4.3	4.7.8	3.3.3	A Recordkeeping Application MAY, if it supports versioning, be able to identify the authoritative version of a record in a recordkeeping system that has multiple versions. [IP A.7]	R
4.4.4	4.7.9	3.3.4	A Recordkeeping Application MUST, if it supports versioning, document the version changes of a record since its creation. [InterPARES B.3]	R
X	X	3.4	***Summary for Management*** This subsection covers the ability of managers to receive reports on the management of records while they are maintained in a recordkeeping system.	SS
	6.2	3.4.1	A Recordkeeping Application SHOULD be able to produce reports for administrators on the activities of the records in a recordkeeping system. [MoReq 3.4.14]	R
	X	3.5	***Application Interoperability*** This subsection covers the ability of a recordkeeping application to interoperate with other record creating and keeping applications while it maintains records.	SS
		3.5.1	A Recordkeeping Application SHOULD be able to interoperate with its institution's other applications. [MoReq 10.8.1-4]	R
4.5	X	3.6	***Additional Records Attributes*** This subsection covers the unique identification of a record, the maintenance of its logical relationships and the identification of its custodian(s) during its maintenance in a recordkeeping system.	SS
4.5.1	4.7.10	3.6.1	A Recordkeeping Application MUST uniquely identify the records it maintains. [Pitt 6c; MoReq 7.1; PRO A.9.3; DoD c2.2.1.4, c2.2.4.1; PERM 15]	R
4.5.2	4.7.11	3.6.2	A Recordkeeping Application MUST maintain the logical relationships between records in a recordkeeping system. [MoReq 3.4.11; PRO A.2.24; DoD c2.2.3.17]	R
4.5.3	4.7.12	3.6.3	A Recordkeeping Application MUST maintain the logical relationships between multiple versions of the same record. [DoD c2.2.3.19]	R
4.5.4	4.7.13	3.6.4	A Recordkeeping Application SHOULD identify the responsible custodian(s) of the records it maintains. [PRO A.5.41]	R
3	2.1	4	**Classification** This section covers the development and management of classification schemes, which include records retention schedules, in recordkeeping systems. It also covers the assigning of records to classes within a classification scheme or multiple schemes and the institutional context of these schemes. Although assigning a record to a scheme assigns meaning and prescribes actions to that record, the execution of those actions is not covered in this section.	S
3.1	X	4.1	***Manage Scheme*** This subsection covers the creation, management, and modification of classification scheme(s) within a recordkeeping system. A classification scheme is a logical system used to arrange records. Usually, classes are related component parts that compose a scheme. This section does not cover the act of classifying records.	SS
3.1.1	2.1.1	4.1.1	A Recordkeeping Application MUST allow the creation and defining of a classification scheme. [MoReq 3.1.5; PRO A.1.3, A.4.1; ISO 9.3.A; DoD c2.2.1.1]	R
3.1.2	2.1.2	4.1.2	A Recordkeeping Application MAY allow the creation and defining of multiple classification schemes. [MoReq 3.1.8; PRO A.1.10]	R
3.1.3	2.1.3	4.1.3	A Recordkeeping Application MAY allow the creation and defining of a vital records classification scheme. [DoD c2.2.6.7]	R
3.1.4	2.1.4	4.1.4	A Recordkeeping Application MUST allow the changing, amending, deleting and adding to a classification scheme.	R

			[Indiana 1.8.7; MoReq 3.1.6, 3.4.1; PRO A.1.4, A.1.6, A.1.8, A.4.4, A.4.6]	
3.1.5	2.1.5	4.1.5	A Recordkeeping Application MUST ensure that classification names are unique. [PRO A.1.18]	R
3.1.6	2.1.6	4.1.6	A Recordkeeping Application SHOULD allow the closing of classes within a scheme so that no new records can be added to a closed class. [PRO A.1.7, A.1.41]	R
3.1.7	2.1.7	4.1.7	A Recordkeeping Application MUST NOT allow the deletion of classes that contain records. [PRO A.1.9]	R
3.1.8	2.1.8	4.1.8	A Recordkeeping Application SHOULD NOT impose any practical limits on the number of classes or class levels that exits within a scheme. [MoReq 3.1.3, 3.2.9; PRO A.1.28]	R
3.1.9	2.1.9	4.1.9	A Recordkeeping Application SHOULD report its classes, schemes, and records in a logical, usable fashion. [MoReq 3.2.10; ISO 9.3.6]	R
3.2	X	4.2	***Retention Schedules*** This subsection covers the management and modification of retention schedules along with act of assigning record(s) to a retention schedule(s). Retention schedules prescribe a record's required length of retention and its disposition. Retention schedules are a type classification scheme. This subsection does not cover the execution of a record's disposition.	SS
3.2.1	2.1.10	4.2.1	A Recordkeeping Application MUST be able to assign a retention schedule to a record. [Indiana 1.8.3; MoReq 5.1.4; PRO A.4.14; ISO 8.1.f]	R
3.2.2	2.1.11	4.2.2	A Recordkeeping Application MUST be able to reassign a retention schedule to a record. [PRO A.4.21]	R
3.2.3	2.1.12	4.2.3	An Institution MUST associate retention schedules with dispositions and retention periods and the reasons and sources for these determinations. [Pitt 1b; MoReq 5.1.3, 5.1.11, 5.17, 5.10; PRO A.4.7, A.4.9, A.4.10, A.4.12; ISO 8.1.f, 9.2.c.1-3]	R
3.2.4	2.1.13	4.2.4	An Institution SHOULD be able to change the dispositions and retention periods of the retention schedules. [Indiana 1.8.7; MoReq 5.1.15-16; PRO A.4.6, A.4.1]	R
3.3	X	4.3	***Naming*** This subsection covers the naming of a classification scheme and its classes within a recordkeeping system.	SS
3.3.1	2.1.14	4.3.1	A Recordkeeping Application SHOULD support a naming scheme for classification taxonomies. [MoReq 3.1.4]	R
3.3.2	2.1.15	4.3.2	A Recordkeeping Application MAY support user-defined naming schemes for classification taxonomies. [MoReq 3.1.4]	R
3.3.3	2.1.16	4.3.3	A Recordkeeping Application MAY support the use of controlled vocabulary terms to support the creation of naming schemes. [MoReq 3.2.6, 3.2.8; PRO A.1.24; ISO 9.5.3]	R
3.3.4	2.1.17	4.3.4	A Recordkeeping Application MAY use one of two strategies for creating naming schemes: a structured alpha/numeric system or a human understandable textual system. [MoReq 3.2.2; PRO A.1.14-15]	R
3.3.5	2.1.18	4.3.5	A Recordkeeping Application MAY support the mandatory use of a naming scheme. [PRO A.1.20, A.1.36]	R
3.4	X	4.4	***Assign Classification*** This subsection covers assigning record(s) to a class(es) within a classification scheme in a recordkeeping system. Although assigning a record to a scheme assigns meaning and prescribes actions to that record, the execution of those actions is not covered in this subsection.	SS
3.4.1	2.1.19	4.4.1	An Institution MUST classify records (assign records to a pre-established class in a classification scheme and, within each class, to the dossiers to which they belong. [ISO 4.2.1-4.2.2]	R

3.4.2	2.1.20	4.4.2	A Recordkeeping Application MUST assign all of the records it maintains to a class or multiple classes of a classification scheme. [Indiana 1.8.3, 1.2.4; MoReq 6.1.1; PRO A.2.19, A.2.21, A.4.55]	R
3.4.3	2.1.21	4.4.3	A Recordkeeping Application MUST be able to assign a classification to a particular record that overrides the classification of the group of records that contains the individual record. [MoReq 5.1.14]	R
3.4.4	2.1.22	4.4.4	A Recordkeeping Application MUST be able to reassign a record to a different class. [MoReq 3.4.2, 5.1.16; PRO A.1.47, A.2.50, A.4.21]	R
3.4.5	2.1.23	4.4.5	A Recordkeeping Application MAY support the use of controlled vocabulary terms to support the classification of records.[PRO A.1.37]	R
3.4.6	2.1.24	4.4.6	A Recordkeeping Application MAY support records being classified as vital records. [MoReq 4.3.6]	R
3.5	X	4.5	***Institution Context*** This subsection covers the institutional context into which a classification scheme within a recordkeeping system should fit.	SS
3.5.1	2.1.25	4.5.1	An Institution SHOULD ensure that its recordkeeping applications are compatible with the institution's classification scheme(s). [Indiana 1.3.1; MoReq 3.1.1]	R
3.5.2	2.1.26	4.5.2	An Institution SHOULD ensure its classification scheme(s) reflect its business processes. [ISO 8.2.2.b, 9.5.2]	R
1	2.2	5	**Retention and Disposition** This section covers the act of executing the disposition of records according to a records retention schedule. This usually means the act of removing records and their metadata from the recordkeeping application for either destruction or for transfer to a preservation application. The work also includes reviewing records before carrying out their disposition and the application of legal holds on records that are involved in a legal action, audit, or review. This section does not cover the creation and assigning of records retention schedules. See Subsection 4.2.	S
1.1	X	5.1	***Execution*** This subsection covers the execution of a record's disposition, which usually means either destruction or transfer to a semi-active, inactive, or preservation application.	SS
1.1.1	2.2.1	5.1.1	An Institution SHOULD dispose of records that no longer have operational value, either by permitting (arranging for) their destruction, or by transferring (arranging for) their transfer to a preservation repository. [ISO, 4.3.9, MoReq 5]	R
x	2.2.2	5.1.2	People MUST make a determination on the disposition of the record reviewed. [MoReq 5.2.10, 5.10]	R
1.1.2	2.2.3	5.1.3	Procedures MUST articulate the management of records disposition, in particular the destruction or transfer of records to a preservation system. [MoReq 5.2.10, 5.3.1; ISO 9.9]	R
1.1.3	2.2.4	5.1.4	Procedures MUST allow for the confidential destruction of all copies and instances of records scheduled for destruction. [MoReq 5.3.9; PRO A.4.74, B.3.26; DoD c2.2.10.6; ISO 9.9]	R
1.1.4	2.2.5	5.1.5	A Recordkeeping Application MUST confidentially destroy records scheduled for destruction in a manner that does not allow their recovery. [Pitt 10; MoReq 5.2.13, 5.3.14, 9.3.2; PRO A.4.67-68; DoD c2.2.6.63; ISO 9.9.a; HIPAA 45CFR164.310]	R
1.1.5	2.2.6	5.1.6	A Recordkeeping Application SHOULD be able to retain metadata about records that it destroys. [Pitt 10C; MoReq 5.2.15-16; DoD c2.2.6.4]	R
1.1.6	2.2.7	5.1.7	A Recordkeeping Application MUST be able to successfully transfer records scheduled for long-term retention to a preservation system. [MoReq 5.3.3, 5.3.5, 5.3.7; ISO 9.9.c]	R

