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](#_Toc444093521)

[Specifications of HIM Business Requirements 5](#_Toc444093522)

[Principle of Health Information Availability: Business Requirements 5](#_Toc444093523)

[Principle of Health Information Integrity: Business Requirements 7](#_Toc444093524)

[Principle of Health Information Protection: Business Requirements 9](#_Toc444093525)

[Principle of Health Information Accountability: Business Requirements 10](#_Toc444093526)

[Principle of Health Information Transperancy: Business Requirements 12](#_Toc444093527)

[Principle of Health Information Compliance: Business Requirements 13](#_Toc444093528)

[Principle of Health Information Disposition: Business Requirements 14](#_Toc444093529)

[Principle of Health Information Retention: Business Requirements 15](#_Toc444093530)

# 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)

**Target Audience**

This specification is targeted to

1. Organizations (e.g. healthcare organizations, public health agencies, payers/insurance companies, academia) and professionals that originates, manages, and use healthcare data
2. HIT Vendors and consultants involved in the design and implementation of HIT systems
3. HIEs that collect, manage, and share data
4. SDOs
5. Consumers (e.g. patients, care givers, employees, employers) involved in data origination, management, and use of healthcare data
6. Implementers - Organization’s staff involved in implementation of HIT Systems
7. Educators of HIT programs – need to be reflected in core domains

In 2016, we are only focusing on the target audiences in #1-4. In the initial analysis (January – March) we are focusing on target audience #1.

Incorporate to address that these requirements are applicable to ALL technical actors (IS), so the term entity in the context of IHE definitions of actors is Content Creator (sender) and Content Consumer (receiver)

**Development Process** (Received feedback that business requirements should be objectively verifiable – Need to be able to prove that each requirement has been met e.g. an audit)

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

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) i.e., information shall be available upon request of authorized entity in the output (via a viewable display for online and printed (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. |
| 2. Ability to access (i.e., information is there and I can get to it) information across various systems (electronic and manual) and across patient populations, payers, labor resource management and research. This includes the abilities to search, identify, locate, and retrieve (see item 3 below) the information required to support organization’s ongoing activities via queries. This requirement is focused on how information from various sources is accessed. |
| 3. Ability to search, identify, locate and retrieve individual’s specific information in continually expanding volumes of information and across multiple systems including various electronic HIS, data warehouses, payer data systems, business and research information systems, and manual repositories (paper-based document locations, storages, etc.). This requirement is focused on tracking sources where information resides (HISs, other HICT products and manual repositories). |
| 4. Ability to assemble (via search, identify, locate and retrieve) information in a consistent and coordinated fashion (timely and accurate (complete and correct)) from disparate electronic systems, both internal and external to the organization. |
| 5. Ability to present/provide information for a specific purpose from disparate electronic systems, both internal and external to the organization. |
| 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. – Data Integrity, data provenance |
| 7. Ability to address multiple demands for having the right information available at the right time for the right requestor. |
| 8. 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/migrated into   * a compatible format from non-compatible media (MAC vs PC), non-compatible software versions and * a machine-readable format (scanned, digitized, coded, and other).   –Pt registration and ToC Use cases |
| 9. 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 |
| 10. 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. |
| 11. Ability to ensure clinical and public health business continuity and availability of information during a disaster, system malfunction, or data corruption. |
| 12. Ability to manage record lifecycle (create, use, migrate, manage, store, preserve, dispose) while complying with regulations and internal policies. - Retention |
| 13. 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.-Retention |
| 14. 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. |
| 15. 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. |

