Document Title Requirements of a Trustworthy Electronic Recordkeeping System in a College or University Setting

Document Number 1.1

Version Draft for Public Comment

Date 08/16/05

NHPRC Grant Number 2004-083
I. Organization

1. Organization
   Outline of the organization of this document.

2. Introduction
   Definition of the purpose of this document and articulation of its basic assumptions.

3. Form of the Requirements
   The scope and syntax of the requirements for a trustworthy recordkeeping system, including sample requirements with explanations of each section of a requirement entry.

4. Recordkeeping System Requirements
   Lists and definitions of the requirements for a recordkeeping system creating, managing, and distributing authentic records. This section organizes the requirements into ten sections:
   4.1. Compliance
      An institution’s identification of and compliance with the laws, regulations, standards, and best practices that govern its recordkeeping practices.
   4.2. Creation and Capture
      An institution’s creation and capture of records through its recordkeeping application(s) and an institution’s requirement to create records to document its activities.
   4.3. Maintenance
      An institution’s identification and management of records in recordkeeping application(s), which includes location tracking, versioning management, and unique identifier management.
   4.4. Classification
      The development and management of classification schemes, which include records retention schedules, for records. The assigning of records to classes within a scheme or multiple schemes and the institutional context of these schemes.
   4.5. Retention and Disposition
      The act of executing the disposition of the records according to a records retention schedule. This usually means the act of removing records and its metadata from the recordkeeping application for either destruction or for transfer to a preservation application.
   4.6. Protection from Loss or Corruption
      An institution’s discovery and/or prevention of unauthorized, accidental, or unwanted deletion, change, or corruption of records.
   4.7. Preservation
      A recordkeeping application’s procedures and the institutions planning process to mitigate issues of media decay and hardware and software obsolescence and to allow the interoperability and openness of its records.
4.8. **Use Rights**
   An institution’s management of users’ right to view and/or receive the content of records.

4.9. **Discovery and Delivery**
   A recordkeeping application enabling users to search and discover records along with the application disseminating meaningful and functional records to users.

4.10. **Design and Performance**
   The software and hardware design and performance of the recordkeeping application, including system maintenance, scalability, design constraints, and testing and verification.

5. **Degrees of Obligation for each Requirement**
   Definitions of the three requirement levels for implementation of each requirement.

6. **Glossary of Terms**
   Definitions of the terms this document uses.

7. **Bibliography of Sources**
   Bibliographic entries on the ten reports upon which this report bases its requirements.
II. Introduction

This document 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 examined research includes:

- Indiana University, *Requirements for Electronic Records Management Systems*
  In this document referred to as: Indiana

- University of Pittsburgh, *Functional Requirements for Evidence in Recordkeeping*
  In this document referred to as: Pitt

- Center for Technology in Government, *Functional Requirements to Ensure the Creation, Maintenance, and Preservation of Electronic Records*
  In this document referred to as: CTG

- IDA Programme of the European Commission, *Model Requirements for the Management of Electronic Records*
  In this document referred to as: MoReq

- Public Records Office, *Functional Requirements for Electronic Records Management Systems*
  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*
  In this document referred to as: InterPARES

  In this document referred to as: DoD

- International Organization for Standardization, *ISO 15489-1: 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)
  In this document referred to as: PERM
• Health Information Privacy Protection Act
  In this document referred to as: HIPPA

See Section VII for a bibliography of these reports. This document 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.

The essential nature of the modern office at colleges and universities—complete with hybrid paper/electronic systems, digital environments established to support manipulation and repurposing of data at the expense of recordkeeping, obsolescence of hardware and software, media decay, the proprietary and idiosyncratic nature of applications, and other problems—makes it difficult for archivists to provide for the long-term preservation of authentic electronic records and maintain the accountability of the organizations and operations which those records are supposed to document. This nature of the modern office leads institutions to create and maintain electronic records that they cannot automatically trust and depend on in the same way that institutions trust and depend on traditional paper records. In general, archivists have difficulty preserving electronic records that are: (1) accessible, readable, or intelligible due to compatibility and obsolescence issues; (2) identifiable and retrievable due to an incongruence of classifications and/or taxonomies; and (3) reliable in the accuracy of their content due to the ease of updating and altering records, either inadvertently or purposefully.

