AHIMA Standards Task Force

Information Governance Standards Project

Specification of Business Requirements for

Information Management Practices in Healthcare

Chicago, Illinois, USA

2016

Copyright ©2016 by the American Health Information Management Association. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, photocopying, recording, or otherwise, without the prior written permission of the AHIMA, 233 North Michigan Avenue, 21st Floor, Chicago, Illinois, 60601-5809 (<https://secure.ahima.org/publications/reprint/index.aspx>).

During the public comment process, notwithstanding the provisions noted above, this document may be reviewed by a commenter (reviewer) as part of AHIMA’s public comment process, and the commenter (reviewer) restricts access to the document only to him/herself, and only during public comment period.

**ISBN: TBD**

**AHIMA Product No.: TBD**

**Limit of Liability/Disclaimer of Warranty**: THIS DOCUMENT IS TO BE USED, AS IS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. WHILE EVERY PRECAUSTION HAS BEEN TAKEN IN THE PREPARATION OF THIS DOCUMENT, AHIMA ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMISSIONS. NEITHER IS ANY LIABILITY ASSUMED FOR DAMAGES RESULTING FROM THE USE OF THE INFORMATION OR INSTRUCTIONS CONTAINED HEREIN, IT IS FURTHER STATED THAT AHIMA IS NOT RESPONSIBLE FOR ANY DAMAGE TO OR LOSS OF DATA OR EQUIPMENT THAT RESULTS DIRECTLY OR INDIRECTLY FROM THE USE OF THIS DOCUMENT.

The websites listed in this document were current and valid as of the date of publication. However, webpage addresses and the information on them may change at any time. The user has the responsibility to perform his/her own web searches to locate any site addresses listed here that are no longer valid.

**Acknowledgement**

AHIMA thanks ARMA International for use of the following in adapting and creating materials for healthcare industry use in IG adoption:   Generally Accepted Recordkeeping Principles® and the Information Governance Maturity Model. [www.arma.org/principles. ARMA International 2013](http://www.arma.org/principles.%20ARMA%20International%202013).

For more information about AHIMA Press publications, including updates, visit <http://www.ahima.org/publications/updates.aspx>

**AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION**

**233 North Michigan Avenue, 21st Floor**

**Chicago, Illinois 60601-5809**

**ahima.org**

Table of Contents

[AHIMA Standards Task Force Members 2016 4](#_Toc456003122)

[Synopsis 6](#_Toc456003123)

[Specifications of HIM Business Requirements 9](#_Toc456003124)

[Principle of Health Information Availability: Business Requirements 9](#_Toc456003125)

[Principle of Health Information Integrity: Business Requirements 11](#_Toc456003126)

[Principle of Health Information Protection: Business Requirements 14](#_Toc456003127)

[Principle of Health Information Accountability: Business Requirements 15](#_Toc456003128)

[Principle of Health Information Transparency: Business Requirements 16](#_Toc456003129)

[Principle of Health Information Compliance: Business Requirements 17](#_Toc456003130)

[Principle of Health Information Retention: Business Requirements 18](#_Toc456003131)

[Principle of Health Information Disposition: Business Requirements 19](#_Toc456003132)

[Appendix 1: Glossary of Terms 20](#_Toc456003133)

# AHIMA Standards Task Force Members 2016

| **Name** | **Affiliation** |
| --- | --- |
| Kathleen Addison | Alberta Health Services |
| Linda Bailey-Woods | Plante Moran |
| DeShawna Hill-Burns | Advocate Trinity Hospital |
| Carlyn Doyle | Multnomah County Department of Assets |
| Susan Clark | eHealthcare Consulting |
| Alane Combs | Coastal Healthcare |
| Vicki Delgado | Kindred Hospital Albuquerque |
| Robert Giannini | ECRI Institute PSO |
| Elisa Gorton | St. Vincent's Medical Center |
| Darice Grzybowski | H.I.Mentors,LLC |
| Aviva Halpert | Advize Proactive Consulting |
| Regina Harrison | Veterans Health Administration |
| Aaron Haskett | Sutter Health |
| Beth Horn | Chapa-De Indian Health Services |
| Sandra Huyck | Beaumont Health System |
| Theresa Jones | Resurrection University |
| Satyendra Kaith | Kaplan Higher Education Group |
| Robin Keeney | VHC, Inc. |
| Katherine Lusk | Dallas Children’s Medical Center |
| Susan Lucci | Just Associates |
| Jennifer Manahan | Via Christi Clinic, PA |
| Marcia Matthias | Southern Illinois Healthcare |
| Tabitha McDaniel | McKesson |
| Lori McNeil Tolley | Boston Children's Hospital |
| Sharon Meyer | Ministry Health Care |
| Nicole Miller | Miller And Miller Associates |
| Megan Munns | Just Associates |
| Neysa Noreen | Children's Hospitals and Clinics of Minnesota |
| Sandra Nunn | KAMC Consulting |
| Michael Nusbaum | M.H. Nusbaum & Associates Ltd. |
| Teri Phillips | HSHS St Anthony’s Memorial Hospital |
| Bill Reisbick | William B Reisbick, Esq. |
| DeAnn Tucker | Owensboro Health |
| Mick Talley | University Bancorp of Ann Arbor |
| Christine Taylor | University of Washington Medicine |
| DeAnn Tucker | Owensboro Health |
| Traci Waugh | North Valley Hospital |
| Valerie Wilson | HCA Information Technology Services |
| Lee Wise | Summit Medical Center |
| Donna Young | Southern Illinois Healthcare |
| **AHIMA Staff** | |
| Dr. Anna Orlova | Senior Director, Standards |
| Harry Rhodes | Director, National Standards |
| Diana Warner | Director, HIM Practice Excellence |

# Synopsis

Built upon the established collaboration with the Integrating the Healthcare Enterprise (IHE) – a collaborative of health information technology (HIT) vendors, users and associations of healthcare professionals to develop interoperability standards – AHIMA will continue working with stakeholders guiding the development of functional standards to support health information management (HIM) practices.

