INFORMATION GOVERNANCE
Principles for Healthcare (IGPHC)™

INFORMATION GOVERNANCE Principles for Healthcare (IGPHC)™

©2014 by the American Health Information Management Association

PREAMBLE

Complete, current, and accurate *information* is essential for any organization in the healthcare industry to achieve its goals. Adoption of an information governance program underscores the organization's commitment to managing its information as a valued strategic asset. Governance of clinical and operational information:

- Improves quality of care and patient safety
- Improves population health
- Increases operational efficiency and effectiveness
- Reduces costs
- Reduces risk

Information governance helps manage and control information by supporting the organization's activities and ensuring compliance with its duties. Drawing from definitions of Gartner and ARMA International, AHIMA defines information governance as an organization-wide framework for managing information throughout its lifecycle and supporting the organization's strategy, operations, regulatory, legal, risk, and environmental requirements.

Information governance establishes policy, prioritizes investments, values and protects information assets, and determines accountabilities for managing information, making it an imperative for healthcare. It also promotes objectivity through robust, repeatable processes insulated from individual, organizational, political, or other biases, and then protects information with suitable controls. By following *information governance* principles, organizations conduct their operations effectively, while ensuring compliance with legal requirements and other duties and responsibilities.

Healthcare as a Unique Information Environment

Trust plays a critical role in healthcare delivery. Patients entrust their personal information to healthcare organizations, creating distinct requirements for confidentiality, privacy, and security. These organizations, regardless of their roles in healthcare, must earn the confidence of patients and society, through a firm commitment to ethical and responsible handling of personal information.

Embedded in trust is the expectation of information *integrity*, which depends on the completeness and correctness of data. Heightened focus on integrity to ensure confidence in information is demanded by the nature of healthcare, changes in care delivery and payment models, the increasing adoption of electronic systems, and the importance of reliable information exchange.

Healthcare organizations have an obligation to define uses of information and to define the policies and practices for governing use of the information. This includes protected health information, personally identifiable information, de-identified and anonymized information, aggregate and detailed information used to satisfy mandatory or voluntary reporting purposes, operational needs, secondary uses of data/information, and other uses based on the role and mission of the organization.

Research is fundamental to advancing the science of medicine. New guidelines, protocols, treatments, interventions and wellness insights, all developed through research, are essential to elevating population health. Research, whether focused on clinical care, delivery systems, or payment models, depends on trusted information.

> “Trust plays a critical role in healthcare delivery. Patients entrust their personal information to healthcare organizations, creating distinct requirements for confidentiality, privacy, and security. These organizations, regardless of their roles in healthcare, must earn the confidence of patients and society, through a firm commitment to ethical and responsible handling of personal information.”

Healthcare organizations must value and govern not only their clinical, but their nonclinical information, such as human resources, operational, financial, legal, and marketing information. Reliable information is essential to reducing healthcare delivery costs and improving operational efficiencies. For these reasons, establishing and implementing principles for the governance of clinical and nonclinical information, in all formats and on all media, increases in significance.

> “The adherence to information and technology standards across healthcare is compelled, as standards are crucial to information use and exchange given the imperatives of integrity, security and interoperability.”

The *healthcare ecosystem* consists of a variety of organizations and stakeholders, who share common goals. These organizations encompass healthcare *providers*, as well as *nonproviders*. Providers include all types and settings of healthcare service organizations. Nonproviders include organizations such as information exchanges, health plans, third party administrators, data clearinghouses, and other information intensive organizations. Indeed, an organization's entire *workforce*, including employed and contracted individuals, and where applicable all members of its nonemployed medical and professional staffs, are accountable for the responsible and ethical handling of information. The responsibility for practicing in accordance with organization's governance policies and procedures extends to outsourced services and their workforces, as well as to business partners and affiliates who use information or handle any aspect of information management for the organization.

Challenges facing the healthcare industry include:

- Expanding numbers of electronic systems/applications in use within and across organizations,
- Growing volume and variety of data and information,
- Expanding uses of healthcare information,
- Proliferation of medical devices creating data for which reliable integration into systems/applications is essential,
- State of interoperability across devices and systems, and
- Reliability of shared and exchanged information.

These challenges and complexities underscore the need for information governance, and the need for their due consideration in its adoption. The adherence to information and technology standards across healthcare is compelled, as standards are crucial to information use and exchange given the imperatives of integrity, security and *interoperability*.