1.1.7	2.2.8	5.1.8	A Recordkeeping Application SHOULD be able to retain metadata about records that it transfers to a preservation system. [DoD c2.2.6.5.4]	R
1.1.8	2.2.9	5.1.9	A Recordkeeping Application MAY track the actual time of disposition for a record based on the retention schedule assigned to that record. [PRO A.4.29, A.4.35-36, A.4.49]	R
1.2	X	5.2	***Compliance with Schedules*** The subsection covers the need for the disposition of records to be executed in compliance with appropriate retention schedules.	SS
1.2.1	2.2.10	5.2.1	An Institution MUST base the disposition of its records and audit trails on authorized and approved records retention schedules. [Indiana 1.4.2, 1.8, 1.8.1-2; MoReq 3.4.6; PRO A.1.46; ISO 7.1, 9.9]	R
3.2.5	2.2.11	5.2.2	An Institution MUST assign retention schedules to all of its records. [Indiana 1.8.6]	R
1.2.2	2.2.12	5.2.3	A Recordkeeping Application SHOULD be able to manage a variety of retention period configurations and disposition instructions. [DoD c2.2.2.2, c2.2.2.4, c2.2.2.4.1-3, c2.2.2.5]	R
1.2.3	2.2.13	5.2.4	A Recordkeeping Application SHOULD be able to adjust the scheduled disposition of a record if the content of the retention schedule that governs the record changes. [DoD c2.2.2.6, c2.2.2.7]	R
1.3	2.2.14	5.3	***Review*** This subsection covers the review of records before executing their disposition prescribed by their assigned retention schedule.	SS
1.3.1	2.2.15	5.3.1	Procedures MUST articulate steps for reviewing records before their scheduled disposition is executed. [MoReq 5.1.10; 5.2, ISO 9.9]	R
1.3.2	X	5.3.2	A Recordkeeping Application SHOULD alert people of and present to them for review records, including vital records, that has a pending disposition. [Indiana 1.8.4; MoReq 5.1.10, 5.2.1, 5.2.3-4, 5.2.7-8, 9.3.7; PRO A.4.32, A.4.45-46, A.4.64;]	R
1.4	X	5.4	***Legal Holds*** This subsection covers managing the process of suspending the execution of a record's disposition that is a part of any ongoing or reasonably expected legal action or proceedings, litigation, audit, investigation, or review.	SS
1.4.1	2.2.16	5.4.1	An Institution MUST be aware of ongoing and reasonably expected legal action or proceedings, litigation, audit, investigation, or review that involves or may involve its records and identify any records so affected. [Indiana 1.8.5; ISO 9.9]	R
1.4.2	2.2.17	5.4.2	Procedures MUST allow for the interruption of the scheduled disposition of a legal hold on records that are or are expected to be involved in legal action or proceedings, litigation, audit, investigation, or review. [Indiana 1.8.5; PRO A.4.25-26, A.4.38; DoD c2.2.6.4.1; ISO 9.9]	R
1.4.3	2.2.18	5.4.3	Procedures MUST allow for the appropriate lifting of legal holds on records and the resumption of their scheduled disposition. [PRO A.4.27; DoD c2.2.6.4.3]	R
X	5.1	6	**Protective** This section covers the recordkeeping institution's discovery and/or prevention of unauthorized, accidental, or unwanted deletion, change, or corruption of records. It covers access control, detection and response to unauthorized actions, protecting records from tampering, and disaster preparation. All of these activities are undertaken to maintain the data integrity and fixity of records.	S
5.1	X	6.1	***Define Access Controls*** This subsection covers the definition of access controls, or the assigning responsibility for the creation, modification, annotation, relocation, and destruction of records. A more detailed discussion of implementing access controls is in the Use Rights section.	SS

5.1.1	5.1.1	6.1.1	An Institution MUST explicitly assign responsibility for the creation, modification, annotation, relocation, and destruction of records on the basis of a person’s authority and capacity to carry out an administrative activity. [Indiana 1.7.2; IP A.2]	R
5.1.2	5.1.2	6.1.2	An Application MUST confer exclusive capabilities upon people to exercise the responsibility for creation, modification, annotation, relocation, and destruction of records as defined by an institution. [Indiana 1.4.1; DoD c2.2.5.2, c2.2.7.4; ISO 8.3.6; HIPAA 45CFR164.308; IP A.2]	R
5.1.3	5.1.3	6.1.3	An Application SHOULD manage the security level of the records it maintains. [MoReq 9.3.3, 9.3.5]	R
5.1.4	5.1.4	6.1.4	An Application MUST NOT allow unauthorized changes to the records it maintains. [Indiana 1.7.1; MoReq 3.2.1, 4.5.4, 6.1.4; PRO A.2.41; DoD c2.2.5.4; ISO 9.7.d]	R
5.1.5	5.1.5	6.1.5	An Application MUST NOT allow unauthorized creation of records. [Pitt 8]	R
5.1.6	5.1.6	6.1.6	An Application MAY tailor its user interface to the user’s appropriate access level. [PRO A.8.9]	R
5.1.7	5.1.7	6.1.7	Infrastructure MUST NOT allow unauthorized access to the workstations and hardware that contain or provide access to records. [HIPAA 45CFR164.310]	R
5.1.8	5.1.8	6.1.8	An Institution SHOULD demonstrate it has created and maintains a reasonable access criteria and it has successfully implemented the criteria. [InterPARES A.2; ISO 8.3.6]	R
4.7	X	6.2	***Intrusion Detection and Response*** This subsection covers the detection of and response to unauthorized access to and tampering of records in a recordkeeping system.	SS
4.7.1	5.1.9	6.2.1	An Institution SHOULD create and maintain policies and procedures to detect, contain, and correct security violations. [HIPAA 45CFR164.308, 45CFR164.310, 45CFR164.312]	R
4.7.2	5.1.10	6.2.2	Procedures MUST provide a reasonable guarantee that records are protected from tampering. [Pitt 9a; PRO A.2.15; ISO 7.1.1, 8.2.2.c; HIPAA 45CFR164.306]	R
4.7.3	5.1.11	6.2.3	Procedures MUST prescribe periodic software security updates. [HIPAA 45CFR164.308]	R
4.7.4	5.1.12	6.2.4	An Institution SHOULD perform a periodic review of its security procedures. [InterPARES B.1.b; HIPAA 45CFR164.308]	R
4.7.5	5.1.13	6.2.5	An Application SHOULD be able to facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of records, or possible compromise of sensitive information. [DoD c2.2.8.3.2]	R
4.7.6	5.1.14	6.2.6	An Institution SHOULD create and maintain policies and procedures to perform regular reviews of audit logs and log-in attempts. [HIPAA 45CFR164.308]	R
4.6	X	6.3	***Disaster Preparation*** This subsection covers the planning for and response to disasters that have an impact on the creation, capture, management, and use of records in a recordkeeping system.	SS
4.6.1	5.1.15	6.3.1	Institution SHOULD create backup and failure mode procedures for its records and vital records. [Indiana 1.9, 1.9.4; Pitt 2d; MoReq 4.3.7; InterPARES A.3; ISO 8.3.3]	R
4.6.2	5.1.16	6.3.2	Procedures SHOULD provide for the automated backup of the institution’s records, metadata, audit trails, and configuration settings. [MoReq 4.3, 4.3.1, 9.1.2-3; PRO A.9.11, A.9.17; DoD c2.2.9.1]	R
4.6.3	5.1.17	6.3.3	An Application MUST NOT hinder automated backup of the institution’s records. [DoD c2.2.9.1, MoReq 4.3.1]	R
4.6.4	5.1.18	6.3.4	Procedures SHOULD articulate the actions needed to be undertaken during primary system failure. [Pitt 2d; MoReq	R

			4.3.5; HIPAA 45CFR164.308]	
4.6.5	5.1.19	6.3.5	Infrastructure SHOULD allow for backups to be stored at geographically distant locations. [PRO A.9.12; DoD c2.2.9.2]	R
4.6.6	5.1.20	6.3.6	An Application SHOULD provide facilities for restoring data from backup data and returning the data stores to a consistent state. [Pitt 4d; MoReq 11.3.5, 4.3.3, 4.3.4; PRO A.9.14-16; DoD c2.2.9.3, c2.2.9.3.1-2, c2.2.9.4-5; HIPAA 45CFR164.308]	R
4.6.7	5.1.21	6.3.7	Institutions SHOULD test and review backup and failure mode procedures. [HIPAA 45CFR164.308, 45CFR164.310]	R
4.1	X	6.4	***Data Integrity*** This subsection covers the enforcement of the data integrity of records in a recordkeeping system.	SS
4.1.1	5.1.22	6.4.1	A Recordkeeping Application MUST enforce data integrity at all times. [MoReq 3.4.12; PRO A.9.2; ISO 8.3.6]	R
X	X	6.5	***Record Fixity*** This subsection covers the maintenance of the fixity of records in a recordkeeping system.	SS
4.1.2	5.1.23	6.5.1	A Recordkeeping Application MUST be able to maintain a record's fixity. [PRO A.2.14, A.2.18; InterPARES B.1.C; DoD c2.2.3.8]	R
X	4.8	7	**Preservation** This section covers the recordkeeping system's procedures and planning process to mitigate issues of media decay and hardware and software obsolescence and to allow the interoperability and openness of its records. This also concerns the ability of a recordkeeping system to transfer records to a preservation system.	S
X	2.3	7.1	***Planning*** This subsection covers the process of establishing plans for preserving records in a recordkeeping system over time.	SS
X	2.3.1	7.1.1	An Institution SHOULD establish plans for preserving records as long as needed. [Indiana 1.9; MoReq 11.7.4; PERM non dod 4]	R
X	2.3.2	7.1.2	An Institution SHOULD establish plans for ensuring the accessibility and functionality of records over time; these may include migration, emulation, and normalization plans. [InterPARES A.4; ISO 8.3.5, 9.6]	R
X	2.3.3	7.1.3	An Institution SHOULD establish plans for managing preservation metadata and attaching it to records. [MoReq 5.3.10, 11.7.7; PERM 5, 6]	R
X	X	7.2	***Preservation System Integration*** This subsection covers the ability of a recordkeeping application to export records to a preservation system.	SS
1.1.9	4.8.1	7.2.1	A Recordkeeping Application SHOULD be able to export records to a preservation system. [PRO A.4.50, A.4.58; PERM non dod 1]	R
1.1.9	4.8.2	7.2.2	A Recordkeeping Application MUST, if it can export records to a preservation system, export records in a manner that preserves their recordness. [PRO A.4.50-52; InterPARES A.8; DoD c2.2.6.5.3; PERM non dod 1]	R
X	X	7.3	***Media Issues*** This subsection covers the management of storage media and the migration of records in a recordkeeping system from one storage media to another.	SS
X	4.8.3	7.3.1	Procedures MUST allow for storage media to be maintained in an appropriate physical environment. [MoReq 11.7.1; ISO 8.3.3]	R
X	4.8.4	7.3.2	Procedures SHOULD allow for periodic checks for media deterioration. [MoReq 11.7.2, 9.1.5]	R