To address user needs with HIT adoption, AHIMA has been leading the development of best practices and guidelines for information management and information governance as a part of a new globally-focused AHIMA initiative on Information Governance (IG).[[1]](#footnote-1),[[2]](#footnote-2) The IG initiative provides an organization-wide framework for managing information throughout its lifecycle, while, supporting the organization’s strategy, operations, regulatory, legal, risk, and environmental requirements. The AHIMA IG Initiative – a key component of AHIMA's overall strategy to develop guidelines, operating rules and standards for healthcare documentation practices – served as a foundation for the AHIMA-IHE collaborative activities, which resulted in publication of the AHIMA-IHE white paper “Health IT Standards for HIM Practices” (<http://qrs.ly/lb4vec0>) in 2015.

This document specifies HIM Business requirements for the eight AHIMA IG principles in health care (IGPHC) *information availability, integrity, protection, accountability, transparency, compliance, retention and disposition.* Table 1 shows AHIMA efforts for specifying business requirements completed in 2015 as a part of the AHIMA-IHE white paper as well as the 2016 effort of the AHIMA Standards Taskforce.

Table 1. Business Requirements Specified by IG Principle

|  |  |
| --- | --- |
| Information Governance Principles: Business Requirements | |
| 2015 AHIMA-IHE White Paper | 2016 Standards Taskforce |
| 1. Information availability 2. Information integrity 3. Information protection | 1. Information accountability 2. Information compliance 3. Information transparency 4. Information retention 5. Information disposition |

Specification of HIM business requirements is a part of the collaborative informatics-based approach for translating HIM practices into HIT standards that was deployed in the 2015 AHIMA-IHE White paper. This approach of guiding the development of HIT standards to support HIM practices is shown on Figure 1 below.

**Approach**



**IG Principles in Healthcare | Use Cases for Standards**

Figure 1. Approach for Guiding the Development of HIT Standards to Support HIM Practices

(Source: AHIMA-IHE White Paper, 2015)

**Target Audience**

This specification is targeted to

1. Organizations (e.g. healthcare organizations, public health agencies, payers/insurance companies, academia) involved in origination, management, and use of healthcare data
2. Health professionals that originate, manage, and use healthcare data
3. Implementers - Organization’s staff involved in implementation of HIT Systems
4. HIT vendors and consultants involved in the design, development and implementation of HIT systems
5. Health information exchange (HIE) entities that collect, manage, and exchange data
6. Standards developers at various standards development organizations (SDOs)
7. Consumers (e.g. patients, care givers, employees, employers) involved in creation, management, and use of healthcare data and
8. Educators involved in HIT, HIM and informatics training.

In 2016, we are only focusing on the target audiences in #1-6.

**Scope**

Because one of the goals of information governance is to manage information using an integrated, holistic, and enterprise approach, this specification is applicable to all classes and types of information (clinical, financial, administrative, operational) created, used, or received by a health care organization, regardless of media, format, or source. It includes, but is not limited to, externally generated information such as that generated through information exchange as well as patient-generated information.

**Development Process**

Business requirements have been derived from the description of business processes e.g. statements formulated by each principle in the 2014 AHIMA’s Information Governance Principles for Healthcare (IGPHC)[[3]](#footnote-3) white paper. The AHIMA Standards Taskforce subject matter experts (SMEs) conducted a thorough review of each statement in consensus-based discussions. In addition, the requirements were reviewed by a broader audience of HIM and other professionals as part of a public comment period. Finalized statements were further used to harmonize the requirements with the AHIMA Information Governance Adoption Model (IGAM)[[4]](#footnote-4), allowing that organizations interested in the IGAM assessment could prove that each requirement has been met.

**Glossary**

Glossary of Terms was developed in the 2015 AHIMA-IHE White paper “Health IT Standards for HIM Practices” (<http://qrs.ly/lb4vec0>). Appendix 1 contains the original Glossary of Terms with additional terms and definitions added during the development of the Specification of Business Requirements for

AHIMA IGPHC.

We are also in the process of uploading the terms from the Glossary into the Standards Knowledge Management Tool (SKMT, URL: http://www.skmtglossary.org/) – an international Joint Initiative for Global Standards Harmonization Health Informatics Document Registry and Glossary.

Sections that follow provide specifications of HIM business requirements for each IG principle.

# Specifications of HIM Business Requirements

## 

## Principle of Health Information Availability: Business Requirements

|  |
| --- |
| Definition |
| **Health Information Availability** is defined as the ability of an organization to maintain information in a manner that ensures *timely, accurate, and efficient* retrieval of information by authorized entity[[5]](#footnote-5). For example, information shall be available upon request by any authorized entity in the required output format (e.g. a viewable display for online and paper-based output). |

