AHIMA Standards Task Force

HIM Standards for HIM Practice Project

Specification of Business Requirements for

AHIMA Information Governance Principles for Health Care (IGPHC)

Chicago, Illinois, USA

2016

Table of Contents

[Synopsis 3](#_Toc439935415)

[Specifications of HIM Business Requirements 5](#_Toc439935416)

[Principle of Information Availability: Business Requirements 5](#_Toc439935417)

[Principle of Information Integrity: Business Requirements 6](#_Toc439935418)

[Principle of Information Protection: Business Requirements 7](#_Toc439935419)

[Principle of Information Accountability: Business Requirements 8](#_Toc439935420)

[Principle of Information Transperancy: Business Requirements 9](#_Toc439935421)

[Principle of Information Compliance: Business Requirements 10](#_Toc439935422)

[Principle of Information Retention: Business Requirements 11](#_Toc439935423)

[Principle of Information Disposition: Business Requirements 12](#_Toc439935424)

# 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 vendors 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) such as *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)

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

# Specifications of HIM Business Requirements

## 

## Principle of Information Availability: Business Requirements

|  |
| --- |
| Definition |
| **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,[[3]](#footnote-3) i.e., information shall be available upon request of authorized entity.  This information may be used by:   * The healthcare team, patients, and other caregivers * Authorized members of the workforce and others authorized users consistent with regulations * Legal and compliance authorities for discovery and regulatory review purposes and * Internal and external reviewers for purposes including but not limited to payer audit, financial audit, case management, and quality assurance. |

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. |
| 2. Ability to search, identify, locate and retrieve patient specific information in continually expanding volumes of information and across multiple systems including various electronic HIS and manual systems (paper-based document locations, storages, etc.). This requirement is focused on tracking sources where information resides (HISs, other HICT products and manual systems). |
| 3. Ability to access information across various systems (electronic and manual) and across patient populations. This includes the abilities to search, identify, locate, and retrieve the information required to support organization’s ongoing activities via queries. This requirement is focused on how information from various sources is accessed. |
| 4. Ability to assemble information from disparate electronic systems, both internal and external to the actual or virtual location(s) of the organization. |
| 5. Ability to address multiple demands for having the right information available at the right time for the right requestor. |
| 6. Ability to access information created with legacy hardware and software systems. In case of impending system obsolescence, information with organizational value should be migrated to currently supported hardware and/or converted into a machine-readable format. |
| 7. Ability to maintain metadata services across all participating systems assigning structural and descriptive characteristics to information including data provenance information (authors and dates of creation, modification, sending, receipt, access, etc.). |
| 8. 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. |
| 9. 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. |
| 10. Ability to enable trust of requestor in information by ensuring the timeliness, accuracy (completeness and correctness), and efficiency of information availability based on implementation of business requirements 1-9 above. |

## Principle of Information Integrity: Business Requirements

|  |
| --- |
| Definition |
| **Information Integrity** – the state of being whole or unimpaired – is defined as the ability of data to maintain its structure and attributes to assure representation of intended content and meaning.[[4]](#footnote-4) |

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. |
| 2. Ability to maintain integrity of information to comply with safety, quality of care, and compliance with applicable voluntary, regulatory and legal requirements. |
| 3. Ability to maintain integrity of information in adherence to the organization’s policies and procedures. |
| 4. Ability to provide appropriate workforce training on information management and governance to support integrity of information. |
| 5. Ability to enable trust of requestor in the integrity of information by ensuring the authenticity, timeliness, accuracy, and completeness, admissibility of records for litigation purposes. |
| 6. Ability to ensure 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 actual or virtual location(s) of the organization. |
| 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 implement ongoing quality control measures to include field-specific data edits built into systems/applications; monitoring and correction of patient identity errors; monitoring and correction of documentation completeness and data accuracy; and ongoing data quality controls, and monitoring and correction in adherence to existing standards. |
| 11. Ability to prove reliability and integrity of information through audit process to validate measures for ensuring the reliability and integrity of information. |
| 12. Ability to monitor hardware, network infrastructure, software, storage, and other system components for reliability of performance. |
| 13. Ability to maintain formal change control processes as part of a reliable information environment. |
| 14. Ability to test HIS capabilities to support business requirements 1-13 including validation of data and all appropriate metadata. |

## 

## Principle of Information Protection: Business Requirements

|  |
| --- |
| Definition |
| **Information Protection** is defined as guarding against “(1) inappropriate acquisition, access, disclosure or use of protected health information as well as (2) loss, tampering, and corruption of health information.”[[5]](#footnote-5) Thus, part 1 of this definition relates to protection of Information Availability and part 2 – to protection of Information Integrity. |

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 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. |
| 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. |
| 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. |
| 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. |
| 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. |
| 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. |
| 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. |