X	4.8.5	7.3.3	Procedures MUST allow for the migration of records from one storage media to another in a manner that preserves the recordness of the records. [Indiana 1.9.1; MoReq 4.4]	R
X	X	7.4	***Technology Obsolescence*** This subsection covers the prevention of records in a recordkeeping system being stranded on obsolete technologies.	SS
X	2.3.4	7.4.1	An Institution MUST plan for and execute strategies for preserving the recordness of their records as it uses new technologies and discontinues use of old ones. [InterPARES A.4; DoD c2.2.10.3, c2.2.10.3.1-4]	R
X	2.3.5	7.4.2	An Institution SHOULD select open, well-documented, and widely-accepted document formats for its record creation in order to combat technology obsolesce. [MoReq 11.7.5]	R
X	X	7.5	***Preserve Recordness*** This subsection covers the preservation of the context, content, structure, and functionality of records in a recordkeeping system.	SS
4.2.3	4.7.14	7.5.1	Procedures MUST preserve context, structure, and content of records throughout all recordkeeping activities. [Pitt 9; PERM non dod5, 2]	R
	X	7.5.2	Procedures MUST preserve the functionality and essential appearance of records throughout all recordkeeping activities. [DoD c2.2.5.3; ISO 8.3.5]	R
4.2.4	4.7.15	7.5.3	Procedures MUST preserve the chain of custody of records throughout all recordkeeping activities. [InterPARES B.1]	R
4.2.5	4.7.16	7.5.4	Procedures MUST preserve the logical boundaries and the relationships between records throughout all recordkeeping activities. [Pitt 9b1, 9b2]	R
5.2	2.4	8	**Use Rights** This section covers the institution's management of users' rights to view and/or receive records. This includes the development, management, and review of records and user security profiles. It also includes the management of access controls and authentication of users.	S
X	X	8.1	***Access Controls*** This subsection covers the development and management of processes that control the access of records in a recordkeeping system.	SS
5.2.1	2.4.1	8.1.1	An Institution MUST develop and implement access control rules for its records. [MoReq 4.6.5; ISO 9.7; PERM 25; HIPAA 45CFR 164.308, 45CFR 164.312]	R
5.2.2	2.4.2	8.1.2	Procedures MUST insure that only authorized users gain access to records. [MoReq 4.1.1; PRO A.5.25, A.5.42, A.5.46-50]	R
5.2.3	2.4.3	8.1.3	An Institution MAY designate people as custodians of records and the custodians are responsible for implementing the access control rules governing their records. [PRO A.5.41, A.5.43-44; ISO 9.7.e]	R
5.2.4	2.4.4	8.1.4	A Recordkeeping Application SHOULD limit search results to the records the user has rights to access. [MoReq 4.1.10, 4.1.12, 8.1.28; PRO A.3.18, A.5.51-52, B.3.18]	R
5.3	5.2	8.2	***Record Security Profile*** This subsection covers the creation and management of security profiles for records in a recordkeeping system. This subsection also covers the assigning of a security profile to a record in a recordkeeping system.	SS
5.3.1	X	X	An Institution MUST create and modify records security profiles. [[ISO 4.3.5]]	
5.3.2	5.2.1	8.2.1	A Recordkeeping Application MUST allow records security profiles to be created and modified. [MoReq 9.3.5; PRO A.5.36]	R

5.3.3	5.2.2	8.2.2	A Recordkeeping Application MUST allow record security profiles to be assigned to records. [MoReq 4.6.1; PRO A.2.26, A.5.5, A.5.26, A.5.27; ISO 9.7.2]	R
5.3.4	5.2.3	8.2.3	A Recordkeeping Application SHOULD allow time sensitive records profiles that are valid for a limited time period to be assigned to records and should automatically be switched to another records security profile when their valid time period expires. [PRO A.5.38-39]	R
X	X	8.3	***User Security Profile*** This subsection covers the creation and management of security profiles for users who use records in a recordkeeping system. This subsection also covers the assigning of a security profile to a user who uses records in a recordkeeping system.	SS
5.3.5	5.2.4	8.3.1	A Recordkeeping Application MUST allow user security profiles to be created and modified. [MoReq 9.1.8; PRO A.5.11, A.5.17-18, A.5.20-22]	R
5.3.6	5.2.5	8.3.2	A Recordkeeping Application MUST assign or reassign user security profiles to people. [MoReq 4.1.2, 4.1.5, 4.6.7, 9.1.7; PRO A.5.5, A.5.10, A.5.13, A.5.16, A.5.24; DoD c2.2.7.3]	R
X	X	8.4	***Authentication*** This subsection covers the process of authenticating users—verifying a user is who he or she purports to be—who are trying to use records in a recordkeeping system.	SS
5.3.7	5.2.6	8.4.1	Infrastructure SHOULD provide services for secure authentication. [PRO A.5, A.5.1, A.5.11; DoD c2.2.7.1; HIPAA 45CFR164.312]	R
5.3.8	5.2.7	8.4.2	A Recordkeeping Application MUST authenticate users before providing services. [PRO A.5, A.5.1, A.5.11; DoD c2.2.7.1; HIPAA 45CFR164.312]	R
X	X	8.5	***Review Security Profiles*** This subsection covers the process of reviewing and modifying user and record security profiles.	SS
5.3.9	5.2.8	8.5.1	Procedures SHOULD allow for the periodic review of access control rules, records security profiles, and user security profiles. [MoReq 4.6.12; PRO A.5.40; ISO 9.7; HIPAA 45CFR164.308]	R
5.3.10	5.2.9	8.5.2	Procedures SHOULD allow for the modification of access control rules, records security profiles, and user security profiles based on the findings of a review. [HIPAA 45CFR164.308]	R
X	4.9	9	**Discovery and Delivery** This section covers the recordkeeping system enabling users to search and discover records along with the system disseminating meaningful and functional records to users. This includes the management of searching mechanisms and query techniques. In addition it covers services to allow browsing and the proper rendering of complex records, a record's recordness, and redacted records.	S
5.3	X	9.1	***Searching*** This subsection covers the capabilities of a recordkeeping system to search the records it maintains.	SS
5.4.1	4.9.1	9.1.1	A Recordkeeping Application MUST ensure all of its records and metadata are discoverable. [Indiana 1.10.2-3; MoReq 8.1.4-5, 8.1.7; PRO A.3.4, A.3.6, A.3.8, A.3.17; PERM 18]	R
5.4.2	4.9.2	9.1.2	A Recordkeeping Application SHOULD provide an integrated search interface. [MoReq 8.1.2; PRO A.3.7]	R
5.4.3	4.9.3	9.1.3	A Recordkeeping Application SHOULD support external search engines in addition to any integrated search interface. [PRO A.3.19]	R
5.4.4	4.9.4	9.1.4	A Recordkeeping Application MUST, if it has an integrated search interface, present search results. [PRO A.3.15; DoD c2.2.6.8.5]	R

5.4.5	4.9.5	9.1.5	A Recordkeeping Application MUST be able to render all records returned in a search results list. [MoReq 8.2.1; PRO A.3.20; DoD c2.2.6.8.10]	R
5.4.6	4.9.6	9.1.6	A Recordkeeping Application SHOULD provide capabilities to manage a search results list including, but not limited to, order, number of hits per page, filter results files, and saving search results. [MoReq 8.1.17, 8.1.24-25; DoD c2.2.6.8.5]	R
5.4.7	4.9.7	9.1.7	A Recordkeeping Application MUST support searching by records' identifiers. [MoReq 8.1.16, 8.1.23]	R
5.4.8	4.9.8	9.1.8	A Recordkeeping Application SHOULD be able to save and reuse queries. [MoReq 8.1.20; PRO A.3.11-12]	R
5.5	X	9.2	***Query Techniques*** This subsection covers the searching techniques a recordkeeping system employs to search the records it maintains.	SS
5.5.1	4.9.9	9.2.1	A Recordkeeping Application SHOULD support the full text search of the records and metadata it maintains. [MoReq 8.1.8; DoD c3.2.9]	R
5.5.2	4.9.10	9.2.2	A Recordkeeping Application SHOULD support searching metadata fields containing controlled vocabulary terms managed by thesauri. [MoReq 8.1.10; PRO A.3.5; DoD c3.2.9]	R
5.5.3	4.9.11	9.2.3	A Recordkeeping Application SHOULD support searching multiple metadata fields and/or full text of records. [MoReq 8.1.6; PRO A.3.9; DoD c2.2.6.8.2]	R
5.5.4	4.9.12	9.2.4	A Recordkeeping Application SHOULD support the use of Boolean and/or relational search operators such as "and" "or" "not" "less than" "greater than" "equal to." [MoReq 9.1.8; PRO A.3.13; DoD c2.2.6.8.4]	R
5.5.5	4.9.13	9.2.5	A Recordkeeping Application SHOULD support wild card and/or pattern matching searches. [MoReq 8.1.11; PRO A.3.13; DoD c2.2.6.8.3]	R
5.5.6	4.9.14	9.2.6	A Recordkeeping Application SHOULD support the iterative refinement of a search by adding search conditions to a previously run search—i.e. narrow a search. [MoReq 8.1.21]	R
5.5.7	4.9.15	9.2.7	A Recordkeeping Application MAY support word proximity searching. [MoReq 8.1.12]	R
5.5.8	4.9.16	9.2.8	A Recordkeeping Application MAY support searching null values. [DoD c2.2.6.8.6]	R
5.5.9	4.9.17	9.2.9	A Recordkeeping Application MAY support searching time intervals. [MoReq 8.1.22]	R
5.6	X	9.3	***Rendering Complex Objects*** This subsection covers the ability of a recordkeeping system to deliver a complex record it maintains to a user in a manner that maintains the full functionality of that record.	SS
5.6.1	4.9.18	9.3.1	A Recordkeeping Application MUST render all of the components of a record and its metadata in a logical manner. [Indiana 1.10.4; MoReq 8.2.3; PRO A.3.21]	R
5.6.2	4.9.19	9.3.2	A Recordkeeping Application MUST be able to render records together with their associated metadata. [MoReq 8.1.15; PRO A.3.24; DoD c2.2.3.21; PERM 23]	R
5.6.3	4.9.20	9.3.3	A Recordkeeping Application MUST be able to render records on to appropriate output mediums which should at least include graphical display and printer output. [MoReq 8.2, 8.3, 8.4.1; Pro A.3.25-26, A.3.28-29; PERM 3, 10, 14, 16, 17, 24, non dod 2]	R
5.6.4	4.9.21	9.3.4	A Recordkeeping Application SHOULD be able to render records into an open export format. [PRO A.3.31]	R
5.6.5	4.9.22	9.3.5	A Recordkeeping Application SHOULD be able to render records independently of their creating environments. [MoReq 8.2.2; PRO A.3.22; DoD c3.2.14]	R