Specification 1: HIM Business Requirements: Health Information Availability

| Health Information Availability: Business Requirements |
| --- |
| 1. Ability to capture and maintain information in a manner that ensures timely, accurate (complete and correct), and efficient access and retrieval. – *See Integrity Requirement #1 and #5; Protection #9; Accountability #7; Transparency #5* |
| 2. Ability to access information across various systems (electronic and manual) and across patient populations. This includes the abilities to search, identify, locate, and retrieve clinical, payer, labor resource management and research information required to support organization’s ongoing activities via queries. This requirement is focused on how information from various sources is accessed. *– See Availability # 3; Integrity #5 and #7; Retention #1 and #6* |
| 3. Ability to search, identify, locate and retrieve an individual’s specific information from continually-expanding volumes of information, across multiple systems (including various HIT products, data warehouses, payer data systems, business and research information systems, and paper-based repositories. This requirement includes tracking sources where information resides. *– See Availability # 2; Integrity #5* |
| 4. Ability to assemble (via search, identify, locate and retrieve) information in a consistent and coordinated fashion (timely, complete and correct) from disparate electronic systems, both internal and external to the organization. *– See Integrity #5* |
| 5. Ability to present/provide information that originates from disparate electronic systems, both internal and external to the organization in a meaningful way, and for a specific purpose. *– See Integrity #5 and #16* |
| 6. Ability to link (semantically and contextually), map, couple, group or integrate clinical and business information in a timely, accurate manner, to support organizational business requirements.  *– See Integrity #5, #7, #16 and #17* |
| 7. Ability to address multiple demands for having the right information available at the right time, in the right place, and in the right context for an authorized requestor.*– See Availability # 2 and #3* |
| 8. Ability to access information created with legacy hardware and software systems within an organization. In case of impending system obsolescence, information with organizational value should be migrated to currently supported hardware/software and/or converted/migrated into a compatible format from non-compatible media (MAC vs PC) and non-compatible software versions. *– See Integrity #5* |
| 9. Ability to access information imported from an external organization by incorporating pertinent content into the organization’s health information system, e.g., by scanning, digitizing and codifying external information, as defined by organization and jurisdictional policies. *– See Integrity #5* |
| 10. Ability to maintain metadata services across all participating systems assigning structural and descriptive characteristics to information including data provenance information. The latter means the lineage of data or data life cycle that contains the data's origins and where it moves over time. Specific data elements include authors and dates of creation, modification, sending, receipt, access, etc.). *– See Integrity #15; Protection #5* |
| 11. Ability to ensure levels of redundancy, failover, contingencies and other risk management practices to minimize risks of non-availability of information due to a disaster, system malfunction, or data corruption. *– See Protection #5* |
| 12. Ability to ensure clinical and public health business continuity and availability of information during a disaster, system malfunction, or data corruption. *– See Protection #5; Retention #2* |
| 13. Ability to manage record lifecycle (create, use, migrate, manage, store, preserve, dispose) while complying with regulations and internal policies. *– See Retention #1* |
| 14. Ability to ensure permanently preserved (archived or contained in a tiered storage) information is managed in a manner that supports access of accurate information in a cost effective manner regardless of storage medium. *– See Disposition #10* |
| 15. Ability to maintain the workforce capabilities on the most current methods to capture, maintain and access information assuring the work processes consistencies despite of workforce turnover. |
| 16. Ability to enable trust in information by ensuring the timeliness, accuracy (completeness and correctness), and efficiency of information availability based on implementation of business requirements 1-14 above. |
| 17. Ability to maintain and update information inventories, i.e., inventory of data repositories, warehouses or resources from which to retrieve, store, and maintain data and information that includes, but are not limited to, application-specific databases, diagnostic biomedical devices, master patient indexes, patient medical records, ancillary health information systems, payer systems and other. |
| 18. Ability to create, maintain the data inventory for retention schedule. *– See Retention #5* |
| 19. Ability to specify the storage medium on which information will be maintained. *– See Retention #1* |

## Principle of Health Information Integrity: Business Requirements

|  |
| --- |
| Definition |
| **Health Information Integrity** – the state of being whole or unimpaired – is defined as the ability to maintain the structure and attributes of data, documents and records, in order to ensure representation of intended content and meaning in the output in the human usable format such as via display for online view and printed (paper-based) matter).[[6]](#footnote-6) |

Specification 2: HIM Business Requirements: Health Information Integrity

| Health Information Integrity: Business Requirements |
| --- |
| 1. Ability to maintain information in a manner that ensures confidence in its authenticity, timeliness, accuracy, and completeness. *– See Availability #1* |
| 2. Ability to maintain integrity of information to comply with safety, quality of care, and compliance to applicable voluntary, regulatory and legal requirements. *– See Compliance #1, #2, #4* |
| 3. Ability to maintain integrity of information through adherence to an organization’s policies and procedures, including compliance to retention, archive, and destruction guidelines and requirements. *– See Retention #2, #3* |
| 4. Ability to provide appropriate workforce training on information management and governance, in order to support integrity of information. |
| 5. Ability to ensure that an entity that requests information can trust the integrity of the information it receives, by ensuring the authenticity, timeliness, accuracy, completeness, reproducibility, consistency and admissibility of records for all purposes, including internal and external use, sharing, disclosure, exchange, release of information (ROI) and other purposes. *– See Availability #1-6, #8, #9* |
| 6. Ability to ensure the integrity of information through reliable system controls that support the organization’s ongoing activities across various systems. |
| 7. Ability to manage integrity of information received from disparate electronic systems, both internal and external to the organization, via data provenance, i.e., identification of original source of document creation, date of creation, and date of any changes of content of document or data within the document. *– See Availability #2, #6* |
| 8. Ability to demonstrate oversight by senior management of adherence to approved policies and procedures necessary to maintain reliability of information. |
| 9. Ability to ensure reliability of data and information based on the nature and type of healthcare organization processes and systems for creation and capture, processing, and other applicable stages of the information’s lifecycle. |
| 10. Ability to ensure that all output of information (viewable and printed)   * is assembled, formatted and presented (i.e., how information is presented to a human) in chronological order to guarantee the timeliness of information * preserves the status of originality to identify the original and subsequent sources of information (initial print vs. secondary print) * enables sequential page numbering * contains patient- and record-identifying data (document metadata) in all documentation. |
| 11. Ability to implement ongoing quality control measures including:   * deploying ongoing data quality controls with field-specific data edits built into systems/applications; * monitoring and correction of patient identity errors; * monitoring and correction of documentation completeness and data accuracy issues; and * monitoring and correction of data in adherence to existing standards. |
| 12. Ability to prove reliability and integrity of information through an audit process to validate measures (e.g., controls, protocols, metrics, key performance indicators) for ensuring the reliability and integrity of information. |
| 13. Ability to manage the process of amending information by displaying amended information for a completed encounter for a closed record. This display may include the amendment itself, author, date, and time of the amendment; any change in information is considered an amendment. The history of the amendments will be kept in an audit log. *– See Compliance # 6* |
| 14. Ability to manage the process of amending information by displaying amended information for an active encounter for an open record. This display may include the amendment itself, author, date, and time of the amendment; any change in information is considered an amendment. The history of the amendments will be kept in an audit log. *– See Compliance # 6* |
| 15. Ability to monitor, test and alert (automatically or via human intervention) hardware, network infrastructure, software, storage, and other system components for reliability of performance in order to support documentation integrity by reconciliation of input and output for all content interfaces, content assembly and system integration components. |
| 16. Ability to maintain formal change control processes and audit log of changes as part of a reliable information environment, so as to differentiate any dynamic changes of information (e.g., change in the value of the data element, change in a template, change of interface, change of processes and other) through viewable display and printing capability. – *See Compliance # 6; Availability #5* |
| 17. Ability to ensure that creation, authentication, revision, and completion of the episode of care’s content (e.g., a single entry, order, note, report or other record component) has viewable display; and various content components can be linked within an episode of care record. *– See Availability #5 and #6* |
| 18. Ability to establish parameters for “enable / disable” capabilities for “copy and paste” in HIT product. |
| 19. Ability to track “copy and paste” usage (e.g., via color coding, flags, notes, and/or using other visual identifiers), so information from a previous entry is identifiable and viewable in a subsequent entry, as well as presented in a complete chronological sequence within a single episode of care. This will include maintaining metadata on “copy and paste” usage in a data audit of the use of the “copy and paste” function including the source, date, time, author of performing copy and paste. |
| 20. Ability to establish parameters for “enable / disable” capabilities for a “pre-populate” in HIT product. |
| 21. Ability to track “pre-populate” usage (e.g., via color coding, flags, notes, and/or using other visual identifiers), so information from a previous entry is identifiable and viewable in a subsequent entry and presented in a complete chronological sequence within a single episode of care. This will include maintaining metadata on “pre-populate” usage in a data audit of the use of the “pre-populate” function including the source, date, time, author of performing pre-populate. |
| 22. Ability to maintain transition/change of ownership and any permanent change in custodianship of health information, such as when it is transferred to another party due to a merger or acquisition of another hospital, clinic, or physician practice or when an organization discontinues a practice, service, or other business;[[7]](#footnote-7) demonstrate that the transition/change of ownership and any permanent change in custodianship was successful implemented. |
| 23. Ability to ensure that when information is converted or migrated to new media, the integrity of the migrated information is preserved. |