- Despite the diversity in the healthcare industry, information across the various types of organizations can be governed using eight principles: accountability, transparency, integrity, protection, compliance, availability, retention, and disposition. These principles can be adopted in any organization within the healthcare industry.

Information Governance Principles for Healthcare

The principles of information governance, known as the *Information Governance Principles for Healthcare (IGPHC)*™, are comprehensive and written broadly. They do not set forth a legal rule for which strict adherence is required by every organization in every circumstance, but are intended to be interpreted and applied depending upon an organization's type, size, role, mission, sophistication, legal environment, and resources.

The *IGPHC*™ are based on practical experience, information theory, and legal doctrine within healthcare and further informed by other established practices and tenets from areas such as quality improvement, safety, risk management, compliance, data governance, information technology governance, privacy, and security. They are grounded in several common, yet essential, values embedded in healthcare—*accuracy, timeliness, accessibility*, and integrity. These values serve the best interests of the healthcare information consumer, from providers to nonproviders, from researchers to public health officials, from information exchanges to policymakers, from claims administrators to payers, and from patients to society.

AHIMA has convened healthcare industry stakeholders and leaders, as well as information governance experts from other industries to articulate the *IGPHC*™ through adaptation of ARMA International's Generally Accepted Recordkeeping Principles. Based on the general principles which apply to all industries, the *IGPHC*™ are specifically aimed at healthcare industry organizations. Therefore, the *IGPHC*™ apply not only to the governance of healthcare information, but also to the governance of information across all functions of organizations in the healthcare industry.

The adoption of these principles by an organization reflects a dedication to strengthen its information governance, and increase its effectiveness for the benefit of its patients, stakeholders, and society. These principles form the basis upon which every effective information governance program is built, measured, and eventually judged.

Therefore, it is in the best interest of patients, other consumers, society, and all organizations in the healthcare *ecosystem*, that there is full awareness of the *Information Governance Principles for Healthcare (IGPHC)*™ and that *information assets* be managed in accordance with them.

P PRINCIPLE OF ACCOUNTABILITY

An *accountable member of senior leadership*, or a person of comparable authority, shall oversee the information governance program and delegate program responsibility for information management to appropriate individuals.

The governing body of the organization is ultimately accountable for the adoption of information governance practices and should require regular reporting by the designated member of senior leadership. The organization should 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.

An information governance program should:

- Establish an information governance structure for program development and implementation
- Designate a qualified accountable person to develop and implement the program
- Document and approve policies and procedures to guide its implementation
- Remediate identified issues
- Enable auditing as a means of demonstrating the organization is meeting its obligations to both internal and external parties

A basic premise of sound information governance is that within each organization a senior leader is formally designated as responsible for the overall program development and its implementation. The senior leader is accountable for ensuring the information governance program aligns with and supports the goals and strategies of the organization. The senior leader is also accountable for ensuring appropriate resources are allocated to support the program.

Governance should be established throughout the organization, utilizing a collaborative approach, with input of stakeholders, business process owners, and domain experts, assigning defined roles and responsibilities to workforce members. It should be clear where responsibilities reside and how the chain of command builds, implements, and updates the information governance program. For example, sub-committees can be designated to help build policies, define and implement technology, or improve the information governance program.

> "Governance should be established throughout the organization, utilizing a collaborative approach, with input of stakeholders, business process owners and domain experts, assigning defined roles and responsibilities to workforce members."

To assist the workforce in understanding how to implement information governance practices, it is essential that policies and procedures are documented, formally approved, and communicated. The workforce should be continuously trained in program policies and any relevant updates to standardize information governance practices across the organization and to reinforce compliance with and standardization of practices.

A senior leader at an appropriate level of authority shall oversee program compliance monitoring/audit and improvement. Audits should be performed to determine the following:

- The workforce demonstrates program awareness
- The workforce is trained in information governance practices, policies, and responsibilities
- 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
- Policies are up-to-date, adopted, and cover all types of information in all media

An organization's information governance audit should be reported to its board of directors, trustees, audit committee, or other appropriate governing body, committee, or individual to show adherence in accordance with its program requirements and the organization's goals.