5.6.6	4.9.23	9.3.6	A Recordkeeping Application SHOULD be able to render a record simultaneously for multiple users. [PRO A.3.23, DoD c2.2.7.5]	R
5.6.7	4.9.24	9.3.7	A Recordkeeping Application SHOULD be able to render all versions of a record. [DoD c2.2.6.8.9]	R
5.7	X	9.4	***Rendering Recordness*** This subsection covers the ability of a recordkeeping system to deliver a record it maintains to a user in a manner that fully maintains the record's context, structure, and content.	SS
5.7.1	4.9.25	9.4.1	A Recordkeeping Application MUST render a record's content. [Pitt 11, 12; MoReq 8.2.3; PRO A.3.21; PERM 2]	R
5.7.2	4.9.26	9.4.2	A Recordkeeping Application MUST render a record's structure. [Pitt 12, 12b, 12b1; PRO A.3.21; PERM 2]	R
5.7.3	4.9.27	9.4.3	A Recordkeeping Application MUST render a record's context. [Pitt 12, 12b1, 12c; ISO 7.25; PERM 2]	R
5.7.4	4.9.28	9.4.4	A Recordkeeping Application MUST render a record's functionality. [Pitt 11b; DoD c2.2.5.3]	R
5.8	X	9.5	***Availability*** This subsection covers the availability of needed records in a recordkeeping system.	SS
5.8.1	4.9.29	9.5.1	A Recordkeeping Application MUST ensure that records needed for their primary business functions are available. [Indiana 1.10, 1.10.1; Pitt 12a; ISO 8.3.6]	R
5.8.2	4.9.30	9.5.2	A Recordkeeping Application SHOULD ensure that records needed for secondary use are available. [Indiana 1.10, 1.10.1; Pitt 12a]	R
5.8.3	4.9.31	9.5.3	A Recordkeeping Application MUST ensure that its records are available in a timely manner. [Indiana 1.10.1; Pitt 12a; ISO 8.3.6]	R
5.9	X	9.6	***Browsing*** This subsection covers the ability of a recordkeeping application to provide users the capability to browse records.	SS
5.9.1	4.9.32	9.6.1	The Recordkeeping Application SHOULD support the browsing of its classification schemes, including any hierarchical structure in which the records are managed. [MoReq 8.1.13, 8.1.27, 3.1.7; PRO A.3.3; DoD c2.2.1.6]	R
5.10	X	9.7	***Redaction*** This subsection covers the management and execution of redacting records and the delivery redacted versions of records to users.	SS
5.10.1	4.9.33	9.7.1	Procedures SHOULD provide for the redaction of restricted content from records delivered to users that do not have the right to see the restricted output. [Pitt 13; MoReq 9.3.10; PRO A.2.56]	R
5.10.2	4.9.34	9.7.2	A Recordkeeping Application SHOULD be able to create redacted versions of textual, audio, and moving image records. [MoReq 9.3.10]	R
5.10.3	4.9.35	9.7.3	A Recordkeeping Application MUST NOT, if it can redact records, alter the content of a record while creating a redacted version of that record. [Pitt 13a; PRO A.2.56]	R
6	4.10	10	**Design and Performance** This section covers the software and hardware design and performance of the recordkeeping application, including system maintenance, scalability, design constraints, and testing and verification. This section also covers the application's usability.	S
6.1	X	10.1	***Testing and Verification*** This subsection covers the testing and verification of the recordkeeping application's and the infrastructure's performance.	SS
6.1.1	4.10.1	10.1.1	An Institution SHOULD determine an appropriate suite of tests against which the recordkeeping infrastructure and recordkeeping application will be measured and set acceptable ranges for system performance. [Indiana 1.12;	R

			MoReq 11.2, 11.2.5]	
6.1.2	4.10.2	10.1.2	Procedures SHOULD include provisions for regular execution of application and infrastructure tests. [Indiana 1.12; PRO A.9.22]	R
6.1.3	4.10.3	10.1.3	Infrastructure SHOULD reliably pass all tests and perform within stated acceptable ranges. [Indiana 1.12; Moreq 11.2]	R
6.1.4	4.10.4	10.1.4	A Recordkeeping Application SHOULD reliably pass all tests and perform within stated acceptable ranges. [Indiana 1.13; PRO A.9.22; MoReq 11.2, 11.2.1-4]	R
6.1.5	4.10.5	10.1.5	A Recordkeeping Application SHOULD undergo formal verification and be provably correct. [Pitt 4b, 4c]	R
6.2	X	10.2	***System Maintenance*** This subsection covers the maintenance of the recordkeeping application and infrastructure.	SS
6.2.1	4.10.6	10.2.1	Procedures SHOULD contain provisions for all routine maintenance tasks which fall in line with industry best practices. [Pitt 2c; CTG System]	R
6.2.2	4.10.7	10.2.2	A Recordkeeping Application MUST allow convenient access to and the ability to modify any configuration parameters. [MoReq 11.2.7, 9.1.1]	R
6.2.3	4.10.8	10.2.3	Infrastructure SHOULD provide the ability to monitor available storage capacity. [MoReq 9.14; PRO A.9.21	R
6.2.4	4.10.9	10.2.4	An Institution SHOULD determine the acceptable ranges for downtime and minimum numbers of simultaneous users. [MoReq 11.3; DoD c3.1.3]	R
6.2.5	4.10.10	10.2.5	Infrastructure SHOULD be capable of fulfilling downtime and simultaneous user requirements laid out by the institution. [MoReq 11.3]	R
6.3	X	10.3	***User Interface*** This subsection covers the user interfaces of a recordkeeping application.	SS
6.3.1	4.10.11	10.3.1	A Recordkeeping Application SHOULD provide a user interface which is easy to use. [MoReq 11.1; PRO A.8.11; DoD c2.2.5.1]	R
6.3.2	4.10.12	10.3.2	A Recordkeeping Application SHOULD follow generally accepted user interface guidelines by providing a consistent look and feel. [PRO 8.1-3]	R
6.3.3	4.10.13	10.3.3	A Recordkeeping Application MAY provide a remote login facility. [MoReq A.9.7]	R
6.3.4	4.10.14	10.3.4	A Recordkeeping Application SHOULD facilitate use by persons with disabilities by including accessibility features. [PRO A.8.16]	R
6.3.5	4.10.15	10.3.5	A Recordkeeping Application SHOULD provide meaningful error messages in the event of an error, and attempt to guide the user to an appropriate resolution. [PRO A.8.7-8]	R
6.4	X	10.4	***Scalability*** This subsection covers scalability of the recordkeeping system..	SS
6.4.1	X	X	An Institution MUST create rules for formulating Submission Information Packages. [Tufts-Yale]	
6.4.2	X	X	An Institution MUST create rules for formulating Submission Information Packages. [Tufts-Yale]	
6.4.3	4.10.16	10.4.1	A Recordkeeping Application SHOULD be able to both scale up to large organizations, and scale down for smaller organizations. [MoReq 11.2.6, 11.2.8]	R
6.4.2	4.10.17	10.4.2	Institutions SHOULD estimate its medium and long-term scalability requirements and determine acceptable ranges for various scalability metrics. [PRO A.9.23]	R

6.4.3	4.10.18	10.4.3	A Recordkeeping Application SHOULD be capable of fulfilling its institution's scalability requirements, and of operating within acceptable ranges. [PRO A.9.23]	R
6.4.4	4.10.19	10.4.4	A Recordkeeping Application SHOULD NOT impose any practical limit on the number of records which can be managed by the application. [MoReq 6.3.5; PRO A.2.20]	R
6.4.5	4.10.20	10.4.5	A Recordkeeping Application SHOULD provide the ability to synchronize multiple instances of all underlying data stores. [DoD c2.2.3.24]	R
6.5	X	10.5	***Design Constraints*** This subsection covers the design constraints of the recordkeeping application.	SS
6.5.1	4.10.21	10.5.1	A Recordkeeping Application SHOULD be designed around a flexible architecture which can evolve as the institution's needs change. [PRO A.9.1]	R
6.5.2	4.10.22	10.5.2	A Recordkeeping Application MAY support a distributed repository with multi-site service. [PRO A.9.18]	R
6.5.3	4.10.23	10.5.3	A Recordkeeping Application SHOULD provide at least one version of backward compatibility. [DoD c2.1.4]	R
6.4.6	4.10.24	10.5.4	A Recordkeeping Application SHOULD, when it offers remote or distributed services, use efficient network protocols which minimize the amount of data exchange required. [PRO A.9.20]	R

APPENDIX B: PRESERVATION REQUIREMENTS CROSSWALK

The table below presents the preservation requirements from Section V along with their corresponding place in the August 2005 draft for public comment version of the requirements. The full text of each requirement, along with its appropriate sources, is listed in the "Requirement" column. The "Level" column describes if the corresponding row describes a section of the requirements (denoted by an "S"), a subsection (denoted by an "SS"), or an actual requirement (denoted by an "R").