## 

## Principle of Health Information Protection: Business Requirements

|  |
| --- |
| Definition |
| **Health Information Protection** is defined as guarding against (1) inappropriate acquisition, access, disclosure or use of protected health information (i.e., Information Availability) as well as (2) loss, tampering, and corruption of health information (i.e., Information Integrity).[[8]](#footnote-8) |

Specification 3: HIM Business Requirements: Health Information Protection

| Health Information Protection: Business Requirements |
| --- |
| 1. Ability to ensure appropriate levels of protection from breach, corruption and loss of information that is private, confidential, classified and essential to business continuity or that otherwise requires protection. |
| 2. Ability to consistently apply and enforce levels of protection to information, regardless of medium, from the moment the information is created until the moment it reaches or exceeds its retention period and is appropriately disposed. This specifically includes adherence to security, privacy and confidentiality requirements (rules, regulations, policies) when determining a method for the final disposition of information, regardless of source or media. This applies whether the disposition is archival, transfer to another organization, preservation for permanent storage, or destruction. *– See Disposition #5* |
| 3. Ability to establish an audit program that defines a clear process for verifying whether sensitive secure information is being handled in accordance with the organization’s policies and procedures. *– See Transparency #9* |
| 4. Ability to manage and balance compliance with the varying degrees of protection, mandated by laws, regulations, and/or organizational policies for information generated and managed by an organization. *– See Compliance #1* |
| 5. Ability to provide security, business continuity, and disaster recovery processes that will ensure continued operation and continued protection, during and after periods of failure or disruption. *–See Availability #10, #11 and #12* |
| 6. Ability to assign and manage appropriate levels of information access and security clearance to all members of the workforce and other authorized parties relevant to their roles or duties. *– See Transparency #6* |
| 7. Ability to maintain appropriate security safeguards, clearly defined and enforced by organizational policies, designed to protect electronic information from being inappropriately viewed, e-mailed, downloaded, uploaded, or otherwise proliferated—intentionally or inadvertently, even by individuals with legitimate access to the system. *– See Transparency #6* |
| 8. Ability to provide physical security safeguards of computing and access devices or any equipment containing private, secret, or confidential information or intellectual property of the organization. – *See Transparency #6* |
| 9. Ability to audit that information is   * appropriately protected, accessed, stored, and released with a properly documented audit trail *– See Compliance #4* * information is available whenever and wherever it is needed *– See Availability #1* * information is retained for the appropriate amount of time and properly dispositioned when no longer required. *– See Accountability #7; Retention #5; Disposition #5* |

## Principle of Health Information Accountability: Business Requirements

|  |
| --- |
| Definition |
| **Health Information Accountability** is the obligation of an individual or organization to account for its activities, accept responsibility for them, and to disclose the results in a transparent manner.  A qualified person, with executive sponsorship and authority, is charged with, and is accountable for, building and maintaining effective health information management functions and services. This professional is responsible for the stewardship of health information within the information governance framework of the organization[[9]](#footnote-9). |

Specification 4: HIM Business Requirements: Health Information Accountability

|  |
| --- |
| **Health Information Accountability: Business Requirements** |
| 1. Ability to continuously document, approve, communicate and train the workforce on policies and procedures to guide the accountability program implementation, remediate identified issues, and enable auditing as a means of demonstrating the organization is meeting its obligations to both internal and external parties. |
| 2. Ability to solicit input from stakeholders, business process owners, and domain experts to improve the accountability program as needed with details regarding improvements on specific roles and responsibilities of workforce member. |
| 3. Ability to conduct information governance practices with regular reporting to senior leadership on measurable outcomes defined by the program. *– See Transparency #7* |
| 4. Ability to ensure that senior leadership has the responsibility to oversee the information governance program and resources to support the program. *– See Transparency #7* |
| 5. Ability to ensure policies and procedures to guide an organization’s workforce and agents in conducting the audit. |
| 6. Ability to continuously improve an organization’s capability in demonstrating a workforce’s awareness about practices, policies, and responsibilities. |
| 7. Ability to audit that information is appropriately protected, accessed, stored, and released with a properly documented audit trail, information is available whenever and wherever it is needed, information is retained for the appropriate amount of time and properly dispositioned when no longer required. *– See Availability #1; Retention #3; Protection #9* |
| 8. Ability to ensure that policies and processes are up-to-date, adopted, and cover all types of information in all media. *– See Compliance #2 and #4* |

## Principle of Health Information Transparency: Business Requirements

|  |
| --- |
| Definition |
| **Health Information Transparency** is the degree to which stakeholders are made aware of how health information is created, collected, maintained, used and shared/exchanged/disclosed. Transparency is demonstrated through clear descriptions of the uses and sharing/exchange/disclosure of identified and de-identified, individual, or aggregate healthcare information.[[10]](#footnote-10) Transparency assures that information is created appropriately and in compliance with applicable regulation and organizational policies. |