In order to address these issues, an organization must recognize that the purpose of the preservation of electronic records is to transmit authentic electronic content across time and space that people can reasonably judge to be authentic. This is a continuous process that begins at the moment of creation.

Authenticity is the trustworthiness of the record as a record—that the record is what it purports to be and has not been tampered with or corrupted in essential respects. A person cannot automatically presume the authenticity of an electronic record, he or she must weigh the evidence that the record either is or is not what it purports to be and either has or has not been modified or corrupted in essential respects and then judge whether the record is authentic or not. Authenticity is not a component of a record but the judgment a person makes about a record. When this report refers to “authentic records” or “authentic electronic records” it is shorthand for records that a reasonable person would judge as authentic. One cannot judge the authenticity of a recordkeeping system, only its trustworthiness.

In order to be able to reasonably judge a record as authentic, one must be able to establish its identity and demonstrate its integrity. One must ensure that electronic records are clearly identifiable, of demonstrable integrity, and that accidental corruption or purposeful tampering has not occurred since they were created and set aside. One can accomplish this by maintaining the records in a trustworthy electronic recordkeeping
A trustworthy recordkeeping system ensures the preservation of a record’s identity and integrity, protecting it from corruption and tampering. Therefore, a record created/captured and managed in a trustworthy recordkeeping system can be presumed to be authentic.

The archival and records and information management communities have used the term electronic recordkeeping system in a number of ways. Some conceive of a recordkeeping system broadly as the entire framework of recordkeeping, while others conceive of it more narrowly, describing the specific computer application tasked to store records. In addition, the elements that make up a recordkeeping system and the factors (controls) that influence recordkeeping have been described interchangeably. The imprecise use of the term electronic recordkeeping system in documents articulating recordkeeping requirements, in addition to a limited interest and expertise, may have hindered university records professionals’ efforts to turn these documents into evaluation tools and detailed implementation and application development guidelines. In order to alleviate this problem, this report has explicitly defined a trustworthy electronic recordkeeping system and the composition of its elements. In addition it has also differentiated between the components of a recordkeeping system and the records controls that influence and shape an institution’s recordkeeping activities. This should allow this report to lend itself to easier translation into evaluation, development, and implementation guidelines.

A trustworthy electronic recordkeeping system is the combination of all the Recordkeeping Components—People, Institutions, Applications, Infrastructure, and Procedures—necessary for records to be created, collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition in a manner that provides a circumstantial probability of the authenticity of those records and a likelihood that a reasonable person would judge those records as authentic.

An Institution uses a combination of Components to help it meet its recordkeeping needs and expectations that are articulated or manifested in Records Controls—Requirements, Policies, Responsibilities, and Practices. For example, one or more of the Institution’s Procedures articulates the actions required to execute its Recordkeeping Policies. In turn, a Recordkeeping Procedure governs the Institution’s use and the behaviors of one or more of its Recordkeeping Applications. A Recordkeeping Application executes and helps individuals or units within an Institution execute the steps of recordkeeping Procedures which in turn articulate the actions required by the Institution’s Recordkeeping Policies. See Figure 1.
Records Controls
- Requirements (internal/external)
- Responsibilities (internal/external)
- Policies
- Practices

Institution

Recordkeeping System
- Institution
- People
- Procedures
- Infrastructure
- Applications

Figure 1
Relationship of Records Controls and Recordkeeping Systems

Recordkeeping Requirements, Responsibilities, Policies, and Practices—collectively known as Records Controls exert recordkeeping needs and expectations on the Institution. Requirements and Responsibilities and can be external and internal to the Institution. See the Glossary, Section VI, for how this report defines the components of Records Controls.

In response the Institution employs the components—the Institution’s People, Procedures, Infrastructure, and Applications, as well as the Institution itself as a single entity—that compose its Recordkeeping Systems to meet these needs and expectations. See the Glossary, Section VI, for how this report defines the components of Recordkeeping Systems.
III. Form of the Requirements

The requirements for a recordkeeping application described in Section III are for either the Application itself or for People, Institution, Procedure, or Infrastructure. No requirements are expressed as requirements for Recordkeeping System. As Records Controls themselves impose requirements on recordkeeping systems, the document does not include requirements for any Controls.