## Principle of Information Accountability: Business Requirements

|  |
| --- |
| Definition |
| **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[[6]](#footnote-6). |

Specification 4: HIM Business Requirements: Health Information Accountability

|  |
| --- |
| **Health Information Accountability: Business Requirements** |
| 1. Establish senior leadership responsibility to oversee the information governance program and resources to support the program.  Ability to document and verify acceptance of senior leadership individuals to oversee the information governance program and resources to support the program.  Ability to document qualifications for those in the roles of executive sponsorship or authority. |
| 2. Establish adoption of information governance practices with regular reporting to senior leadership.  Ability to document implementation and adoption plan.  Ability to create executive summary reports that will be delivered with designated frequency and to whom they are shared. |
| 3. Adopt policies and procedures to guide its workforce and agents and ensure its program can be audited and continually improved to support the organization’s goals.  Ability to create and document policies in an organized manner.  Ability to effectively make policies available to all staff with notifications mechanism of new or revised policies. |
| 4. Establish the program throughout the organization and continuously document, approve, communicate and train on policies and procedures to guide the program implementation, remediates identified issues, and enable auditing as a means of demonstrating the organization is meeting its obligations to both internal and external parties.  Ability to document IG program plan and requirements.  Ability to document creation, revision, review, and approval process for policies.  Ability to create and document process for training and retraining. |
| 5. Establish the program throughout the organization with input of stakeholders, business process owners, and domain experts, assigning defined roles and responsibilities to workforce member.  Ability to define and document stakeholders, business process owners, and domain experts by role.  Ability to facilitate policy feedback from end users, review feedback with identified committee, and respond. |
| 6. Ability to audit that the workforce demonstrates program awareness, 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 when and where it is needed, information is retained for the right amount of time and properly dispositioned when no longer required |
| 8. Ability to audit that policies are up-to-date, adopted, and cover all types of information in all media and the process by which this is completed. |
| 9. Ability to calculate program benchmarks and progress toward goals. |
| 10. Ability to make available program metrics and goals visible to all staff. |

## Principle of Information Transperancy: Business Requirements

|  |
| --- |
| Definition |
| **Information Transparency** is the degree to which stakeholders are made aware of how health information is created, collected, maintained, used, shared and disclosed. Transparency is demonstrated through clear descriptions of the uses and sharing of identified and de-identified, individual, or aggregate healthcare information[[7]](#footnote-7). |

Specification 5: HIM Business Requirements: Health Information Transparency

|  |
| --- |
| **Health Information Transparency: Business Requirements** |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

## Principle of Information Compliance: Business Requirements

|  |
| --- |
| Definition |
| **Information Compliance** is the prevention, detection, and resolution of instances of conduct that do not conform to federal, state, or the healthcare organization's ethical and business policies. Compliance is the adherence to policies, procedures, bylaws, guidelines, laws, regulations, contractual agreements, and accreditation standards[[8]](#footnote-8). |

Specification 6: HIM Business Requirements: Health Information Compliance

|  |
| --- |
| **Health Information Compliance: Business Requirements** |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

## Principle of Information Retention: Business Requirements

|  |
| --- |
| Definition |
| **Information Retention** is the mechanism for storing, maintaining and preserving health information. Retention policies and procedures provide for timely retrieval, and establish the lengths of time that various types of records (and/or) information (sets) will be retained by the healthcare organization[[9]](#footnote-9). |