Specification 5: HIM Business Requirements: Health Information Transparency

|  |
| --- |
| **Health Information Transparency: Business Requirements** |
| 1. Ability to document, in an open and verifiable manner, an organization’s processes and activities related to information governance. |
| 2. Ability to share an organization’s documentation with the workforce and other appropriate interested parties (e.g., business associates, patients and consumers, governmental authorities, auditors and investigators, litigants and/or the general public) within legal or regulatory limitations, and consistent with the organization’s business needs. |
| 3. Ability of the organization to define appropriate information uses and the processes for ensuring compliance with policies on appropriate information use. *– See Compliance #1, #2 and #3* |
| 4. Ability to document that the information governance program includes its information management and information control policies and procedures. |
| 5. Ability to:   * document the principles and processes that govern the information governance program * accurately and completely record the activities undertaken to implement the information governance program and * respond to any interested party in a timely manner. *– See Availability #1* |
| 6. Ability to have procedures put in place to control access to protected information, whether it relates to the confidentiality of information or the confidentiality of proprietary processes. *– See Protection #6, #7 and #8* |
| 7. Ability to create and manage the records documenting an organization’s information governance program, to ensure its structure, processes, and practices are transparent, understandable, and available as defined by organizational policies and jurisdictional laws (e.g., in time, appropriate requestors, etc.). *– See Accountability #3 and #4* |
| 8. Ability of an organization to ensure that stakeholders are made aware of how health information is created, acquired, collected, maintained, used, shared and disclosed.  *– See Availability ##1-9, #14 and #16* |
| 9. Ability to demonstrate transparency through clear descriptions of the uses and sharing of identified, de-identified and re-identified information on an individual, or aggregate healthcare information. – *See Availability ##1-9, #14 and #16; Protection #3* |

## Principle of Health Information Compliance: Business Requirements

|  |
| --- |
| Definition |

|  |
| --- |
| **Health** **Information Compliance** is the adherence to documentation policies, procedures, bylaws, mandated guidelines, laws, regulations, contractual agreements, and accreditation standards[[11]](#footnote-11) that impact quality, safety, efficiency and effectiveness of patient care. Compliance programs provide affirmative steps toward assuring ethical and lawful conduct by enhancing detection, resolution and prevention of instances of conduct that do not conform to federal, state or the healthcare organization’s ethical and business policies.[[12]](#footnote-12) |

Specification 6: HIM Business Requirements: Health Information Compliance

|  |
| --- |
| **Health Information Compliance: Business Requirements** |
| 1. Ability to comply with applicable laws, regulations, standards, and organizational policies for maintaining and managing health information. *– See Integrity #2; Transparency #3; Protection #4; Retention #4* |
| 2. Ability to show that the information management systems themselves are subject to legal and regulatory requirements, security access controls, and transaction audit logs. *– See Integrity #2; Protection #10; Accountability #8; Retention #4; Transparency #3* |
| 3. Ability to know what information (content) should be entered into the organization’s records to demonstrate its activities are being conducted in a lawful manner according with organizational policies. This may include business record rules, e-discovery and forensic data. *– See Transparency #3* |
| 4. Ability to enter information into its records in a manner consistent with laws and regulations. *– See Integrity #2; See Protection #9; Retention #6* |
| 5. Ability to maintain its information in the manner and for the time prescribed by law or organizational policy. |
| 6. Ability to develop internal controls to monitor and ensure adherence to rules, regulations, and program requirements, thus assessing and ensuring compliance. *– See Integrity #13 , #14 and #16; Retention #4; Disposition #6* |

## Principle of Health Information Retention: Business Requirements

|  |
| --- |
| Definition |
| **Health Information Retention** is the mechanism for storing, maintaining and preserving health  information (clinical, financial and operational). Retention includes the timeframe for which an organization is required to keep the record and process of record-keeping. Retention policies and procedures provide for timely retrieval, and establish the lengths of time information will be retained by the healthcare organization.[[13]](#footnote-13) Information should not be maintained beyond its useful life. |

Specification 7: HIM Business Requirements: Health Information Retention

|  |
| --- |
| **Health Information Retention: Business Requirements** |
| 1. Ability to ensure information preservation (i.e., archived information) is managed in a structured manner supporting ease of access to accurate information in a cost-effective manner regardless of storage medium. *– See Availability #2, #13 and #19* |
| 2. Ability to maintain an information lifecycle (store, maintain (including retain), make accessible and dispose, and preserve information). *– See Availability #12; Integrity #3* |
| 3. Ability to accommodate information lifecycle management as established by retention policies and schedules, taking into account legal, clinical, regulatory, accreditation, fiscal, operational and historical criteria for establishing the retention period related to specific information. *– See Integrity #3; Accountability #7; Disposition #1* |
| 4. Ability to maintain and update retention schedules, which define the information to be retained, how long it should be retained, and when disposition should occur. *– See Protection #9; Disposition #1; Compliance #1 and #6* |
| 5. Ability to set up and maintain the connection of the retention schedule to data inventories. *– See Availability #18; Protection #9* |
| 6. Ability to monitor compliance with retention policies and ensure that retention schedules are followed and updated as needed. *– See Compliance #4 and #8* |

## Principle of Health Information Disposition: Business Requirements

|  |
| --- |
| Definition |
| **Health Information Disposition** is defined as destruction or preservation of all health information (clinical, financial and operational) created and maintained by an organization in accordance with the records retention requirements. |