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

Several of the ten projects from which this report is based have requirements and sometimes even sections specifically devoted to authenticity, metadata, and documentation. Authenticity—creating the likelihood a reasonable person would judge records as authentic—is the goal of a recordkeeping system, it is not a component of a system. Therefore every requirement exists to work towards creating, maintaining, or delivering authentic records, but there are no requirements in this report explicitly about authenticity.

Documentation and metadata are the fundamental foundation of any trustworthy recordkeeping system. Virtually every facet of a recordkeeping system must be documented and this documentation is often written as metadata. Metadata and documentation are two of six concerns in this report. Concerns are implicit elements of nearly all of the requirements for a trusted recordkeeping system, but there are almost no requirements in this report explicitly about these concerns. Compliance with nearly every requirement requires addressing all six concerns.

The concerns are:

Audit Every action taken in a recordkeeping system to create, collect, organize, categorize, preserve, retrieve, use, or execute the disposition of a record must be auditable. This means that every recordkeeping action produces an account of itself that can be audited and the recordkeeping system must support a process that can execute audits.

Authorization Every action taken in a recordkeeping system to create, collect, organize, categorize, preserve, retrieve, use, or execute the disposition of a record must be undertaken by a person or unit within an institution that has the authority to undertake that action.

Bulk Operations Many actions taken in a recordkeeping system to create, collect, organize, categorize, preserve, retrieve, use, or execute the disposition of a record
must be able to be undertaken in a scaleable manner that will allow an institution to implement the action in a production workflow.

**Documentation** Documentation describing how to execute every action taken in a recordkeeping system to create, collect, organize, categorize, preserve, retrieve, use, or execute the disposition of a record must exist.

**Metadata** Many of actions taken in a recordkeeping system to create, collect, organize, categorize, preserve, retrieve, use, or execute the disposition of a record along with the documentation of these actions manifest themselves as metadata.

**Training** Every person undertaking an action taken in a recordkeeping system to create, collect, organize, categorize, preserve, retrieve, use, or execute the disposition of a record must have the training needed to execute the action successfully.

The requirements in this report are organized into ten sections. Each section has three to ten subsections. All of the requirements are nested within the subsections. Every section and subsection has a brief description. These descriptions are not requirements, rather they are explanations defining the nature and scope of each section and subsection.

Each requirement will have a unique number, the text of the requirement itself, and a citation to one or more of the ten research projects discussed in Section II. The text of the requirement itself will contain one of the five Recordkeeping Components (Application, Infrastructure, Institution, 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 2.
Figure 2
Example Requirement

<table>
<thead>
<tr>
<th>Section Title</th>
<th>Design Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section Description</td>
<td>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.</td>
</tr>
<tr>
<td>Subsection Title</td>
<td>Testing and Verification</td>
</tr>
<tr>
<td>Subsection Description</td>
<td>This subsection covers the testing and verification of the recordkeeping application’s and the infrastructure’s performance.</td>
</tr>
<tr>
<td>Recordkeeping Component</td>
<td>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.</td>
</tr>
<tr>
<td>Degree of Obligation</td>
<td>[Indiana 1.12; MoReq 11.2, 11.2.5]</td>
</tr>
<tr>
<td>Requirement</td>
<td></td>
</tr>
<tr>
<td>Citation</td>
<td></td>
</tr>
</tbody>
</table>
IV. Recordkeeping System Requirements

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.

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.

   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]

   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]

   1.1.3 *People* MUST understand the laws, regulations, standards, best practices and professional ethics that affect their recordkeeping activities. [ISO 8.2.4]

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.

   1.2.1 An *Institution* MUST comply with the laws, regulations, standards, best practices and professional ethics that affect its recordkeeping activities. [Indiana 1.1, 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]

   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]

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.

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]

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.