P PRINCIPLE OF TRANSPARENCY

An organization's processes and activities relating to information governance shall be documented in an open and verifiable manner. Documentation shall be available to the organization's workforce and other appropriate interested parties within any legal or regulatory limitations, and consistent with the organization's business needs.

> "The clearest and most durable evidence of the organization's operations, decisions, activities, and performance are its records and information."

Transparency of the organization's governance practices must extend to definitions of appropriate information uses and the processes for ensuring compliance with policies on appropriate information use.

The clearest and most durable evidence of the organization's operations, decisions, activities, and performance are its records and information. An information governance program includes its information management and information control policies and procedures. To ensure the confidence of interested parties, records documenting the information governance program must themselves adhere to the fundamentals of information management. These records should:

- Document the principles and processes that govern the program
- Accurately and completely record the activities undertaken to implement the program
- Be available to legitimately interested parties in a timely and reasonable manner

The information documented in these records and the extent to which they are available to interested parties will vary depending upon the nature and circumstances of the organization. For example, healthcare organizations have a legitimate need to protect confidential and proprietary information. Therefore, procedures shall be put in place to control access to protected information, whether it relates to the confidentiality of information or the confidentiality of proprietary processes.

Various parties have a legitimate interest in understanding the information governance program activities and processes. In addition to the organization itself and its workforce, those parties include, but are not limited to, patients and consumers, government authorities, auditors and investigators, litigants, and for some organizations, the general public.

Complex and highly regulated records and information management systems may require extensive records documenting their governance. Simple systems may require only a few. In each case, however, the rationale and results should be clear to legitimately interested parties.

Each organization must therefore create and manage the records documenting its information governance program to ensure its structure, processes, and practices are apparent, understandable, and reasonably available to legitimately interested parties.

PRINCIPLE OF INTEGRITY

An information governance program shall be constructed so the information generated by, managed for, and provided to the organization has a reasonable and suitable guarantee of authenticity and reliability.

Integrity of information, which is expected by patients, consumers, stakeholders, and other interested parties such as investors and regulatory agencies, is directly related to the organization's ability to prove that information is *authentic, timely, accurate, and complete*. For the healthcare industry, these dimensions of integrity are essential to ensuring trust in information.

For safety, quality of care, and compliance with applicable voluntary, regulatory and legal requirements, integrity of information should include at least the following considerations:

- Adherence to the organization's policies and procedures
- Appropriate workforce training on information management and governance
- Reliability of information
- Admissibility of records for litigation purposes
- Acceptable audit trails
- Reliability of systems that control information

> "Information governance incorporates the *governance of data*. As data are the building blocks of information, information cannot be reliable if the data are not reliable."

Information from External Sources

It is critical that organizations determine their responsibilities and processes for classifying and managing information received from other sources.

A healthcare organization's information may contain patient or other business information that originated from another healthcare organization. For example, copies of selected patient reports are often sent by one healthcare provider to another where a patient is admitted. Information received from the previous provider is then incorporated into the patient's health record at the receiving organization. Organizations must comply with re-disclosure responsibilities under all relevant laws.

Information Governance Policies and Procedures

Adherence to information governance policies and procedures that have been approved by senior management is essential to an organization's ability to achieve legal and regulatory compliance, as well as consistently carrying out information governance practices. If adherence to policies and procedures is not substantiated, records may be at risk of not being accepted as having evidentiary value.

Appropriate Training on Information Management and Governance

The organization shall provide training to all workforce members, and outsourced or contracted individuals when appropriate, on the meaning and importance of compliance with its policies and procedures.

> “*Integrity* of information, which is expected by patients, consumers, stakeholders and other interested parties such as investors, and regulatory agencies, is directly related to the organization’s ability to prove that information is *authentic, timely, accurate, and complete.*”

Reliability of Information

Organizations should define and apply consistent information governance practices throughout the information lifecycle. This helps ensure information is managed in the usual and ordinary course of business, and in a manner which ensures integrity and compliance with accepted industry standards for quality. Given the variety, complexity, and risks associated with information assets, the lifecycle practices should incorporate a means of classifying and valuing information.