Final Requirements Number	Aug 2005 Requirements Number	Requirement	Level
1	x	**Common Services**	S
1.1	x	**Operating system services**	SS
1.1.1	x	The Application SHOULD function on well-supported operating systems and other core infrastructural software. [CTDR D1.1]	R
1.1.2	x	The Infrastructure SHOULD provide tools to support system level testing. [NARA 26.1]	R
1.1.3	x	The Application SHOULD generate notices to users. [NARA 23.6]	R
1.1.4	x	The Application SHOULD support logging of all system events. [NARA 24.1]	R
1.1.5	x	The Application SHOULD comply with relevant de facto and de jure operating systems standards. [MoReq 11.4]	R
1.1.6	x	The Institution SHOULD have a process to stay current with the latest operating system security fixes. [CTDR D1.10]	R
1.2	x	**Network Services**	SS
1.2.1	x	The Infrastructure SHOULD provide for networked access to records.[NARA 19]	R
1.2.2	x	The networking Infrastructure SHOULD be appropriate to the access services provided and the designated community.[CTDR D2.1]	R
1.2.3	x	If data storage is outsourced or administered externally, there MUST be sufficient network Infrastructure to support this service. [MoReq 11.6]	R
1.2.4	x	A network Application MUST be able to provide metadata necessary for preservation. [MoReq 12.1.22]	R
1.2.5	X	The networking Infrastructure MUST support the security requirements of the instution. [ERA13.6]	
1.2.6	X	The networking Infrastructure SHOULD meet or exceed specified performance reliability requirements [ERA 31.1–31.4]	
1.3	x	**Security Services**	SS
1.3.1	6.1.3	An Application MUST enable the use of user security profiles. [MoReq 9.1.8; PRO A.5.11, A.5.17-18, A.5.20-22]	R
1.3.2	6.1.2	An Application MUST enable the use of record security profiles. [Indiana 1.2.8; DoD c2.2.3.18–c2.2.3.20; NARA 15.2.1]	R
1.3.3	x	Procedures MUST provide a reasonable guarantee that records are protected from tampering. [Pitt 9a; PRO A.2.15; ISO 7.1.1, 8.2.2.c; HIPAA 45CFR164.306; NARA 13–14]	R
1.3.4	x	Procedures MUST prescribe periodic software security updates. [HIPAA 45CFR164.308]	R
1.3.5	X	An Application MUST confer exclusive capabilities upon authorized people to exercise the responsibility for creation, modification, annotation, relocation, and destruction of records as defined by an institution. [Indiana 1.4.1; DoD c2.2.5.2, c2.2.7.4; ISO 8.3.6; HIPAA 45CFR164.308; InterPARES A.2]	R

1.3.6	x	An Application SHOULD manage the security level of the records it maintains. [MoReq 9.3.3, 9.3.5]	R
1.3.7	x	Infrastructure SHOULD provide services for secure authentication. [PRO A.5, A.5.1, A.5.11; DoD c2.2.7.1; HIPAA 45CFR164.312]	R
1.3.8	x	An Application MUST authenticate users before providing services. [PRO A.5, A.5.1, A.5.11; DoD c2.2.7.1; HIPAA 45CFR164.312; Yale A.4]	R
1.3.9	x	An Application MUST NOT allow unauthorized changes to the records it maintains. [Indiana 1.7.1; MoReq 3.2.1, 4.5.4, 6.1.4; PRO A.2.41; DoD c2.2.5.4; ISO 9.7.d; Yale A.4, A.7; NARA 13]	R
1.3.10	x	An Institution SHOULD undertake a periodic system security analysis of its data systems and identify security risks and needs. [CTDR D3.1]	R
1.3.11	x	An Institution SHOULD implement mechanisms to address each of the defined security needs. [CTDR D3.2]	R
1.3.12	x	Natural People MUST have delineated roles, responsibilities, and authorizations. [CTDR D3.3]	R
2	1	**Ingest**	S
2.1	x	**Receive Submission**	SS
2.1.9	x	An Institution SHOULD provide the Producer with progress reports at specific predetermined points throughout the Ingest process. [CTDR B1.7]	R
2.1.10	x	An Institution SHOULD mark the formal acceptance of preservation responsibility. [CTDR B1.9]	R
2.2	x	**Quality Assurance**	SS
2.2.5	X	An Institution SHOULD confirm that the determinations of the feasibility of preservation made during the process of appraisal are still valid. [Tufts-Yale]	R
2.3	x	**Generate AIP**	SS
2.3.3	x	An Institution MUST define how AIPs are derived from SIPs. [CTDR B2.1–B2.3	R
2.3.4	x	An Application SHOULD facilitate the transformation of record components according to the format transformation plan. [Tufts-Yale]	R
2.4	x	**Generate Descriptive Information**	SS
2.4.1	x	An Institution MUST identify the properties of the records it will preserve. [CTDR B1.1]	R
2.4.8	x	An Institution SHOULD generate or acquire preservation metadata.[CTDR B3.6]	R
2.5	x	**Coordinate Updates**	SS
2.5.1	x	An Application MUST facilitate the transfer of records from Ingest into the record components store. [Tufts-Yale]	R
2.5.2	x	An Institution SHOULD deposit AIPs into its preservation system according to its preservation system rules. [Tufts-Yale]	R
2.5.3	X	An Institution MUST update information on preservation actions applied to acquired records. Tufts-Yale]	R
X	1.2.	***Manage transfers***	SS
X	1.2.1.	*Accessioning*	SSS
2.4.5	1.2.1.1.	An Institution MUST register transfers with a unique identifier. [Yale A.5–A.6]	R
X	1.2.2.	*Capture Information about Records*	SSS
2.4.2	1.2.2.1.	An Application SHOULD be capable of automatically extracting metadata for the records it captures from a recordkeeping application (including representation information). [Indiana 1.6.1; MoReq 6.1.6, 6.1.14; Yale B.5; NARA 3.3–3.5; CTDR 3.3, B3.4, B4.1]	R

2.4.3	1.2.2.2.	An Application MUST allow people to manually enter metadata that cannot be automatically extracted from the records captured from a recordkeeping application. [Indiana 1.6.3; MoReq 6.1.9; PRO A.2.38, PERM 12; NARA 3.3.1.2; CTDR B4.1]	R
2.4.4	1.2.2.3.	Procedures MUST provide for the creation of necessary metadata during the capture process that did not exist before capture (including descriptive, technical, and contextual metadata necessary to document ingest). [MoReq 6.1.9; PRO A.2.38, PERM 12, Indiana 1.2.3; Pitt 8a; MoReq 6.1.2, 6.1.3; ISO 7.2.1.b; NARA 3.3; CTDR B4.1]	R
4.1.1	1.2.2.4.	An Application MUST maintain any links established between ingested records and their metadata (and demonstrate referential integrity). [Indiana 1.2.3; MoReq 6.1.3; ISO 7.1.c; CTDR B4.2]	R
X	1.3.	***Accept all types of electronic records***	SS
5.5.11	1.3.1.	An Institution MAY accept all format types in which electronic records are written.	R
2.1.2	1.3.2.	An Application MUST be able to ingest data files in the digital formats in which they were received, as specified by submission agreements. [NARA 6.1–7.2]	R
2.1.3	1.3.3.	An Application SHOULD accept transfers via physical media. [NARA 16.1]	R
2.1.4	1.3.4.	An Application SHOULD accept transfers electronically. [NARA 16.2]	R
2.1.5	1.3.5.	An Application SHOULD accept electronic records that are composed of more than one digital component. [NARA 15.2]	R
2.1.6	1.3.6.	An Application SHOULD be capable of interacting with all of the institution's recordkeeping applications. [Indiana 1.6.2; MoReq 6.2.1; PRO A.2.2; NARA 1.10]	R
X	1.4.	***Check electronic records contained in a transfer***	SS
2.1.1	1.4.1.	An Institution MUST confirm that the transfer is authorized. [NARA 1.2.1; CTDR B1.4]	R
5.6.1	1.4.2.	An Application SHOULD be able to confirm that a transfer is authorized by a submission agreement. [NARA 1.2; CTDR B1.4]	R
5.6.2	1.4.3.	Procedures MUST be able to validate that a records transfer complies with the submission agreement (terms and conditions of transfer). [NARA 1.2.1–1.2.1.2; CTDR B1.6]	R
2.2.1	1.4.4.	An Application MUST confirm the success of a file transfer (verification). [NARA 16.3; CTDR B1.6]	R
2.2.2	1.4.5.	An Application SHOULD be able to technically validate that records components conform to technical file format standards. [Yale B.4; NARA 5.8]	R
5.6.3	1.4.6.	An Institution SHOULD provide feedback to the producer on the success or failure of the transfer. [Yale B.4; CTDR B1.7]	R
2.4.6	1.4.7.	An Application MUST be able to technically validate the metadata it creates or captures. [Indiana 1.6.4; MoReq 6.1.1]	R
2.2.3	1.4.8.	Procedures SHOULD provide for the intellectual validation of the metadata the records preservation system creates or captures during ingest. [Indiana 1.6.4; MoReq 6.1.1]	R
3	2	**Archival Storage**	S
3.1	x	**Receive Data**	SS
3.1.1	x	An Application MUST generate storage identifiers and document them in the appropriate AIPs.[Tufts-Yale]	R
3.1.2	x	An Institution SHOULD gauge anticipated frequency of utilization of AIPs in order to select the most appropriate storage devices or media. [Tufts-Yale]	R
		An Application MAY be capable of adding an "object accession" event to the PDI history. [Tufts-Yale]	R
3.2	x	**Manage Storage Hierarchy**	
3.3	x	**Replace Media**	SS