2.1 Generate Records

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

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]

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]

2.1.3 Procedures SHOULD include quality control mechanics to ensure that accurate records are created.

[Indiana 1.7; Pitt 7a]

2.1.4 People MUST have clearly defined responsibilities for creating records.

[ISO 6.3]

2.1.5 People SHOULD only create records using approved recordkeeping applications and recordkeeping procedures.

[Pitt 3a]

2.2 Preserve Integrity

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

2.2.2 A Recordkeeping Application SHOULD validate 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 Preserve Essential Aspects
This subsection covers the creation and capture of a record’s essential aspects 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 A Recordkeeping Application MAY 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 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.
2.5.2 A Recordkeeping Application MAY adopt one of the following general approaches 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]

2.6 Create and Capture Relations
This subsection covers the creation and capture of the relationships between records.

2.6.1 A Recordkeeping Application MAY be able to capture hyperlinks and other cross-references between records. [PRO A.8.17]

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

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]

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]

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 A Recordkeeping Application MUST 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 the recordkeeping system creates or captures during the creation or capture process. [Indiana 1.6.4; MoReq 6.1.1]

2.7.6 A Recordkeeping Application MUST be able to create and capture descriptive, technical, and contextual metadata.
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 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]

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 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 6.2.1; PRO A.2.2]

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

2.9 Records Registration  
This subsection covers the unique registration of records in a recordkeeping system.

2.9.1 An *Institution* MUST register records by assigning a unique identifier and documenting the date and time when the record is entered into the recordkeeping system.  
[Indiana 1.2.5; MoReq 7.1.5]

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.

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]
2.10.2 A Recordkeeping Application MUST persistently link the format versions of the same records together.
[PRO A.2.12]

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.

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

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]

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]

3.2 Location Tracking
This subsection covers the tracking of a record during its maintenance in a recordkeeping system.

3.2.1 A Recordkeeping Application MUST be able to track the location of records in a recordkeeping system.
[MoReq 4.4.1]

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]

3.2.3 Procedures MUST articulate steps that govern the receipt, removal, and movement of hardware and media that store electronic records.
[HIPPA 45CFR164.310(d)(1), 45CFR164.310(d)(2)(iii)]

3.3 Versioning
This subsection covers the management of versions of records while they are maintained in a recordkeeping system.
3.3.1 A Recordkeeping Application SHOULD support versioning.  
[Indiana 1.2.9]

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]

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]

3.3.4 A Recordkeeping Application MUST, if it supports versioning, document the version changes of a record since its creation.  
[InterPARES B.3]

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.

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]

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.

3.5.1 A Recordkeeping Application SHOULD be able to interoperate with its institution’s other applications.  
[MoReq 10.8.1-4]

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.

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]
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]

3.6.3 A Recordkeeping Application MUST maintain the logical relationships between multiple versions of the same record.
[DoD c2.2.3.19]

3.6.4 A Recordkeeping Application SHOULD identify the responsible custodian(s) of the records it maintains.
[PRO A.5.41]

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.

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.

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]

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

4.1.3 A Recordkeeping Application MAY allow the creation and defining of a vital records classification scheme.
[DoD c2.2.6.7]

4.1.4 A Recordkeeping 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]
4.1.5 A Recordkeeping Application MUST ensure that classification names are unique.
[PRO A.1.18]

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]

4.1.7 A Recordkeeping Application MUST NOT allow the deletion of classes that contain records.
[PRO A.1.9]

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]

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]

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.

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]

4.2.2 A Recordkeeping Application MUST be able to reassign a retention schedule to a record.
[PRO A.4.21]

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]

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

4.3.1 A Recordkeeping Application SHOULD support a naming scheme for classification taxonomies.
[MoReq 3.1.4]

4.3.2 A Recordkeeping Application MAY support user-defined naming schemes for classification taxonomies.
[MoReq 3.1.4]

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]

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]

4.3.5 A Recordkeeping Application MAY support the mandatory use of a naming scheme.
[PRO A.1.20, A.1.36]

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.

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.

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]

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]
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]

4.4.5 A Recordkeeping Application MAY support the use of controlled vocabulary terms to support the classification of records.
[PRO A.1.37]

4.4.6 A Recordkeeping Application MAY support records being classified as vital records.
[MoReq 4.3.6]

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

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]

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

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.

5.1 Compliance with Schedules
The subsection covers the need for the disposition of records to be executed in compliance with appropriate retention schedules.