Reliability of information is of paramount importance in the delivery of healthcare services. Based on the nature and type of healthcare organization, measures to ensure reliability of data and information should be built in to processes and systems for creation and capture, processing, and other applicable stages of the information’s lifecycle. Such measures will promote quality of care, patient safety, and operational efficiency. Examples of such ongoing measures include field-specific data edits built into systems/applications; monitoring and correction of vendor identity errors and patient identity errors; monitoring and correction of documentation completeness and data accuracy; and ongoing data quality controls.

Information governance incorporates the *governance of data*. As data are the building blocks of information, information cannot be reliable if the data are not reliable. Data and information are inextricably linked, and the goals of information governance will not be achieved if practices do not ensure trustworthy data. In the governance of data, the organization should define expected *attributes of data quality*, and the practices and responsibilities for achieving those attributes.

Acceptable Audit Trails

Audit trails are essential in proving reliability of the information and in proving that practices to achieve quality attributes are in place. Therefore, acceptable audit and quality assurance processes should be in place and verifiable. These should be designed to audit and reinforce measures for ensuring the reliability and integrity of information.

Reliability of the Systems

The information systems must be reliable to ensure validity and integrity of the content. Therefore hardware, network infrastructure, software, storage, and other components should be monitored for reliability of performance, and prompt action taken to mitigate identified problems and risks. Formal *change control* processes should be part of maintaining a reliable information environment. These change control processes should require testing of functionality, and validation of data and all appropriate metadata. Given the number of disparate systems, applications, and medical devices in use within and across healthcare delivery organization, and the frequency with which data and information are exchanged, diligence around adherence to interoperability standards is critical to enabling information reliability.

P PRINCIPLE OF PROTECTION

An information governance program must ensure the appropriate levels of protection from breach, corruption and loss are provided for information that is private, confidential, secret, classified, essential to business continuity, or otherwise requires protection.

> “Every system, electronic or manual, that generates, collects, stores, transmits, uses, archives, and dispositions data and information must be governed with protection in mind.”

These levels of protection must be applied to information, regardless of medium, from the moment it is created to the moment it reaches or exceeds its retention period and is appropriately dispositioned. Therefore, every system, electronic or manual, that generates, collects, stores, transmits, uses, archives, and dispositions data and information must be governed with protection in mind.

Information generated or managed by an organization requires varying degrees of protection, as mandated by laws, regulations, and/or organizational policies. An organization's governance should also mandate processes to ensure continued operation and continued protection, during and after periods of failure or disruption.

Information protection takes multiple forms. First, each system must enable management of security access controls. Only members of the workforce and other authorized parties with the appropriate levels of access or security clearance may access information relevant to their roles or duties. Reliably protecting electronic and physical assets requires use of tools such as user authentication, key card access restrictions, and other relevant measures. This also requires that as the workforce and other authorized parties transition in status or job function, respective level of access is changed immediately to a level appropriate to the new role and duties.

Second, protection requires preventing information, regardless of medium, from leaking outside the organization, either by physical or electronic means. This includes ensuring that electronic information cannot be inappropriately viewed, e-mailed, downloaded, uploaded, or otherwise proliferated—intentionally or inadvertently, even by individuals with legitimate access to the system. For example, a managed file transfer technology can reduce workforce contact with protected health information (PHI), personally identifiable information (PII) or other protected information, using automated file transfers. It is imperative that appropriate safeguards be clearly defined in organizational policy and that compliance be monitored. Measures to protect information must also include physical security of computing and access devices or any equipment containing private, secret, or confidential information or intellectual property of the organization.

Security, privacy and confidentiality requirements (rules, regulations, policies) should be observed when determining a method for the final disposition of information, regardless of source or media. Whether that disposition is archival, transfer to another organization, preservation for permanent storage, or destruction, appropriate protection must be considered in defining the process. For example, the workforce should:

- Implement reasonable safeguards to limit incidental disclosures of PHI and PII
- Receive training on disposal policies and procedures
- Not abandon or dispose of information, particularly PHI or PII or other private information in containers that are accessible by the public or other unauthorized persons
- Provide validation of disposal method, time, date, and accountable party

Finally, an organization's audit program should have a clear process to validate whether sensitive information is being handled in accordance with the organization's policies and procedures, and should be compliant with applicable laws and business practices.

PRINCIPLE OF COMPLIANCE

An information governance program shall be constructed to comply with applicable laws, regulations, standards, and organizational policies.