Specification 7: HIM Business Requirements: Health Information Retention

|  |
| --- |
| **Health Information Retention: Business Requirements** |
| 1. Definition of “Use Case”. A concise scenario that maps standards for what functions the computer can perform to aid Specification #7 Health Information Retention. Use “crisp” statements and principles to:   \* Segment EHR clinical (and other information) to earmark appropriate retention time intervals;  \* To be based on Federal, State, and Local laws and regulations. Accreditation standards. Professional Society guidelines;  \* Including Metadata to enable tracking the source of the data (who, what, when, location); and,  \* Including legal defense needs, discovery, litigation holds, etc. |
| 1. The life cycle of records management begins when information is created and ends when information is destroyed. The goal is for organizations to manage each step in the record life cycle to ensure record availability. Health information resides in multiple storage media and locations creating the need for a clearly defined record retention plan. Record retention schedules must:   \* Ensure that patient health information is available to meet the needs of continued patient care, legal requirements, research, education and other legitimate uses;  \* Include guidelines that specify what information is kept, and the storage medium on which it will be maintained (e.g. paper, microfilm, optical disc, magnetic tape); and,  \* Include clear destruction policies and procedures that include appropriate methods of destruction for each medium on which information is maintained. |
| 1. Federal Retention Requirements. Examples:   \* Institutional Review Board (IRB) documentation. (patient consent, investigation/study proposals, correspondence, minutes, IRB policies and procedures, patient injury, etc.);  \* EMTALA ED patient care, screening exam, transfer documentation, ED log, etc.:  \* Behavioral Health/Substance Abuse treatment records (42 CFR);  \* Medicare Conditions of Participation record retention (for Hospitals 5 years; for Critical Access Hospitals 6 years;  \* OSHA. 30 years for employees exposed to toxic substances;  \* HIPAA Privacy Requirements (actual/potential breach reporting, policy and procedure, staff education, etc.);  \* Radioactive drug records;  \* Higher Education Act of 1965 (20 USC Sec. 1232g); and,  \* Others. |
| 1. State and Local Retention Requirements: 2. Organizations with multi-state locations must carefully research the statutes and regulations for each state. When state requirements differ, there are at least two options:   \* Utilize the longest retention requirements among the various states; or,  \* Where requirements are substantially dissimilar, a retention “grid” will need to be constructed to specifically set forth each state’s requirements discreetly. The computer will need to be programmed to utilize the requirements of the state where the facility that created the record is located.   1. The clinical record retention requirements for records of adults, minors, and deceased patients will often be different. Also, many states have statutes that “toll” (or delay) the statute of limitation for delayed discovery of negligence, fraud, etc. Example retention periods:   \* Adult patients. 7 years;  \* Minor patients. Age of Majority (18 or 21 years), plus the length of the statute of limitations; and,  \* Deceased patients. 5 years after death.   1. Certain types of records may need to be retained “permanently”. Examples:   \* Institutional Review Board. (Minutes, policies, consents, etc.);  \* Inpatient Admission Log;  \* Birth Certificates and Logs;  \* Death Certificates and Logs;  \* Discharge from the OR and Log;  \* Index to Patient Records; and.  \* Tumor Registry.   1. State Record Retention Requirements may include:   \* Sexually transmitted diseases;  \* Child/Vulnerable Adult Abuse;  \* Communicable Diseases;   1. Radiation Exposure Monitoring (OSHA and State Counterpart);   \* Blood Bank/Transfusions;  \* Medical Staff/Nursing CME Records;  \* Professional Licensing/Credentialing Records;  \* Gunshot/Stab Wound Care. |
| 1. Accreditation Record Retention Requirements: Joint Commission/NCQA, etc. |
| 1. Litigation holds, potential claims, investigations. Records involved in any open investigation, audit, or pending/potential litigation must not be destroyed until the matter has been formally closed and the statute of limitation expires. |
| 1. Destruction. State laws may require an abstract of Destroyed Patient Care Information, and specification of which method of destruction was utilized (which must provide no possibility of reconstruction of the information). The abstract should state that the records were destroyed in the “normal course of business” pursuant to the Record Retention Policy. Also, it must bear the signatures of those individuals supervising and witnessing the destruction. Business Associates Agreements must be utilized if outsourcing the destruction |
| 1. Establish an authority to create and enforce a retention policy and procedure that addresses 1) specificity of information stored on all types of media, (paper, images, optical disk, microfilm, DVD, and CD-ROM) 2) the time period for which this information is kept. (Kathy Downing, 2013) |
| 1. Inventories 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, and patient medical records and health information (Kathy Downing, 2013) |
| 1. Establish and authority to monitor compliance and vet retention regulations and standards |
| 1. Ensure the availability of timely, relevant data and information for patient care purposes. (Kathy Downing, 2013) |
| 1. Specify what information is kept, the time period for which it is kept, and the storage medium on which it will be maintained (e.g., paper, microfilm, optical disk, magnetic tape). (Kathy Downing, 2013) |
| 1. Establish and authority to create and enforce a destruction policy and procedure that includes appropriate/compliant methods of destruction and documentation of the destruction for each medium on which information is maintained. (Kathy Downing, 2013) |

## Principle of Information Disposition: Business Requirements

|  |
| --- |
| Definition |
| **Information Disposition** includes destruction as well as 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[[10]](#footnote-10). |

Specification 8: HIM Business Requirements: Health Information Disposition

|  |
| --- |
| **Health Information Disposition: Business Requirements** |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

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> 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-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> [↑](#footnote-ref-3)
4. In formulating this definition we revised the original definition of information integrity in AHIMA Pocket Glossary, 2013. [↑](#footnote-ref-4)
5. American Health Information Management Association (AHIMA). Pocket Glossary of Health Information Management and Technology. Chicago, IL. 2014. p.134 [↑](#footnote-ref-5)
6. 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-6)
7. American Health Information Management Association. "Information Governance Principles for Healthcare (IGPHC)TM." 2014 Chicago, IL. [↑](#footnote-ref-7)
8. 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-8)
9. American Health Information Management Association. *AHIMA Pocket Glossary of Health Information Management and Technology*, 4th Edition. Chicago, IL, 2014. p.130 [↑](#footnote-ref-9)
10. 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-10)