5.1.1 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]

5.1.2 An Institution MUST assign retention schedules to all of its records.
[Indiana 1.8.6]
5.1.3 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]

5.1.4 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]

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

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

5.2.2 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;]

5.3 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.

5.3.1 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.

5.3.2 People MUST make a determination on the disposition of the record reviewed. 
[MoReq 5.2.10, 5.10]

5.3.3 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]

5.3.4 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]
5.3.5 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, HIPPA 45CFR164.310(d)(2)(ii)]

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

5.3.7 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.e]

5.3.8 A Recordkeeping Application SHOULD be able to retain metadata about records that it transfers to a preservation system. [DoD c2.2.6.5.4]

5.3.9 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]

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.

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]

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]

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]

6 Protection from Loss or Corruption
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.

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.

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]

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; HIPPA 45CFR164.308(a)(1)(ii)(A); IP A.2]

6.1.3 An Application SHOULD manage the security level of the records it maintains.

[MoReq 9.3.3, 9.3.5]

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]

6.1.5 An Application MUST NOT allow unauthorized creation of records.

[Pitt 8]

6.1.6 An Application MAY tailor its user interface to the user’s appropriate access level.

[PRO A.8.9]

6.1.7 Infrastructure MUST NOT allow unauthorized access to the workstations and hardware that contain or provide access to records.

[HIPPA 45CFR164.310(a)(1), 45CFR164.310(a)(2)(ii), 45CFR164.310(c)]
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]

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.

6.2.1 An Institution SHOULD create and maintain policies and procedures to detect, contain, and correct security violations. [HIPPA 45CFR164.308(a)(1)(i), 45CFR164.308(a)(6)(ii), 45CFR308(a)(5)(ii)(B), 45CFR308(a)(5)(ii)(D), 45CFR312(c)(1), 45CFR312(e)(2)(i), 45CFR310(a)(2)(ii)]

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; HIPPA 45CFR164.306(a)(2)]

6.2.3 Procedures MUST prescribe periodic software security updates. [HIPPA 45CFR164.308(a)(5)(ii)(A)]

6.2.4 An Institution SHOULD perform a periodic review of its security procedures. [InterPARES B.1.b; HIPPA 45CFR164.308(a)(8)]

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]

6.2.6 An Institution SHOULD create and maintain policies and procedures to perform regular reviews of audit logs and log-in attempts. [HIPPA 45CFR164.308(a)(1)(ii)(D), 45CFR164.308(a)(5)(ii)(C)]

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.

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]
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]

6.3.3 An Application MUST NOT hinder automated backup of the institution’s records.

6.3.4 Procedures SHOULD articulate the actions needed to be undertaken during primary system failure.  
[Pitt 2d; MoReq 4.3.5; HIPPA 45CFR164.308(a)(7)(i), HIPPA 45CFR164.308(a)(7)(ii)(C)]

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

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, c2.2.9.3, c2.2.9.3.1-2, c2.2.9.4-5; HIPPA 45CFR164.308(a)(7)(ii)(B)]

6.3.7 Institutions SHOULD test and review backup and failure mode procedures.  

6.4 Data Integrity
This subsection covers the enforcement of the data integrity of records in a recordkeeping system.

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]

6.5 Record Fixity
This subsection covers the maintenance of the fixity of records in a recordkeeping system.

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]

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.

7.1 Planning
This subsection covers the process of establishing plans for preserving records in a recordkeeping system over time.

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]

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]

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]

7.2 Preservation System Integration
This subsection covers the ability of a recordkeeping application to export records to a preservation system.

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]

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]

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.

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]

7.3.2 Procedures SHOULD allow for periodic checks for media deterioration.
[MoReq 11.7.2, 9.1.5]
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]

7.4 Technology Obsolescence
This subsection covers the prevention of records in a recordkeeping system being stranded on obsolete technologies.

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]

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]

7.5 Preserve Recordness
This subsection covers the preservation of the context, content, structure, and functionality of records in a recordkeeping system.

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

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]

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

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

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.
8.1 Access Controls
This subsection covers the development and management of processes that control the access of records in a recordkeeping system.