It is the duty of every organization to comply with applicable legal and regulatory requirements; those for maintaining and managing health information and those for managing other organizational information. Some healthcare requirements warrant special attention and consideration. For example, laws governing privacy and confidentiality, and fraud and abuse are particularly important to healthcare organizations. An organization's credibility and legal standing rest upon its ability to demonstrate that it conducts its activities in a lawful manner and manages information risks effectively. The absence of information, or poor quality of information required to demonstrate this damages an organization's credibility and may impair its standing in legal matters or jeopardize its ability to conduct business.

The duty of compliance affects systems and processes for information management and governance in two ways:

1. The information management systems and processes should contain information showing the organization's activities are conducted in an ethical and lawful manner.
2. The information management systems themselves are subject to legal and regulatory requirements, such as medical coding standards, security access controls, and transaction audit logs.

It follows from this that every organization should:

- Know what information should be entered into its records to demonstrate its activities are being conducted in a lawful manner.
- Enter that information into its records in a manner consistent with laws and regulations.
- Maintain its information in the manner and for the time prescribed by law or organizational policy.
- Develop internal controls to monitor adherence to rules, regulations, and program requirements, thus assessing and ensuring compliance.

> "An organization's credibility and legal standing rest upon its ability to demonstrate that it conducts its activities in a lawful manner and manages information risks effectively."

Organizations subject to codes of conduct, ethics rules, standards of practice, or other authorities are also subject to a duty to comply with them. To the extent that information management systems are required to demonstrate compliance, the organization's information must be maintained in accordance with these codes, rules, or authorities.

Policies are internal rules of conduct for the organization and the organization's own statement of what it deems as correct conduct. By its nature, a policy imposes a duty of compliance upon the organization and its workforce. To comply with legal and regulatory requirements, an organization should develop, adopt, monitor, and enforce suitable policies.

The precise manner and duties of compliance will vary among different types of healthcare organizations. Some organizations may be subject to multiple laws and regulatory requirements, as well as codes of ethics and accreditation standards. It may, in turn, require the organization to adopt, integrate, and enforce multiple policies for information governance.

Every organization should construct and enforce its policies and conduct its activities in an appropriate manner to ensure compliance with the totality of authorities applicable to it.

P PRINCIPLE OF AVAILABILITY

An organization shall maintain information in a manner that ensures *timely, accurate, and efficient* retrieval.

Stakeholder trust in information and in the healthcare operations themselves is impacted by an organization's ability to ensure the timely, accurate, and efficiency of information availability.

A successful and responsible organization must have the ability to identify, locate, and retrieve the information required to support its ongoing activities. This information may be used by:

- The healthcare team, patients, and other caregivers
- Authorized members of the workforce and others authorized consistent with regulations
- Legal and compliance authorities for discovery and regulatory review purposes
- Internal and external reviewers for purposes including but not limited to: payer *audit*, financial audit, case management, and quality assurance.

Having the right information available at the right time for the right individual depends upon an organization's ability to address multiple demands. The organization must search for information in continually expanding volumes of information and multiple systems. For some organizations this includes multiple electronic and manual systems. Transactions are increasingly conducted across disparate electronic systems, both internal and external to the actual or virtual location(s) of the organization, complicating queries and access to data across those systems. Managing both vendor relationships and employee turnover can also challenge organizations to update their workforce and agents on the most current methods to access information.

To ensure critical information availability, organizations must determine levels of redundancy, failover, and contingencies needed based on risk of nonavailability of electronic systems and information.

Metadata

Efficient information availability, effective preservation and disposition, and effective database administration require assigning structural and descriptive characteristics to information. Metadata should be utilized in all applicable systems to facilitate information availability. *Metadata* are the structured information that describe, explain, locate, or otherwise make it easier to retrieve, use, audit, and manage information. Metadata consist of indexing terms and attributes; metadata are data about data. Metadata are typically categorized into groups including but not limited to: administrative, content, descriptive, preservation, and structural. For example, dates of creation, sending, receipt, last access, and last modified are examples of administrative metadata.

Backups, Conversion, Migration

To mitigate the effects of a disaster, system malfunction, or data corruption, information should be backed up routinely. Information created with legacy hardware and software systems should also be reviewed periodically to verify the information can be accessed with current systems. In case of impending system obsolescence, information with organizational value should be migrated to currently supported hardware and/or converted into a readable format.