Actors for the use cases: 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

## Principle of Health Information Integrity: Business Requirements

|  |
| --- |
| Definition |
| **Health Information Integrity** – the state of being whole or unimpaired – is defined as the ability of data, documents and records to maintain their structure and attributes to assure representation of intended content and meaning in the output in the human usable format (via a viewable display for online and printed (paper-based) output).[[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. – cross reference with availability |
| 2. Ability to maintain integrity of information to comply with safety, quality of care, and compliance with applicable voluntary, regulatory and legal requirements. – Cross-reference with compliance |
| 3. Ability to maintain integrity of information in adherence to the organization’s policies and procedures including compliance with retention, archive, and destruction guidelines and requirements. – Cross reference with retention |
| 4. Ability to provide appropriate workforce training on information management and governance to support integrity of information. |
| 5. Ability to ensure trust of requestor in the integrity of information by ensuring the authenticity, timeliness, accuracy, completeness, and admissibility of records for all purposes including internal and external use, sharing, disclosure, exchange, release of information (ROI) and other purposes. Cross-reference with protection and availability |
| 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 organization via identification of original source of document creation, date of creation, and date of any changes of content of document or data within the document. - Cross-reference with protection and availability |
| 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. |
| 9. Ability to ensure that all output (viewable and printed) of the episode of care record   * 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 and * contains patient and record identifying data (i.e., patient and record demographics (document metadata)) as well as metadata and document identification data that need to be included in all documentation. – Availability is capture or just view??? VERIFY Req #/position; Check IHE XDW profile for their metadata to see it this is addressed |
| 10. 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. |
| 11. Ability to prove reliability and integrity of information through audit process to validate measures (e.g., controls, protocols, metrics, key performance indicators) for ensuring the reliability and integrity of information. |
| 12. Ability to manage the process of amending post-encounter data, document, and records by maintaining a visible history of the amendment itself, author, date, and time of the amendment. Once the encounter is complete, any change in data, document or the record is considered an amendment. |
| 13. 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. |
| 13. Ability to maintain formal change control processes as part of a reliable information environment, so as to differentiate any dynamic changes (e.g., change in the value of the data element, change in a template, document change, records change, change of interface, change of processes and other) through viewable display and printing capability. |
| 14. Ability to test HIS capabilities to support business requirements 1-13 including validation of data and all appropriate metadata. |
| 15. 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. |
| 16. Ability to establish parameters for “enable / disable” capabilities for “copy and paste” HIT function. |
| 17. 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 “copy and paste” function including the source, date, time, author of performing copy and paste. |
| 16. Ability to establish parameters for “enable / disable” capabilities for “pre-populate” HIT function |
| 17. 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 “pre-populate” function including the source, date, time, author of performing pre-populate. |

## 

**To Glossary:**

Term record includes episode of care and longitudinal record

Define - viewable display (e.g. in track changes or audit document) and a printed output (with and without changes)

Proof of integrity or conformity to integrity??? Availability means it is there. Integrity of viewing information

## 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 as well as (2) loss, tampering, and corruption of health information.”[[7]](#footnote-7) 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. |
| 10. Ability to audit that information is   * appropriately protected, accessed, stored, and released with a properly documented audit trail; Compliance * information is available when and where it is needed; Availability * information is retained for the right amount of time and properly dispositioned when no longer required (This is in ACOUNTABILITY AND RETENTION) |

## 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[[8]](#footnote-8). |

Specification 4: HIM Business Requirements: Health Information Accountability

|  |
| --- |
| **Health Information Accountability: Business Requirements** |
| 1. Ability to continuously document, approve, communicate and train 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 – define specifics in the checklist. |
| 3. Ability to conduct information governance practices with regular reporting to senior leadership on measurable outcomes defined by the program. |
| 4. Ability to ensure that senior leadership has the responsibility to oversee the information governance program and resources to support the program. |
| 5. Ability to ensure policies and procedures to guide organization’s workforce and agents in conducting the audit. |
| 6. Ability to continuously improve organization’s capability in demonstrating 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 when and where it is needed, information is retained for the right amount of time and properly dispositioned when no longer required (See also RETENTION and PROTECTION)HIM CHECKLIST |
| 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. (COMPLIANCE?)(HIM CHECKLIST?) |
|  |
| **Potential checklist items** |
| a. Ability to create and document organizational policies on health information management. |
| b. Ability to effectively make policies available to all staff with notifications mechanism of new or revised policies. |
| c. Ability to document and verify acceptance of senior leadership individuals to oversee the information governance program and resources to support the program. |
| d. Ability to document qualifications for those in the roles of executive sponsorship or authority. |
| e. Ability to document implementation and adoption plan. |
| f. Ability to create executive summary reports that will be delivered with designated frequency and to whom they are shared. |
| g. Ability to document IG program plan and requirements. |
| h. Ability to document creation, revision, review, and approval process for policies. |
| i. Ability to create and document process for training and retraining. |
| j. Ability to define and document stakeholders, business process owners, and domain experts by role. |
| k. Ability to facilitate policy feedback from end users, review feedback with identified committee, and respond. |
| l. Ability to calculate program benchmarks and progress toward goals. |
| m. Ability to make available program metrics and goals visible to all staff. |

## 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.[[9]](#footnote-9) Transparency assures that information is created appropriately and in compliance with the regulation and organizational policies. – cross harmonize with the compliance |