Specification 8: HIM Business Requirements: Health Information Disposition

|  |
| --- |
| **Health Information Disposition: Business Requirements** |
| 1. Ability to manage the process of disposition including identify, segregate, and purge/destroy information by criteria outlined in the retention schedules, and document the disposition process. Disposition “triggers” include day/month/year of discharge or encounter, day/month/year of report, date of patient birth, diagnoses, and other variables. *– See Retention #3* |
| 2. Ability to retain a disposition log by date of secure destruction or preservation in accordance with the organizational and jurisdictional policies and retention schedule. The log may include the patient name and ID number, admit/discharge/encounter dates as well as facility name and ID number. |
| 3. Ability to establish a process to authorize and enforce dispositions and procedures that provide methods of disposition. These may include shredding, incineration, long-term storage and other. |
| 4. Ability to certify that information is transported (e.g., moved to a vendor for destruction), and that the information has been destroyed in secure manner, completely and irreversibly, in accordance with the organizational and jurisdictional policies and retention schedule. |
| 5. Ability to ensure   * the disposition/destruction of the media (e.g., paper, images, optical disk, microfilm, DVD, CD-ROM, previous storage media, documentation from another facility or provider within the healthcare system, or external information) that contained health information, when this information is converted to new media (e.g., EHR, mHealth applications, etc.) according to the organizational policies and retention schedule. *– See Protection #2 and #9.* * Information integrity when information is moved from old to new media. – See Integrity #X * Audit log is created with data provenance, and that old media is disposed of securely. |
| 6. Ability to ensure all versions and copies of the information are accounted for in the disposition, i.e., ability to destroy all information and media according to retention schedules. *– See Compliance #6* |
| 7. Ability to place information on “destruction holds” which suspends the disposition of the information in the event of pending or reasonably-anticipated litigation, regulatory action, or other related activity. Ability to notify affected workforce when a destruction hold is issued. |
| 8. Ability to lift destruction holds and to notify the effected workforce, such that retention periods and disposition may resume. |
| 9. Ability to inform a patient about disposition policies, as required. |
| 10. Ability to ensure information preservation (i.e., archived information) is managed in a structured manner supporting ease of access to accurate information in a cost effective manner regardless of storage medium. *– See Availability #14* |
| 11. Ability to ensure that, when information is converted or migrated to new media, the disposition of the previous media will be warranted according to the organizational policies. |

# Appendix 1: Glossary of Terms

| Term | Definition |
| --- | --- |
| **Clinical pathway** | A flow of activities and documentation derived from the clinical guidelines as related to a specific episode of care (Figures 5 and 8).  Clinical pathway is a tool designed to coordinate multidisciplinary care planning for specific diagnoses and treatments. [[14]](#footnote-14)  Clinical pathway – also known as a clinical workflow document (specification or checklist) – is developed by physicians (medical informaticians) at the facility. It serves as a practice management protocol. This protocol defined information and data requirements (forms, documents) associated with the episode of care. The information and data requirements (forms, documents content) are also called case definitions, i.e., specific instructions on how to document specific activity within the function based on the clinical guidelines.[[15]](#footnote-15)  The oversight of the correct recording of information according to the clinical pathway protocol and case definition is conducted by the facility’s Clinical Documentation Improvement (CDI) team of the HIM department. CDI team is also involved in developing templates (standardized formats) for forms and documents used in the clinical pathway to document the episode of care/encounter.[[16]](#footnote-16) |
| **Chain of custody** | Please provide definition: |
| **Data life cycle** | Please provide definition: |
| **Data provenance** | This is a very broad topic that has many meanings in different contexts. The W3C Provenance Incubator Group developed a working definition of provenance as: ”Provenance of a resource is a record that describes entities and processes involved in producing and delivering or otherwise influencing that resource. Provenance provides a critical foundation for assessing authenticity, enabling trust, and allowing reproducibility. Provenance assertions are a form of contextual metadata and can themselves become important records with their own provenance.”[[17]](#footnote-17) |
| **Designated record set** | Organizations may be required to identify their designated record set, which is defined as a group of records maintained by or for a covered entity that is: The record of what you acted upon to treat the patient.   1. The medical records and billing records about individuals maintained by or for a covered healthcare provider 2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan 3. Used, in whole or part, by or for the covered entity to make decisions about individuals.”[[18]](#footnote-18)   With the definition of the designated record set in mind, the organization must identify the content and data sets specific to their facility. Once the necessary information for the designated record set has been determined, it is required that this information and content be defined and documented within organizational policies. |
| **Disclosure** | Defined by federal regulations disclosure as “the release, transfer, provision of, access to, or divulging in any othermanner of information outside the entity holding the information.”[[19]](#footnote-19) |
| **Document** | Any analog or digital, formatted, and preserved “container” of data or information[[20]](#footnote-20) |
| **Document/Form/Screen** | The terms “Form”, “Document” and “Screen” are used interchangeably in this white paper. This is a broad category that is being used for input modes. Form/document/screen is the representation of knowledge assembled from data collected during the Episode of care/Encounter or Function/Record Entry. Formal definitions of these terms are the following:  Forms are pages that allow users to fill in and submit information[[21]](#footnote-21)  Document is any analog or digital, formatted and preserved “container” of data or information.[[22]](#footnote-22)Screen prototype is a sketch of the user interface of each screen that is anticipated in a project.[[23]](#footnote-23)  Information in the Form/Document/Screen can be delivered as scanned document, pdf, structured text (based on HL7 CDA or FHIR standards) or message (string of data).  The content for specific forms/documents generated under the episode of care/encounter’s functions such as patients demographic, assessment notes, test orders and results, care plans, medication prescriptions and other (Table 1) is out of scope for this white paper. It may be developed under the IHE Content Profiles in the future. |
| **Electronic document management system (EDMS)** | A multi-component health information technology system designed to serve as a single central platform from which release of information is managed.[[24]](#footnote-24) |