> "Efficient information availability, effective preservation and disposition, and effective database administration require assigning structural and descriptive characteristics to information. Metadata should be utilized in all applicable systems to facilitate information availability."

Routine Disposition

To effectively manage the availability of its information assets at a reasonable cost, an organization should—in the normal course of business—regularly remove obsolete or redundant data and information. This will make the remaining information, which has ongoing value to the organization, more identifiable and accessible, enhance system performance, and reduce the maintenance costs of storage, backup, and migration.

> “Having the right information available at the right time for the right individual depends upon an organization’s ability to address multiple demands.”

However, removing unneeded information should occur in adherence with the organization’s information retention policies, which should also provide for suspending its disposition in the event of pending or ongoing legal process, audit, or, where appropriate, freedom of information requests.

Well-Designed Storage

An organization’s workforce is more likely to retrieve and use information for better decision making and more effective work if the organization has well-designed storage processes and access to understandable, retrievable, relevant, and consistent information. With properly structured information, personal productivity is improved, storage costs are minimized, and the reliability and speed of retrieval are optimized.

Accessibility through sufficient and readily available access points or devices is applicable to all types of stored information, including, but not limited to, clinical and nonclinical information regardless of storage medium.

Further, complete and accessible records and information in a well-managed environment minimize inconsistent and erroneous interpretation of the facts, simplify legal processes and regulatory investigations, and protect valuable information from being lost, corrupted, or stolen.

P PRINCIPLE OF RETENTION

An organization shall maintain its information for an appropriate time, taking into account its legal, regulatory, fiscal, operational, risk, and historical requirements.

Information documents an organization’s operations and is essential to effectively managing the organization. The ability to properly and consistently retain all relevant information is especially important, as organizations create and store large quantities—most of it in electronic form.

The ability to retrieve and access information should be maintained throughout its retention period. Accessibility through currently and readily available access points or devices is applicable to all types of stored information, including, but not limited to, clinical and nonclinical information regardless of storage medium.

To control information volume, an organization needs an information retention program that defines what information to retain, how long to maintain it and how to dispose of it when it is no longer required. This is based on the concept that information has a *lifecycle*, which begins at its creation and ends at its final disposition.

As part of its retention program, an organization must develop an information *retention schedule*, which specifies what information must be retained and for what length of time. Retention decisions are based on the type of information, and the organization’s legal, regulatory, fiscal, operational, clinical, role/mission, and historical requirements.

- **Legal and Regulatory**—Local, national, and international laws mandate the retention of information for a specified period of time—generally a minimum period—but may include a maximum period as well. To comply with these laws and regulations, an organization should conduct research in consultation with appropriate experts such as legal counsel to determine all retention requirements. Failure to comply may result in costly penalties and loss of legal rights.

- **Fiscal**—Information with financial or tax value should be retained to ensure the timely payment of obligations and the proper receipt of receivables, as well as to support the organization's financial audits and tax returns. Information related to the filing and support of governmental or payer reporting requirements should also be retained. In conjunction with legal counsel, workforce responsible for fiscal compliance should help determine fiscal retention requirements.
- **Operational**—An organization should determine how long information is needed to satisfy its operational needs. This is usually determined by interviewing the individuals most knowledgeable about the operational value of each information type.
- **Clinical**—As applicable, and based on the nature of care and/services services provided and its role, an organization should determine and how long information in the aggregate and by information type should be retained to satisfy clinical needs.
- **Role/Mission**—Based on the organization's role and/or mission in the healthcare industry, retention periods for all or specific types of information may be established outside time periods otherwise required. An example of such need is organizations conducting or participating in research.
- **Historical**—Information that depicts the history of an organization should be preserved and properly archived for the life of that organization. Examples of historical information include articles of incorporation, bylaws, charters, and boards of directors' minutes. Examples of historical clinical information include medical staff bylaws and minutes. Historical information normally constitutes a very small percentage of an organization's total retained information volume.

Information retention schedules should be reviewed periodically and revised regularly. Some internal changes in the organization such as mergers and acquisitions or lines of business changes, or types of records generated, as well as external events such as legal, regulatory, or fiscal changes, may require revisions. If a revision decreases a retention period for a particular records series, then that records series should be destroyed as soon as possible to comply with the revised information retention schedules.