Specification 5: HIM Business Requirements: Health Information Transparency

|  |
| --- |
| **Health Information Transparency: Business Requirements** |
| 1. Ability to document in an open and verifiable manner organization’s processes and activities related to information governance. |
| 2. Ability to share 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. Compliance |
| 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 interested party in a timely manner - Availability |
| 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. Protection! Availability! |
| 7. Ability to create and manage the records documenting organization’s information governance program to ensure its structure, processes, and practices are apparent, understandable, and available as defined by organizational policies and jurisdictional laws (e.g., in time, appropriate requestors, etc.) |
| 8. Ability of organization to ensure stakeholders are made aware of how health information is created, acquired, collected, maintained, used, shared and disclosed. |
| 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[[10]](#endnote-1). Protection |

## Principle of Health Information Compliance: Business Requirements

|  |
| --- |
| Definition – Review again with the TF members |
| **Health** **Information Compliance** is the adherence to policies, procedures, bylaws, guidelines, laws, regulations, contractual agreements, and accreditation standards[[11]](#footnote-10). Compliance program is involved in prevention, detection, and resolution of instances of conduct that do not conform to federal, state, or the healthcare organization's ethical and business policies. |

|  |
| --- |
| **Sandra:**  **Health** **Information Compliance** is the adherence to documentation policies, procedures, bylaws, mandated guidelines, laws, regulations, contractual agreements, and accreditation standards[[12]](#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 prevention, detection and resolution of instances of conduct that do not conform to federal, state or the healthcare organization’s ethical and business policies.[[13]](#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. |
| 2. Ability to demonstrate that organization conducts its activities in a lawful manner and manages information risks effectively. |
| 3. Ability to show that the information management processes and systems contain information demonstrating the organization’s activities are conducted in an ethical and lawful manner. |
| 4. Ability for the organization to show that the information management systems themselves are subject to legal and regulatory requirements, such as vocabulary and terminology standards (e.g., clinical coding and classifications), security access controls, and transaction audit logs. |
| 5. 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. |
| 6. Ability to enter information into its records in a manner consistent with laws and regulations |
| 7. Ability to maintain its information in the manner and for the time prescribed by law or organizational policy. |
| 8. Ability to develop internal controls to monitor adherence to rules, regulations, and program requirements, thus assessing and ensuring compliance |

## Principle of Health Information Disposition: Business Requirements – Move After Retention

|  |
| --- |
| Definition |
| **Health Information Disposition** is defined as 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[[14]](#footnote-13). |

Specification 8: HIM Business Requirements: Health Information Disposition

|  |
| --- |
| **Health Information Disposition: Business Requirements** |
| 1. Ability to identify, segregate, and purge/destroy electronic records by various criteria and combinations of such criteria, including, but not limited to: day/month/year of discharge or encounter, encounter patient or service type, date of birth, diagnoses, procedures, facility location, physicians, and other variables. |
| 1. Ability to identify, segregate, and purge/destroy electronic records by criteria outlined in the retention schedules. Disposition “triggers” include day/month/year of discharge or encounter, day/month/year of report, date of patient birth, diagnoses, and other variables. - Retention |
| 2. Ability to retain a master list of all records by name, number, admit/discharge/encounter dates, and facility by date of destruction. |
| 2. Ability to retain a master list of all patients by name, number, admit/discharge/encounter dates, and facility by date of destruction. |
| 3. Ability to provide secure and appropriate disposition for information no longer required to be maintained by applicable laws and the organization’s policies. |
| 3. Ability to provide secure and appropriate disposition for information that reaches its retention period as required by applicable laws, an organization’s policies, and/or retention schedules. |
| 4. Ability to establish an authority to create and enforce a disposition policy and procedure that includes appropriate/compliant methods (provide examples for the checklist) of destruction and documentation of the destruction for each medium on which information is maintained. |
| 4. Ability to establish a process to authorize and enforce dispositions and a procedure that provides methods (provide examples for the checklist) of disposition. |
| 5. Ability to handle a permanent change in custodianship of the 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 a organization discontinues a practice, service, or other business. |
| 5. Ability to handle a permanent change in ownership and custody of information, when it is transferred to another party or organization due to a merger or acquisition, or or when a party or organization discontinues a practice, service, or other health care related business. |
| 6. Ability to certify the information is transported and destroyed in a secure manner and that the information has been destroyed completely and irreversibly when required. |
| 7. Ability to ensure that when information is converted or migrated to new media the disposition of the previous media may also be warranted according to the organizational policies. |
| 8. Ability to ensure all versions and copies of the information are accounted for in the disposition |
| 9. Ability to document organization’s disposition process. Ability to track and maintain documentation of disposition when it occurs. |
| 10. Ability to suspend the disposition in the event of pending or reasonably anticipated litigation or a regulatory action |
| 10. 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. |
| 11. Ability to designate information in consultation with counsel both as to scope and time to be held pending resolution of the litigation or audit and notify the affected workforce when a hold is issued as well as when the hold is released, so that the disposition process may be resumed |
| 11. Ability to lift destruction holds and to notify effected workforce , so that retention periods and disposition may resume. |