| **Episode of care/ Encounter** | In this White paper, the **episode of care/encounter** is referred to a visit or multiple visits or interaction(s) between patient and provider and/or ancillary services within the facility. The type of episode of care/encounter is defined by the service type (e.g., inpatient, outpatient, emergency department (ED), long-term care and others). Additional discussions are needed to align the terms for episode of care/encounter/ and visit with terminology used by other countries.  The term “episode of care” is also the unit of payment under the home health prospective payment system (HHPPS)[[25]](#footnote-25)  Term **interaction** includes phone calls, e-mail communication, telemedicine sessions, e-visits and other. Specific states of the interaction (**registration, admission, disposition, discharge or transfer)** are the **states** of the patient’s interaction, as described under **Start and the End of the Episode of Care/Encounter** below. |
| **Function, event, step** | The episode of care/encounter is comprised of **functions/events/steps**.  The **Function** of the episode of care/encounter is defined as entity or the activity that involve a single healthcare department, service area or discipline, [[26]](#footnote-26) e.g., visit registration/admission; triage; nurse's and physician's assessment; laboratory and diagnostic testing; diagnosis and care plan; prescription; discharge/transfer/disposition and other (Figure 5).  The **Event** is defined as an action or activity that occurs within a system and/or network, inclusive of its boundaries.[[27]](#footnote-27)  The **Step** is defined as a sub-action or sub-activity that occurs within a specific event of care. |
| **Information actions listed below:** | |
| **access** | The ability of a subject to view, change, or communicate with an object in a computer system[[28]](#footnote-28) |
| **assemble** | Please provide definition |
| **capture** | The entering of data into a usable format. Data capture may be done in a manual or electronic format.[[29]](#footnote-29) |
| **couple** | Please provide definition |
| **group** | Please provide definition |
| **identify** | data that directly identifies a single individual[[30]](#footnote-30) |
| **integrate** | Please provide definition |
| **Link contextuall~~y~~** | Post- coordination (if x then y) |
| **link semantically** | Formal representation of a directed associative relation or partitive relation between two concepts[[31]](#footnote-31) |
| **locate** | Please provide definition |
| **map** | The process of associating concepts from one coding system with concepts from another coding system and defining their equivalence in accordance with a documented rationale and a given purpose[[32]](#footnote-32) |
| **present** | To submit for consideration or action. Immediate, not in the future[[33]](#footnote-33) |
| **print** | Output from a computer system that generates a file containing an image of information that can be printed[[34]](#footnote-34) |
| **provide** | Please provide definition |
| **retrieve** | Please provide definition |
| **search** | Please provide definition |
| **secondary print** | Please provide definition (define initial print vs. secondary print– See Integrity #10) |
| **Information inventory** | The inventory of data repositories, warehouses or resources from which to retrieve, store, and maintain data and information that includes, but are not limited to, application-specific databases, diagnostic biomedical devices, master patient indexes, patient medical records, ancillary health information systems, payer systems and other. |
| **Information Lifecycle** | The cycle of gathering, recording, processing, storing, sharing, transmitting, retrieving, and disposing of information (AHIMA)[[35]](#footnote-35) |
| **Legal health record (LHR)** | The subset of all patient specific data created or accumulated by a healthcare provider that constitutes the organization’s official business record, and is typically used when responding to formal requests for information for legal and legally permissible purposes[[36]](#footnote-36) |
| **Proof of integrity** | Please provide definition |
| **Record** | According to HIMSS, **record** is defined as a document stating results achieved or providing evidence of activities preformed.[[37]](#footnote-37)  Our record definition analysis showed the need to define further the relationship between records generated throughout healthcare delivery in the context of record lifecycle for the lifetime record, episode of care record, function record and record entry. We proposed the following record hierarchy and definitions:  **Lifetime Record (prenatal, birth-death)** is defined as longitudinal health record, i.e., a permanent, coordinated patient record of information that was acted upon to treat the patient, listed in chronological order and maintained across time from birth to death.[[38]](#footnote-38)  **Record of Episode of Care (admission-discharge)** is defined as full medical documentation generated during the episode of care, i.e., in a period of continuous medical care performed by healthcare professionals in relation to a particular clinical problem or situation. This period may include one or more healthcare services given by a provider. (For our purposes we are limiting the definition to inpatient status.)  **Documentation:** The recording of pertinent healthcare findings, interventions, and responses to treatment as a business record and form of communication among caregivers.[[39]](#footnote-39)  **Record at the Function Level or Record Entry** is defined as full medical documentation generated during the activities performed under a function. It is defined as the notation made in a patient's health record, whether paper or electronic, by the responsible healthcare practitioner to document an event or observation associated with healthcare services provided to the patient.[[40]](#footnote-40) For some functions, this can be o**ne document, e.g., registration form;** for other functions, in which several documents may comprise the record entry, e.g., testing: consent for procedure, test order, test result report.  Please note that in the standards development organizations (HL7, ISO), the term Record Entry is used for a single document only.  **Record at Data Entry Leve**l is defined as a collection of parts that are related to, or associated with, a record for a specific activity.  Using the terminology of the HL7 Clinical Document Architecture (CDA) standards, these parts follow the following hierarchy: record’s **Sections, Templates** and **Data** **Fields**.  Using terminology of HL7 Fast Healthcare Information Resource (FHIR) standard, these parts can be represented as record’s “**resources**.” These parts of the record can be completed by various business actors. |
| **Release of information (ROI)** | The process of disclosing patient identifiable information from the health record to another party.[[41]](#footnote-41) |
| **Tiered storage** | It is a storage networking method where data is stored on various types of media based on performance, availability and recovery requirements. For example, data intended for restoration in the event of data loss or corruption could be stored locally -- for fast recovery -- while data for regulatory purposes could be archived to lower cost disks.[[42]](#footnote-42) |
| **Use** | Under federal regulations; use of PHI is “the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.”[[43]](#footnote-43) |
| **Viewable display** | Please provide definition  e.g. in track changes or audit document) and a printed output (with and without changes) |