8.1.1 An Institution MUST develop and implement access control rules for its records.
[MoReq 4.6.5; ISO 9.7; PERM 25; HIPPA 45CFR 164.308(a)(3)(i), 45CFR 164.312(a)(1)]

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]

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

8.1.4 A Recordkeeping 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]

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.

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

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]

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]

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.

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]

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]

8.4 Authentication of Users
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.

8.4.1 Infrastructure SHOULD provide services for secure authentication.
[PRO A.5, A.5.1, A.5.11; DoD c2.2.7.1; HIPPA 45CFR164.312(d)]

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; HIPPA 45CFR164.312(d)]

8.5 Review Security Profiles
This subsection covers the process of reviewing and modifying user and record security profiles.

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; HIPPA 45CFR164.308(a)(3)(ii)(B)]

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.
[HIPPA 45CFR164.308(a)(4)(ii)(C)]

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

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]

9.1.2 A Recordkeeping Application SHOULD provide an integrated search interface.
[MoReq 8.1.2; PRO A.3.7]

9.1.3 A Recordkeeping Application SHOULD support external search engines in addition to any integrated search interface.
[PRO A.3.19]

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]

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]

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]

9.1.7 A Recordkeeping Application MUST support searching by records’ identifiers.
[MoReq 8.1.16, 8.1.23]

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

9.2 Query Techniques
This subsection covers the searching techniques a recordkeeping system employs to search the records it maintains.

9.2.1 A Recordkeeping Application SHOULD support the full text search of the records and metadata it maintains.
A Recordkeeping Application SHOULD support searching metadata fields containing controlled vocabulary terms managed by thesauri.

A Recordkeeping Application SHOULD support searching multiple metadata fields and/or full text of records.

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.”

A Recordkeeping Application SHOULD support wild card and/or pattern matching searches.

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.

A Recordkeeping Application MAY support word proximity searching.

A Recordkeeping Application MAY support searching null values.

A Recordkeeping Application MAY support searching time intervals.

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.

A Recordkeeping Application MUST render all of the components of a record and its metadata in a logical manner.

A Recordkeeping Application MUST be able to render records together with their associated metadata.
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.

9.3.4 A Recordkeeping Application SHOULD be able to render records into an open export format.

9.3.5 A Recordkeeping Application SHOULD be able to render records independently of their creating environments.

9.3.6 A Recordkeeping Application SHOULD be able to render a record simultaneously for multiple users.

9.3.7 A Recordkeeping Application SHOULD be able to render all versions of a record.

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.

9.4.1 A Recordkeeping Application MUST render a record’s content.

9.4.2 A Recordkeeping Application MUST render a record’s structure.

9.4.3 A Recordkeeping Application MUST render a record’s context.

9.4.4 A Recordkeeping Application MUST render a record’s functionality.

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

9.5.2 A *Recordkeeping Application* SHOULD ensure that records needed for secondary use are available.

[Indiana 1.10, 1.10.1; Pitt 12a]

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]

9.6 Browsing

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

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]

9.7 Redaction

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

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]

9.7.2 A *Recordkeeping Application* SHOULD be able to create redacted versions of textual, audio, and moving image records.

[MoReq 9.3.10]

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]

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.
10.1 Testing and Verification
This subsection covers the testing and verification of the recordkeeping application’s and the infrastructure’s performance.

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; MoReq 11.2, 11.2.5]

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

10.1.3 Infrastructure SHOULD reliably pass all tests and perform within stated acceptable ranges.
[Indiana 1.12; MoReq 11.2]

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]

10.1.5 A Recordkeeping Application SHOULD undergo formal verification and be provably correct.
[Pitt 4b, 4c]

10.2 System Maintenance
This subsection covers the maintenance of the recordkeeping application and infrastructure.

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

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]

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

10.2.4 An Institution SHOULD determine the acceptable ranges for downtime and minimum numbers of simultaneous users.
10.2.5 *Infrastructure* SHOULD be capable of fulfilling downtime and simultaneous user requirements laid out by the institution.

[MoReq 11.3]

10.3 User Interface

This subsection covers the user interfaces of a recordkeeping application.