## Principle of Health Information Retention: Business Requirements – Move before Disposition

|  |
| --- |
| Definition |
| **Health Information Retention** is the mechanism for storing, maintaining and preserving information Retention policies and procedures provide for timely retrieval, and establish the lengths of time information will be retained by the healthcare organization.[[15]](#footnote-14) |

Specification 7: HIM Business Requirements: Health Information Retention

|  |
| --- |
| **Health Information Retention: Business Requirements** |
| 1. Ability to store, maintain (including retain), make accessible and disposition information throughout its lifecycle. |
| 2. Ability to accommodate information lifecycle management which is established by the retention policies and schedules, taking into account legal, clinical, regulatory, fiscal, operational and historical criteria for establishing retention period related to specific information. |
| 3. Ability to maintain and update retention schedules, which defines the information to be retained, how long it should be retained, and when disposition should occur. |
| ~~4. Ability to retrieve, access, and read information throughout its life cycle.~~  -Availability |
| ~~3. Ability to implement information lifecycle management including disposition~~. Integrity |
| 4. Ability to define what information to retain, how long to maintain it and how to dispose of it when it is no longer required. |
| 4. Ability to maintain an information retention schedule, which specifies what information must be retained and for what length of time. |
| 5. Ability to store, maintain and preserve health information. |
| 6. Ability to create and enforce a retention policy and procedure that addresses specificity of information stored on all types of media (paper, images, optical disk, microfilm, DVD, and CD-ROM); and the time period for which this information is kept.[[16]](#footnote-15) |
| 7. Ability to maintain 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 |
| 8. Ability to monitor compliance and vet retention regulations and standards |
| 9. Ability to ensure the availability of timely, relevant data and information for patient care purposes. |
| 10. Ability to 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. |
| 10. Ability to specify the storage medium on which information it will be maintained |
| 11. 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 (Copied from ACCOUNTABILITY, also in PROTECTION) |
| Ability to manage retention of information while complying with regulations and internal policies regarding disposition. Information should not be maintained beyond its useful live. - Availability |
| Ability to ensure archived information is managed in a structured manner supporting ease in access of accurate information in a cost effective manner regardless of storage medium.-Availability |

Notes to consider for retention:

HEALTH INFORMATION RETENTION (Specification #7)

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.

2. Information life cycelt begins when information is created and ends when information isdispositioned. The goal is for organizations to manage each step in information life cycle to ensure information accessibility and readability. Health information resides in multiple storage media and locations creating the need for information mapping. . 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.

3. 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.

CFRs

State laws and statutes

Professional organizations (e.g., CLIA)

4. State and Local Retention Requirements:

a. 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.

b. 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 on limitations; and,

\* Deceased patients. 5 years after death.

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.

State Record Retention Requirements may include:

\* Sexually transmitted diseases;

\* Child/Vulnerable Adult Abuse;

\* Communicable Diseases;

\*Radiation Exposure Monitoring (OSHA and State Counterpart);

\* Blood Bank/Transfusions;

\* Medical Staff/Nursing CME Records;

\* Professional Licensing/Credentialing Records;

\* Gunshot/Stab Wound Care.

5. Accreditation Record Retention Requirements: Joint Commission/NCQA, etc.

6. 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.

7. 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. 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> 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 InformationManagement Association (AHIMA). Spell out IGIQ.org - PROVIDE THE FULL REFERENCE [↑](#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). Pocket Glossary of Health Information Management and Technology. Chicago, IL. 2014. p.134 [↑](#footnote-ref-7)
8. 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-8)
9. American Health Information Management Association. "Information Governance Principles for Healthcare (IGPHC)TM." 2014 Chicago, IL. [↑](#footnote-ref-9)
10. American Health Information Management Association. "Information Governance Principles for Healthcare (IGPHC)TM." 2014 Chicago, IL. [↑](#endnote-ref-1)
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-10)
12. 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)
13. The Office of Inspector General Compliance Model [↑](#footnote-ref-12)
14. 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-13)
15. American Health Information Management Association. AHIMA Pocket Glossary of Health Information Management and Technology, 4th Edition. Chicago, IL, 2014. p.130 [↑](#footnote-ref-14)
16. Downing K, 2013 \_Provide full reference here [↑](#footnote-ref-15)