1. American Health Information Management Association (AHIMA). Information Governance Principles for Healthcare (IGPHC). Chicago, IL. 2014. URL: <http://www.ahima.org/~/media/AHIMA/Files/HIM-Trends/IG_Principles.ashx> [↑](#footnote-ref-1)
2. Cohasset Associates and American Health Information Management Association (AHIMA). Professional Readiness and Opportunity. Information Governance in Healthcare White Paper. Minneapolis, MN. 2015. URL: <http://www.ahima.org/~/media/AHIMA/Files/HIM-Trends/IGSurveyWhitePaperCR_7_27.ashx?la=en> [↑](#footnote-ref-2)
3. American Health Information Management Association (AHIMA). Information Governance Principles for Healthcare (IGPHC). Chicago, IL. 2014. URL: <http://www.ahima.org/~/media/AHIMA/Files/HIM-Trends/IG_Principles.ashx> AHIMA thanks ARMA International for use of the following in adapting and creating materials for healthcare industry use in IG adoption:   Generally Accepted Recordkeeping Principles® and the Information Governance Maturity Model. [www.arma.org/principles](http://www.arma.org/principles). ARMA International 2013. [↑](#footnote-ref-3)
4. American Health Information Management Association (AHIMA). Information Governance IQ, URL: IGIQ.org [↑](#footnote-ref-4)
5. American Health Information Management Association (AHIMA). Information Governance Principles for Healthcare (IGPHC). Chicago, IL. 2014. URL: <http://www.ahima.org/~/media/AHIMA/Files/HIM-Trends/IG_Principles.ashx> [↑](#footnote-ref-5)
6. In formulating this definition we revised the original definition of information integrity in AHIMA Pocket Glossary, 2013. [↑](#footnote-ref-6)
7. American Health Information Management Association (AHIMA). Information Governance Principles for Healthcare (IGPHC). Chicago, IL. 2014. URL: <http://www.ahima.org/~/media/AHIMA/Files/HIM-Trends/IG_Principles.ashx> [↑](#footnote-ref-7)
8. American Health Information Management Association (AHIMA). Pocket Glossary of Health Information Management and Technology. Chicago, IL. 2014. p.134 [↑](#footnote-ref-8)
9. American Health Information Management Association (AHIMA). Information Governance Principles for Healthcare (IGPHC). Chicago, IL. 2014. URL: <http://www.ahima.org/~/media/AHIMA/Files/HIM-Trends/IG_Principles.ashx> [↑](#footnote-ref-9)
10. American Health Information Management Association. "Information Governance Principles for Healthcare (IGPHC)TM." 2014 Chicago, IL. [↑](#footnote-ref-10)
11. Healthcare Information and Management Systems Society. HIMSS Dictionary of Healthcare Information Technology Terms, Acronyms and Organizations, 2nd Edition. Chicago, IL, 2010. p.24 [↑](#footnote-ref-11)
12. The Office of Inspector General Compliance Model – Provide Reference HERE [↑](#footnote-ref-12)
13. American Health Information Management Association. AHIMA Pocket Glossary of Health Information Management and Technology, 4th Edition. Chicago, IL, 2014. p.130 [↑](#footnote-ref-13)
14. American Health Information Management Association (AHIMA). Pocket Glossary of Health Information Management and Technology. Chicago, IL. 2014. p. 28 [↑](#footnote-ref-14)
15. Children’s Medical Center. Guide to clinical documentation improvement. 2nd Edition. Dallas, TX. 2015. [↑](#footnote-ref-15)
16. Solicit from SMEs the samples of such templates and/or provide the link to the examples of these templates. [↑](#footnote-ref-16)
17. World Wide Web Consortium (W3C). Provenance XG final report, 2010. URL <http://www.w3.org/2005/Incubator/prov/XGR-prov-20101214/> [↑](#footnote-ref-17)
18. American Health Information Management Association (AHIMA). Release of Information Toolkit. May 2013. URL: <http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_050184.pdf>. [↑](#footnote-ref-18)
19. United States Department of Health and Human Services (HHS). National Institutes of Health (NIH). How can covered entities use and disclose protected health information for research and comply with the privacy rule? URL: <http://privacyruleandresearch.nih.gov/pr_08.asp> [↑](#footnote-ref-19)
20. American Health Information Management Association (AHIMA). Pocket Glossary of Health Information Management and Technology. Chicago, IL. 2014. p. 49 [↑](#footnote-ref-20)
21. McGraw H. Dictionary of Scientific and Technical Terms. 2003 [↑](#footnote-ref-21)
22. American Health Information Management Association (AHIMA). Pocket Glossary of Health Information Management and Technology. Chicago, IL. 2014. p. 49 [↑](#footnote-ref-22)
23. Ibid, p.133 [↑](#footnote-ref-23)
24. Kohn, D. How information technology supports virtual HIM departments. JAHIMA. 2009, 80(3): URL: <http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_043005.hcsp?dDocName=bok1040035> [↑](#footnote-ref-24)
25. Ibid, p. 55 [↑](#footnote-ref-25)
26. Ibid p.62 [↑](#footnote-ref-26)
27. Health Information Management and Systems Society (HIMSS). Dictionary of Healthcare Information Technology Terms, Acronyms and Organizations. 2010. p.49 [↑](#footnote-ref-27)
28. American Health Information Management Association (AHIMA). Pocket Glossary of Health Information Management and Technology. Chicago, IL. 2014. 2014. p.1 [↑](#footnote-ref-28)
29. "SKMT Glossary Tool." SKMT Glossary Tool. Joint Initiative for Global Standards Harmonization Health Informatics Document Registry and Glossary, n.d. Web. 24 April 2016. URL: <http://www.skmtglossary.org/search.aspx?term_id=8674&SearchExp=capture>. [↑](#footnote-ref-29)
30. International Organization of Standardization (ISO). ISO 25237:2008. [↑](#footnote-ref-30)
31. Ibid. Data capture. [↑](#footnote-ref-31)
32. American Health Information Management Association (AHIMA). Pocket Glossary of Health Information Management and Technology. Chicago, IL. 2014. 2014. p.91 [↑](#footnote-ref-32)
33. A Law Dictionary, Adapted to the Constitution and Laws of the United States. By John Bouvier. (1856). Retrieved April 20 2016. URL: <http://legal-dictionary.thefreedictionary.com/present> [↑](#footnote-ref-33)
34. American Health Information Management Association (AHIMA). Pocket Glossary of Health Information Management and Technology. Chicago, IL. 2014. 2014. p.119 [↑](#footnote-ref-34)
35. American Health Information Management Association (AHIMA). Information Governance Principles for Healthcare (IGPHC). Chicago, IL. 2014. URL: <http://www.ahima.org/~/media/AHIMA/Files/HIM-Trends/IG_Principles.ashx> [↑](#footnote-ref-35)
36. Servais CE. The legal health record. AHIMA, Chicago, IL [↑](#footnote-ref-36)
37. Health Information Management and Systems Society (HIMSS). Dictionary of Healthcare Information Technology Terms, Acronyms and Organizations. 2010. p. 101 [↑](#footnote-ref-37)
38. American Health Information Management Association (AHIMA). Pocket Glossary of Health Information Management and Technology. Chicago, IL. 2014. p.88 [↑](#footnote-ref-38)
39. Same, p.50 [↑](#footnote-ref-39)
40. Same, p.70 [↑](#footnote-ref-40)
41. American Health Information Management Association (AHIMA). Pocket Glossary of Health Information Management and Technology. Chicago, IL. 2014. p.128 [↑](#footnote-ref-41)
42. ITBusinessEdge. Webopedia. URL: <http://www.webopedia.com/TERM/T/tiered_storage.html>. 2016. [↑](#footnote-ref-42)
43. United States Department of Health and Human Services (HHS). Administrative Data Standards and Related Requirements: Definitions [↑](#footnote-ref-43)