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]

10.3.2 A *Recordkeeping Application* SHOULD follow generally accepted user interface guidelines by providing a consistent look and feel.

[PRO 8.1-3]

10.3.3 A *Recordkeeping Application* MAY provide a remote login facility.

[MoReq A.9.7]

10.3.4 A *Recordkeeping Application* SHOULD facilitate use by persons with disabilities by including accessibility features.

[PRO A.8.16]

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]

10.4 Scalability

This subsection covers scalability of the recordkeeping system.

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]

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]

10.4.3 A *Recordkeeping Application* SHOULD be capable of fulfilling its institution’s scalability requirements, and of operating within acceptable ranges.
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]

10.4.5 A Recordkeeping Application SHOULD provide the ability to synchronize multiple instances of all underlying data stores.
[DoD c2.2.3.24]

10.5 Design Constraints
This subsection covers the design constraints of the recordkeeping application.

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]

10.5.2 A Recordkeeping Application MAY support a distributed repository with multi-site service.
[PRO A.9.18]

10.5.3 A Recordkeeping Application SHOULD provide at least one version of backward compatibility.
[DoD c2.1.4]

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]
V. Degrees of Obligation for each Requirement

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. To ensure clarity and accuracy, this document adheres to the RFC 2119 standard for defining requirement levels.\(^1\) 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. 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 exist 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.)

---

VI. Glossary of Terms

Recordkeeping Application: Any electronic program that creates and/or imports and maintains, stores, and distributes electronic records.

Recordkeeping Component: the people, institutions, applications, infrastructure, and procedures necessary for records to be created, collected, organized, and categorized to facilitate the records’ preservation, retrieval, use, and disposition.

Recordkeeping Control: the requirements, policies, assigned responsibilities, and practices that govern a recordkeeping system.

Recordkeeping Infrastructure: All of the physical and administrative resources which enable the recordkeeping process. This includes, without exclusion, buildings, filing cabinets, computer hardware, computer networks and the auxiliary staff necessary to maintain the same.

Recordkeeping Institution: An established organization (American Heritage Dictionary). An Institution creates and uses records to conduct its business. For this document it refers specifically to colleges and universities, although institutions in other industries may adopt this document.

Recordkeeping Policy: Articulate the goals and aims of the institution that creates the policy. Policies exist as documents.

Recordkeeping People: The people who are directly involved with executing the Recordkeeping Procedures. Recordkeeping people perform all of the manual actions which involve records in the Recordkeeping System, including making appraisal decisions, conducting surveys and interacting with producers.

Recordkeeping Procedure: Procedures articulate the actions required to successfully complete a task. Procedures also describe how to execute those actions. Procedures articulate how an Institution will fulfill its policy requirements. Procedures exist as documents.

Recordkeeping Practices: Generally accepted ways of completing tasks involving records. Recordkeeping People will be exposed to Recordkeeping Practices during formal training or on the job.

Recordkeeping Requirements: Formal requirements imposed on the recordkeeping process. These may be exerted by a higher authority, such as a government entity, or internally by institutional bylaws.
Recordkeeping Responsibilities: Requirements imposed on the recordkeeping process exerted by the functional activities of the Institution.

*Recordkeeping System:* a manual or automated system in which records are created, collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition. Recordkeeping Components compose a Recordkeeping System.

*Trustworthy Electronic Recordkeeping System:* the combination of all the recordkeeping components (people, institutions, applications, infrastructure, and processes) necessary for records to be created, collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition in a manner that provides a circumstantial probability of the authenticity of those records.
VII. Bibliography of Sources

Indiana University, *Requirements for Electronic Records Management Systems*
In this document referred to as: Indiana

University of Pittsburgh, *Functional Requirements for Evidence in Recordkeeping*
In this document referred to as: Pitt

In this document referred to as: CTG

In this document referred to as: MoReq

Public Record Office, *Functional Requirements for Electronic Records Management Systems*
In this document referred to as: PRO

In this document referred to as: InterPARES


In this document referred to as: ISO

In this document referred to as: PERM
United States 45 Code of Federal Regulations 162 & 164: *Health Information Privacy Protection Act (HIPPA)*

In this document referred to as: HIPPA