3.3.3	x	Before replacing media, the Instituion SHOULD test new media for manufacturing defects.[Tufts-Yale]	SS
3.3.4	x	An Application MAY automatically update PDI for all records affected by a media replacement with a “media refresh” event. [Tufts-Yale]	R
3.4	x	**Error Checking**	SS
3.5	x	**Disaster Recovery**	SS
3.5.7	x	Juridical People SHOULD have clearly defined responsibilities to maintain service continuity and recovery from disasters.[CTDR D3.6]	R
3.6	x	**Provide Data**	SS
3.6.2	X	An Institution MUST To gather the information required, from descriptive instruments and other preservation information, to satisfy requests for records and/or information about records. [Tufts-Yale]	R
3.6.3	x	An Application MAY automatically update retrieval statistics when providing data. [Tufts-Yale]	R
X	2.1.	***Store records reliably*** (including Protection from Loss or Corruption)	SS
X	2.1.1	***Intrusion Detection and Response***	SSS
1.3.3	2.1.1.1	Procedures MUST provide a reasonable guarantee that records are protected from tampering. [Pitt 9a; PRO A.2.15; ISO 7.1.1, 8.2.2.c; HIPAA 45CFR164.306; NARA 13–14]	R
1.3.3	2.1.1.2	Procedures MUST prescribe periodic software security updates. [HIPAA 45CFR164.308]	R
X	2.1.2	*Disaster Preparation* Disaster preparation is listed more than once in these requirements, both here as part of the Archival Storage activitiy and later (See 4.1.1) as part of the Administration activity. This section refers to requirements necessary to ensure that records components are stored reliably. Later Disaster Prepartion is described in terms of the development and maintenance of policies and procedures regarding disaster preparation.	SSS
3.5.1	2.1.2.1	An Application MUST NOT hinder automated backup of the institution’s records.	R
3.5.2	2.1.2.2	Infrastructure SHOULD allow for backups to be stored at geographically distant locations. [PRO A.9.12; DoD c2.2.9.2; Yale C.2; NARA 10.1.4]	R
3.5.3	2.1.2.3	An Application MUST provide facilities for restoring data from backup data and returning the data stores to a state prior to disaster. [Pitt 4d; MoReq 11.3.5, 4.3.3, 4.3.4; PRO A.9.14-16; DoD c2.2.9.3, c2.2.2.9.3.1-2, c2.2.9.4-5; HIPAA 45CFR164.308; NARA 10.2.3]	R
X	2.1.3	***Manage the Preservation Process***	SSS
X	2.1.3.1	***Media Decay*** (manage media)	SSSS
3.4.1	2.1.3.1.1	Procedures SHOULD allow for periodic checks for media deterioration or loss. [MoReq 11.7.2, 9.1.5; NARA 12.6–12; CTDR D1.5]	R
5.2.1	2.1.3.1.2	An Institution SHOULD develop a physical storage media tracking system. [NARA 11.1]	R
3.2.1	2.1.3.1.3	Procedures MUST allow for storage media to be maintained in an appropriate physical environment. [MoReq 11.7.1; ISO 8.3.3; NARA 12.6]	R
3.3.2	2.1.3.1.4	Procedures MUST allow for the migration of records from one storage media to another in a manner that preserves the recordness of the records. [Indiana 1.9.1; MoReq 4.4; NARA 12.1, 28.2.4, 28.2.5; CTDR D1.7]	R
3.1.3	2.1.3.1.5	An Application MUST NOT modify electronic records to accommodate physical storage media. [NARA 12.2]	R
3.3.1	2.1.3.1.6	An Application MAY provide the automated capability to move electronic records to different media to accommodate new technology. [NARA 12.1]	R
3.5.4	2.1.3.1.7	An Institution SHOULD possess tools for recovery of electronic records from failed media. [NARA 12.4]	R

X	2.1.3.2	***Hardware and Software Obsolescence***	SSSS
X	2.1.3.2.1	An Application MUST have the capability to store copies of electronic records [NARA 10.1]	R
X	2.1.3.3	***Transformation***	SSSS
5.3.1	2.1.3.3.1	An Institution MUST ensure that transformations are synchronized across multiple copies of records, where appropriate (when content information may be conceived as identical). [CTDR D1.4]	R
5.3.2	2.1.3.3.2	An Application SHOULD provide the capability to transform any ingested data file to a different, more persistent format. [NARA 8.5-8.6]	R
5.3.3	2.1.3.3.3	An Application MUST persistently link the format versions of the same records together. [PRO A.2.12; NARA 19.8.9]	R
X	2.1.3.3.4	Upon any transformation, an Application SHOULD NOT involve an irreversible conversion from one data format to another. [Yale A.9; NARA 8]	R
5.3.4	2.1.3.3.5	An Application SHOULD automate the synchronization of transformations across multiple copies of records where appropriate. [CTDR D1.4]	R
X	2.1.4	***Destruction of Records***	SSS
4.4.4	2.1.4.1	An Application MUST provide the capability to destroy the components of any electronic record [NARA 1.5]	R
X	2.1.5	***Monitor Integrity***	SSS
2.2.4	2.1.5.1	An Institution MUST actively monitor the integrity of AIPs [CTDRB3.7]	
5.2.15	2.1.5.1	An Institution MUST actively monitor the integrity of AIPs [CTDRB3.7]	R
X	2.1.5.2	An Application SHOULD be able to check records components using stored signatures or checksums	R
X	2.1.5.3	An Application MUST be able to discover records components which are not enclosed in an AIP (eg, after data loss)	R
X	2.2	***Hardware Replacement and Maintenance***	SS
5.2.2	2.2.1	An Application MUST support migration to new Preservation Application Hardware Environments	R
3.2.2	2.2.2	An Application SHOULD support high-reliability and redundancy features such as clustering and hot spares	R
3.2.3	2.2.3	Infrastructure MUST be able to support migration to new Storage Hardware Environments	R
X	2.3	***Basic Functions***	SS
2.3.2	2.3.1	An Application MUST be able to store records components and bind records components together with an AIP	R
3.6.1	2.3.2	An Application MUST be able to retrieve all the records components of a record	R
4.1.2	2.3.3	An Application MUST be able to maintain a record's Preservation Description Information, which documents all events which affect the record	R
5.5.1	2.3.4	An Institution MUST ensure that all actions taken which affect records cause a Preservation Description Information event to be generated	R
4	3	**Data Management**	S
4.1	x	**Administer Database**	SS
4.2	x	**Perform Queries**	SS
4.2.1	x	An Application MUST ensure all of its records metadata are discoverable. [Indiana 1.10.2-3; MoReq 8.1.4-5, 8.1.7; PRO A.3.4, A.3.6, A.3.8, A.3.17; PERM 18; NARA 19]	R

4.2.2	x	An Application MAY provide integration with external discovery services. [Tufts-Yale]	R
4.3	x	**Generate Report**	SS
4.4	x	**Receive Database Updates**	SS
4.4.1	x	An Application MUST enable the addition of new metadata bistreams or the versioning of an existing bitstream as appropriate. [Tufts-Yale]	R
4.4.2	x	An Application MUST update an AIP with any new storage identifiers and fixity information. [Tufts-Yale]	R
4.4.3	x	An Application MAY automatically update PDI for all affected records with “Metadata Update Event”. [Tufts-Yale]	R
X	3.1	***Information About Records***	SS
X	3.1.1	***Representation Information***	SSS
4.1.3	3.1.1.1	An Institution MUST maintain representation information for all records types stored. [CTDR B3.4]	R
X	3.1.2	***Unique Identifier***	SSS
2.3.5	3.1.2.1	An Application MUST uniquely identify the records it maintains. [Pitt 6c; MoReq 7.1; PRO A.9.3; DoD c2.2.1.4, c2.2.4.1; PERM 15; Yale A.5; NARA 1.1.2.1, 19.1.14; CTDR B2.5]	R
X	3.1.3	***Copies of Records (Versions)***	SSS
4.1.4	3.1.3.1	An Application MUST manage the relationship between the copies of records components in the system. [Indiana 1.2.8; DoD c2.2.3.18–c2.2.3.20; NARA 15.2.1]	R
4.1.5	3.1.3.2	An Application MUST manage the relationship between all copies of records components to their corresponding records. [NARA 7.4]	R
4.1.6	3.1.3.3	An Application MAY support identification of the authoritative version (master copy or preservation copy) of a record component in the system. [InterPARES A.7; NARA 18.5.1]	R
4.1.7	3.1.3.4	An Application MUST document any changes of a record component from the point of ingest. [InterPARES B.3; NARA 8.1.5]	R
4.1.8	3.1.3.5	An Application MUST document items removed from the preservation system, including filenames, timestamps and a person identifier. [Yale D.3; NARA 15.8.1]	R
X	3.1.4	***Location Tracking***	SSS
4.1.9	3.1.4.1	An Application MUST be able to track the location of its records copies. [MoReq 4.4.1; NARA 10.2.4, 10.2.6; CTDR B2.4–B2.5, D1.3]	R
4.1.10	3.1.4.2	An Application MUST track a record’s unique identifier, current location, time of movements, and the person responsible for the movements. [MoReq 4.4.3; ISO 9.8.3; NARA 10.2.6; CTDR B2.4–B2.5]	R
X	3.1.5	***Demonstration of Controls over Records Transfer, Maintenance, and Reproduction.*** This refers to auditable documentation proving the existence of such controls. This does not include requirements for transfer, maintenance, and reproduction of the records themselves.	SSS
5.5.2	3.1.5.1	An Institution SHOULD demonstrate it has created and maintains a reasonable access criteria and it has successfully implemented the criteria. [InterPARES B.1; ISO 8.3.6; NARA 13.2–13.4; CTDR B3.8]	R
5.2.3	3.1.5.2	An Application SHOULD facilitate the creation, maintenance, and distribution of documentation to support a demonstration of controls over records transfer, maintenance, and reproduction. [InterPARES B.1; NARA 6; CTDR B3.8]	R
5	4	**Administration**	S
5.1	1.1.	***Negotiate Submission Agreement***	SS
5.1.1	1.1.1.		R

5.1.3	1.2.1.2.	An Institution MUST provide for transfer of legal custody of records to the archives. [NARA 1.3]	R
5.1.2	1.2.1.3.	An Application MAY automate the implementation of submission agreements. [NARA 1.6–7]	R
5.2	x	**Manage System Configuration**	SS
5.3	x	**Archival Information Update**	SS
5.4	x	**Physical Access Control**	SS
5.4.1	x	An Institution SHOULD create and maintain policies and procedures to detect, contain, and correct security violations. [HIPAA 45CFR164.308, 45CFR164.310, 45CFR164.312]	R
5.4.2	x	Procedures MUST provide a reasonable guarantee that records are protected from tampering. [Pitt 9a; PRO A.2.15; ISO 7.1.1, 8.2.2.c; HIPAA 45CFR164.306]	R
5.4.3	x	An Institution MUST implement procedures to protect the Archive's facilities and equipment from unauthorized access, tampering, or theft. Such facilities include the physical surroundings of all storage devices and media. [HIPAA 45CFR164.310]	R
5.4.4	x	Natural People MUST be authorized to access the Archives' facilities. [HIPAA 45CFR164.308]	R
5.4.5	x	An Institution SHOULD implement physical safeguards for all workstations that access electronic records, to restrict access to authorized users. [HIPAA 45CFR164.310]	R
5.4.6	x	An Instituion MUST NOT dispose of records storage media or make it available for re-use without assuring electronic records are removed. [HIPAA 45CFR164.310]	R
5.5	4.1	**Establish and Maintain Standards and Policies**	SS
5.5.3	6.2.6	Procedures SHOULD exist to redact restricted content from records. [Pitt 13, MoReq 9.3.10; PRO A.2.56; NARA 20.11.2]	R
5.5.15	6.2.6	An Institution SHOULD establish policies regarding rendering the functionality of record types. [Pitt 11b, DoD c2.2.5.3; NARA 8.1.6.5, 20.11.3]	R
5.5.16	6.2.3	An Institution SHOULD establish policies defining the necessary elements of a response to a Consumer request (what is an appropriate response). [CTDR B5.3]	R
5.5.17	6.2.1	An Institution SHOULD establish policies defining the description necessary to ensure records are discoverable. [Indiana 1.10.2-3; MoReq 8.1.4-5, 8.1.7; PRO A.3.4, A.3.6, A.3.8, A.3.17; PERM 18; NARA 19]	R
5.5.18	5.3	Procedures SHOULD exist for managing record types with templates. [NARA 7.2]	R
5.5.19	4.4.5	Procedures SHOULD exist for monitoring the available storage. [Tufts-Yale]	R
5.5.20	x	An Institution SHOULD establish format transformation policies and plans to implant them. [Tufts-Yale]	R
X	4.2	**Protection from Loss or Corruption**	SS
5.6	x	**Audit Submission**	SS
X	4.2.1	**Disaster Preparation**	SSS
5.5.4	4.2.1.1	An Institution SHOULD create backup and failure mode procedures for its records and metadata associated with those records. [Indiana 1.9, 1.9.4; Pitt 2d; MoReq 4.3.7; InterPARES A.3; ISO 8.3.3; NARA 10.2.3, 14.9; CTDR D1.2, D3.4]	R
3.2.4	4.2.1.2	An Institution SHOULD test and review backup and failure mode procedures. [HIPAA 45CFR164.308, 45CFR164.310; NARA 27.1; CTDR D1.2, D3.5]	R
3.5.5	4.2.1.3	Procedures SHOULD provide for the automated backup of the preserved records and preservation metadata. [MoReq 4.3, 4.3.1, 9.1.2-3; PRO A.9.11, A.9.17; Dod c2.2.9.1]	R
3.5.6	4.2.1.4	Procedures SHOULD articulate the actions needed to be undertaken during primary system failure. [Pitt 2d; MoReq 4.3.5; HIPAA 45CFR164.308]	R

x	4.2.2	***Access Control***	SSS
5.5.5	4.2.2.1	An Institution MUST explicitly assign responsibility for the annotation, relocation, and destruction of records on the basis of a person’s authority and capacity to carry out the activity (establishing user security profiles). [Indiana 1.7.2, IP A.2, MoReq 4.6.5, 9.3.5; PRO A.5.36; ISO 9.7; PERM 25; HIPAA 45CFR 164.308, 45CFR164.312; Yale A.5; NARA 13]	R
1.3.3	4.2.2.2	An Application MUST confer exclusive capabilities upon people to exercise the responsibility for annotation, relocation, and destruction of records as defined by an institution. [Indiana 1.4.1; DoD c2.2.5.2, c2.2.7.4; ISO 8.3.6; HIPAA 45CFR164.308; IP A.2; NARA 13]	R
1.3.4	4.2.2.3	Procedures MUST prescribe periodic software security updates. [HIPAA 45CFR164.308]	R
5.5.6	4.2.2.3		R
4.1.11	4.2.2.3		R
4.3.1	4.2.2.4	An Application MUST NOT allow unauthorized changes to the records it maintains. [Indiana 1.7.1; MoReq 3.2.1, 4.5.4, 6.1.4; PRO A.2.41; DoD c2.2.5.4; ISO 9.7.d; Yale A.4, A.7; NARA 13]	R
5.5.7	4.2.2.4		R
1.3.8	4.2.2.4		R
5.6.4	4.2.2.5	An Institution SHOULD create and maintain policies and procedures to detect, contain, and correct security violations. [HIPAA 45CFR164.308, 45CFR164.310, 45CFR164.312; NARA 13]	R
5.5.8	4.2.2.6	An Institution SHOULD perform a periodic review of its security procedures (including reanalysis of security threats or access management system failure). [InterPARES B.1.b; HIPAA 45CFR164.308; CTDR B5.2]	R
5.2.4	4.2.2.6		R
x	4.2.2.7	Procedures SHOULD allow for the periodic review of access control rules, records security profiles, and user security profiles. [MoReq 4.6.12; PRO A.5.40; ISO 9.7; HIPAA 45CFR164.308]	R
x	4.2.2.8	Procedures SHOULD allow for the modification of access control rules, records security profiles, and user security profiles based on the findings of a review. [HIPAA 45CFR164.308; NARA 8.9]	R
x	4.3	***Reporting Capability and Event Log***	SS
5.2.5	4.3.1	An Application MUST be able to identify system failures [NARA 27.2.1; CTDR B5.2]	R
x	4.3.2	An Application SHOULD be able to produce reports for administrators to document any system activity, including failure. [MoReq 3.4.14, NARA 26.1, 26.3.1, 27.2.4; CTDR B5.2]	R
4.3.3	4.3.3	An Application MUST provide the capability to produce documentation of any reproduction or copy process and its effects, including the dates of the records’ reproduction and the name of the responsible person and the impact of the reproduction process on the form of the records components (any changes the records components have undergone). [IP B.2]	R
5.2.6	4.3.4	An Application MAY provide the facility to isolate and resolve failures, provided any activity is documented and any changes to affected records components checked and documented. [NARA 27.2.2–27.2.3]	R
x	4.4	***System Administration***	SS
x	4.4.1	An Application MUST function on well-supported operating systems and other core infrastructure software. [CTDR D1.1]	R
5.2.7	4.4.2	Procedures SHOULD contain provisions for all routine maintenance tasks which fall in line with industry best practices. [Pitt 2c; CTG System; NARA 27; CTDR D1.10]	R
5.2.16	4.4.3	An Application MUST support a stasis mode where no changes are allowed. [Tufts-Yale]	R
2.5.2	4.4.3	An Application MUST support a stasis mode where no changes to records are allowed.	R

5.2.8	4.4.4	An Application MUST allow convenient access to and the ability to modify any configuration parameters. [MoReq 11.2.7, 9.1.1; NARA 27.4]	R
5.2.14	4.4.5	Infrastructure SHOULD provide the ability to monitor available storage capacity. [MoReq 9.14; PRO A.9.21; NARA 27.3.4]	R
5.2.14	4.4.6	An Institution SHOULD determine the maximum number of simultaneous users necessary. [MoReq 11.3; DoD c3.1.3]	R
5.2.9	4.4.7	An Institution SHOULD identify the necessary hours of Application availability. [MoReq 11.3; DoD c3.1.3]	R
5.2.10	4.4.8	Infrastructure SHOULD be capable of fulfilling downtime and simultaneous user requirements laid out by the institution. [MoReq 11.3]	R
5.2.11	4.4.9	An Application MAY provide the capability to monitor overall system state in a consolidated manner. [NARA 27.3]	R
6	5	**Preservation Planning**	S
6.1	x	**Monitor Designated Community**	SS
6.1.3	x	An Institution MUST periodically monitor the acceptability of chosen preservation strategies to existing Consumers and Producers. [Tufts-Yale]	R
6.2	x	**Monitor Technology**	SS
x	5.1	**Preservation Planning framework**	SS
6.3	5.1.1	**Develop Preservation Strategies & Standards**	SSS
6.3.1	x	Juridical People MUST synthesize information about designated communities, technologies, system performance, inventory, and finances in order to recommend preservation strategies and standards. [Tufts-Yale]	
6.3.2	5.1.1.1	An Institution MUST establish plans for preserving records as long as needed and have a written mission statement that reflects a commitment to long-term preservation. [Indiana 1.9; MoReq 11.7.4; PERM non dod 4; NARA 8.9; CTDR 3.1]	R
6.3.3	5.1.1.2	An Institution SHOULD establish strategies for ensuring the accessibility and functionality of records components over time. [InterPARES A.4; ISO 8.3.5, 9.6]	R
6.3.4	5.1.1.3	An Institution SHOULD establish preservation action plans specifying preservation actions to be taken in ensuring the accessibility and functionality of templates of records components over time. [InterPARES A.4; ISO 8.3.5, 9.6; NARA 8.9]	R
6.3.5	5.1.1.4	An Institution SHOULD establish plans for managing preservation metadata and attaching it to records. [MoReq 5.3.10, 11.7.7; PERM 5, 6]	R
5.5.9	5.1.1.5	An Application MAY provide the capability for users to create and maintain preservation and access plans (including the ability to alter plans) [NARA 8.9.1–8.9.6; CTDR B3.10]	R
5.5.10	5.1.1.6	An Application MAY provide the capability for users to associate a preservation and access plan with electronic records [NARA 8.9.5]	R
6.3.6	6.2.6	An Institution SHOULD develop strategies for redaction of restricted content from users. [Pitt 13, MoReq 9.3.10; PRO A.2.56; NARA 20.11.2]	
6.3.7	6.2.5	An Institution SHOULD develop strategies for rendering the functionality of types of records. [Pitt 11b, DoD c2.2.5.3; NARA 8.1.6.5, 20.11.3]	
6.3.8	5.3	An Institution SHOULD develop templates to manage record types. [NARA 7.2]	
x	5.2	**Monitor preservation strategies standards and best practices**	SS
6.2.1	5.2.1	Juridical People SHOULD monitor the state of the art of information technology in order to facilitate preservation planning.	R
5.2.13	5.2.2	5.2.13. An Institution MUST actively monitor the integrity of AIPs. [CTDRB3.7]	

2.4.7	5.2.2	An Institution SHOULD use representation information from appropriate international registries.[CTDR B3.3]	R
x	5.3	***Manage record types.*** This subsection describes the management of sets of specifications about records. Every set of record stored in the system should conform to a type registered for that type of set of records, either at the time it is ingested into the system or through a subsequent transformation.	SS
6.4.1	5.3.1	An Institution SHOULD define records templates to automate preservation planning and processing. [NARA 7]	R
6.1.1	5.3.2		
6.2.2	5.3.2	An Application SHOULD enable monitoring and notification when preservation strategies are no longer viable. [CTDR B3.9]	R
6.2.3	5.3.3	An Institution MUST periodically monitor the viability of chosen preservation strategies. [CTDR B3.9]	R
4.1.12	5.3.4	An Application MAY provide for management of templates within a template repository. [NARA 7.2]	R
4.1.13	5.3.5	An Application MAY provide the capability to associate templates with sets of records. [NARA 7.7.1–7.7.2]	R
7	6	**Access**	S
7.1	x	**Coordinate Access Activities**	
x	6.1	***Use Rights*** This subsection covers the institution's management of users' rights to view and/or receive records. This includes the development, management, and review of records and user security profiles. It also includes the management of access controls and authentication of users.	SS
x	6.1.1	***Access Controls*** This subsection covers the management of processes that control the access of records in a preservation system.	SSS
7.1.1	6.1.1.1	Procedures MUST ensure that only authorized users gain access to records. [MoReq 4.1.1; PRO A.5.25, A.5.42, A.5.46-50; NARA 13]	R
x	6.1.2	***Record Security Profile***	SSS
2.1.7	6.1.2.1		
4.1.14	6.1.2.1	An Application MUST allow records security profiles to be created and modified. [MoReq 9.3.5; PRO A.5.36; NARA 8.9.5, 16.6.2]	R
2.1.8	6.1.2.2		
4.1.15	6.1.2.2	An Application MUST allow record security profiles to be assigned to records. [MoReq 4.6.1; PRO A.2.26, A.5.5, A.5.26, A.5.27; ISO 9.7.2; NARA 8.9.5]	R
4.1.16	6.1.2.3	An Application SHOULD allow time sensitive records profiles that are valid for a limited time period to be assigned to records and should automatically be switched to another records security profile when their valid time period expires. [PRO A.5.38-39; NARA 13.13.2]	R
x	6.1.3	***User Security Profile***	SSS
4.1.17	6.1.3.1	An Application MUST allow user security profiles to be created and modified. [MoReq 9.1.8; PRO A.5.11, A.5.17-18, A.5.20-22]	R
4.1.18	X	An Application MUST allow user security profiles to be linked to natural people. [MoReq 4.1.2, 4.1.5, 4.6.7, 9.1.7; PRO A.5.5, A.5.10, A.5.13, A.5.16, A.5.24; DoD c2.2.7.3]	
4.1.19	X	A Juridical Person SHOULD review records before a time-sensative change is made in the records security profile. [Tufts-Yale]	
7.1.2	6.1.3.2	An Application MUST assign or reassign user security profiles to people. [MoReq 4.1.2, 4.1.5, 4.6.7, 9.1.7; PRO A.5.5, A.5.10, A.5.13, A.5.16, A.5.24; DoD c2.2.7.3]	R
x	6.1.4	***Authentication of Users***	SSS

1.3.7	6.1.4.1	Infrastructure SHOULD provide services for secure authentication. [PRO A.5, A.5.1, A.5.11; DoD c2.2.7.1; HIPAA 45CFR164.312]	R
1.3.8	6.1.4.2	An Application MUST authenticate users before providing services. [PRO A.5, A.5.1, A.5.11; DoD c2.2.7.1; HIPAA 45CFR164.312; Yale A.4]	R
x	6.1.5	***Access Review***	SSS
x	6.2	***Discovery and Delivery***	SS
x	6.2.1	***Searching***	SSS
7.1.3	6.2.1.1	An Application MUST ensure all of its records and metadata are discoverable. [Indiana 1.10.2-3; MoReq 8.1.4-5, 8.1.7; PRO A.3.4, A.3.6, A.3.8, A.3.17; PERM 18; NARA 19]	R
7.1.4	6.2.1.2	An Application MUST be able to render all records returned in a search results list. [MoReq 8.2.1; PRO A.3.20; DoD c2.2.6.8.10; NARA 19.8]	R
7.1.5	6.2.1.3	An Application MUST support searching by records' identifiers. [MoReq 8.1.16, 8.1.23; NARA 19.1.14]	R
7.1.6	6.2.1.4	An Application SHOULD provide an integrated search interface. [MoReq 8.1.2; PRO A.3.7; NARA 19.1, 21]	R
7.3.1	6.2.1.5	An Application MUST, if it has an integrated search interface, present search results. [PRO A.3.15; DoD c2.2.6.8.5; NARA 19.8]	R
7.1.7	6.2.1.6	An Application MAY support resource discovery through external interfaces/mechanisms in addition to any integrated search interface. [PRO A.3.19]	R
7.1.8	6.2.1.7	An Application SHOULD limit search results to the records the user has rights to access. [MoReq 4.1.10, 4.1.12, 8.1.28; PRO A.3.18, A.5.51-52, B.3.18; NARA 19.8.3]	R
7.3.2	6.2.1.8	An Application MAY provide capabilities to manage a search results list including, but not limited to, order, number of hits per page, filter results files, and saving search results. [MoReq 8.1.17; 8.1.24-25; DoD c2.2.6.8.5; NARA 19.8.4–19.12.3]	R
x	6.2.2	***Query Techniques***	SSS
7.1.9	6.2.2.1	An Application SHOULD support the full text search of the records and metadata it maintains. [MoReq 8.1.8; DoD c3.2.9; NARA 19.1.5–19.1.19	R
7.1.10	6.2.2.2	An Application SHOULD support searching metadata fields containing controlled vocabulary terms managed by thesauri. [MoReq 8.1.10; PRO A.3.5; DoD c3.2.9; NARA 19.1.3]	R
7.1.11	6.2.2.3	An Application SHOULD support searching multiple metadata fields and/or full text of records. [MoReq 8.1.6; PRO A.3.9; DoD c2.2.6.8.2; NARA 19]	R
7.1.12	6.2.2.4	An Application SHOULD support the use of Boolean and/or relational search operators such as "and" "or" "not" "less than" "greater than" "equal to." [MoReq 9.1.8; PRO A.3.13; DoD c2.2.6.8.4; NARA 19.1.19]	R
7.1.13	6.2.2.5	An Application SHOULD support wild card and/or pattern matching searches. [MoReq 8.1.11; PRO A.3.13; DoD c2.2.6.8.3; NARA 19.1.24]	R
7.1.14	6.2.2.6	An Application SHOULD support the iterative refinement of a search by adding search conditions to a previously run search—i.e. narrow a search. [MoReq 8.1.21; NARA 19.9]	R
7.1.15	6.2.2.7	An Application MAY support word proximity searching. [MoReq 8.1.12; NARA 19.1.20]	R
7.1.16	6.2.2.8	An Application MAY support searching null values. [DoD c2.2.6.8.6]	R
7.1.17	6.2.2.9	An Application MAY support searching time intervals. [MoReq 8.1.22]	R
x	6.2.3	***Responding to Requests***	SSS

7.3.3	6.2.3.1	An Institution MUST answer a consumer request with an appropriate response (a DIP fulfilling the entire request, a response denying the request, or a DIP fulfilling part of the request accompanied by a response clarifying why the request is only partially fulfilled). [CTDR B5.3]	R
6.1.2	6.2.3.2		
7.1.18	6.2.3.2	An Institution SHOULD document that consumer requests are responded to. [CTDR B5.5]	R
7.3.4	6.2.3.3	An Institution MUST disseminate DIPs that are authentic copies of their corresponding SIPs. [CTDR B5.6]	R
x	6.2.4	***Rendering Complex Objects***	SSS
7.2	x	**Generate DIP**	
7.2.1	6.2.4.1	An Application MUST render all of the components of a record along with their associated metadata in a logical manner. [Indiana 1.10.4; MoReq 8.1.15, 8.2.3; PRO A.3.21–A3.24; DoD c2.2.3.21; PERM 23; NARA 20.9, 20.11]	R
7.2.2	6.2.4.2	An Application MUST be able to render records on to appropriate output media, which should at least include graphical display and printer output. [MoReq 8.2, 8.3, 8.4.1; Pro A.3.25-26, A.3.28-29; PERM 3, 10, 14, 16, 17, 24, non dod 2; NARA 26.3.3, 26.4.1]	R
7.2.3	6.2.4.3	An Application SHOULD be able to render records into an open export format. [PRO A.3.31; NARA 26.4.3]	R
7.2.4	6.2.4.4	An Application SHOULD be able to render records independently of their creating environments. [MoReq 8.2.2; PRO A.3.22; DoD c3.2.14]	R
7.2.5	6.2.4.5	An Application SHOULD be able to render a record simultaneously for multiple users. [PRO A.3.23, DoD c2.2.7.5]	R
7.2.6	6.2.4.6	An Application SHOULD be able to render all versions of a record. [DoD c2.2.6.8.9]	R
x	6.2.5	***Rendering Recordness***	SSS
7.3.5	6.2.5.1	An Application MUST render a record’s content. [Pitt 11, 12; MoReq 8.2.3; PRO A.3.21; PERM 2; NARA 8.1.6.3, 20.11.1]	R
7.3.6	6.2.5.2	An Application MUST render a record’s structure. [Pitt 12, 12b, 12b1; PRO A.3.21; PERM 2; NARA 8.1.6.6, 20.11.4]	R
7.3.7	6.2.5.3	An Application MUST render a record’s context. [Pitt 12, 12b1, 12c; ISO 7.25; PERM 2]	R
7.3.8	6.2.5.4	An Application MUST render a record’s functionality. [Pitt 11b, DoD c2.2.5.3; NARA 8.1.6.5, 20.11.3]	R
x	6.2.6	***Redaction***	SSS
7.2.7	6.2.6.1		
7.3.9	6.2.6.1	Procedures SHOULD provide for the redaction of restricted content from records delivered to users that do not have the right to see the restricted output. [Pitt 13, MoReq 9.3.10; PRO A.2.56; NARA 20.11.2]	R
7.3.10	6.2.6.2	An Application SHOULD be able to create redacted versions of textual, audio, and moving image records. [MoReq 9.3.10; NARA 18]	R
7.3.11	6.2.6.3	An Application MUST NOT, if it can redact records, alter the content of a record while creating a redacted version of that record. [Pitt 13a; PRO A.2.56; NARA 18]	R