Once the retention requirements listed above are determined, an organization should conduct a risk assessment to determine the appropriate retention period for each type of information. Retention decision makers should be aware the presence or absence of information can be either helpful or harmful to the organization. Therefore, to minimize risks and costs associated with retention, it is essential to immediately dispose of information after the retention period expires, in accordance with the organization's retention policy.

> "To control information volume, an organization needs an information retention program that defines what information to retain, how long to maintain it and how to dispose of it when it is no longer required. This is based on the concept that information has a *lifecycle*, which begins at its creation and ends at its final disposition."

PRINCIPLE OF DISPOSITION

An organization shall provide secure and appropriate disposition for information no longer required to be maintained by applicable laws and the organization's policies.

At the completion of its retention period, an organization's information must be designated for disposition. This applies not only to patient health records and data, but many other types of information such as meeting minutes, credentialing files, agreements, financial records, human resource information, and privileged information such as that related to quality assurance.

Disposition includes not only destruction, but also any 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.

In many cases, the appropriate disposition is the destruction of information, in which case the organization should ensure the information is transported and destroyed in a secure and environmentally responsible manner. The organization should document or certify that the information has been destroyed completely and irreversibly when required.

In some cases, healthcare organizations discontinuing their business may choose to transfer records of care to the patients or clients to whom they pertain. All such transfers are considered permanent disposition actions and should be documented.

If records and information are converted or migrated to new media, disposition of the previous media may also be warranted. In all instances, the organization should make a reasonable effort to ensure all versions and copies of the information are accounted for in the disposition. The organization should also document its disposition process.

A duty to suspend disposition may arise in the event of pending or reasonably anticipated litigation or a regulatory action. The organization should 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.

> "Disposition includes not only destruction, but also any 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."

IGPHC™ GLOSSARY OF SELECTED TERMS

The following terms appear in the IGPHC™ or are closely related to such terms. This set of definitions is not intended to be an exhaustive set of IG related terms and should be used in conjunction with relevant glossaries including AHIMA's Pocket Glossary of Health Information Management and Technology.

Definition sources are referenced as follows:

AHIMA—Pocket Glossary of Health Information Management and Technology

ARMA—Glossary of Records and Information Management Terms

M-W—Merriam-Webster Online Dictionary and Thesaurus

Task Force—definition developed by AHIMA IG Task Force

Accessibility: easily obtainable and legal to access with strong protections and controls built into the process (AHIMA)

Accountable Member of Senior Leadership: (examples include) CEO, C-Suite, President, Agency Director, Practice Partner, Administrator, Executive Director, Owner/Operator—(Task Force)

Accuracy: the extent to which the data are free of identifiable errors (AHIMA)

Audit, Auditing: the review of information-related activities to ensure that sufficient policies, procedures, and controls are in place and complied with to meet all operational, legal, and regulatory obligations and to identify where and how improvements should be made (ARMA)

Audit Trail: a record that allows a sequence of activities to be reconstructed, reviewed, and examined. (M-W). 1. A chronological set of computerized records that provides evidence of information system activity (log-ins, log-outs, file accesses) used to determine security violations. 2. A record that shows who has accessed a computer system, when it was accessed, and what operations were performed (AHIMA)

Authentic, Authenticity: the genuineness of a record, that it is what it purports to be; information is authentic if proven to be immune from tampering and corruption (AHIMA)

Availability: extent to which information is available, whenever and wherever it is needed (AHIMA). Definitions contextual to the Availability Principle: **(1)Timely:** (context of Availability) having the requested information available for the requestor before that requestor needs to make a decision for the next step in their workflow without an unreasonable wait (Task Force) **(2) Accurate:** verifying that the information retrieved matches the request for the correct item or person at the correct level of detail (Task Force) **(3) Efficient:** the sum of the organization's decisions to balance three competing imperatives: accuracy of the information retrieved, verifying that the requestor has rights to the information, and the speed in which the information is delivered to the requestor (Task Force)

Change Control: expected standard practice to ensure that changes software, hardware, firmware, or other components to technical infrastructure are introduced in a predefined, controlled manner. The practice should include testing of applicable aspects, including the impact or data and metadata integrity. Effective change control practices will minimize disruption and the need to fall-back on planned changes (Task Force)

Complete, Completeness: an element of a legally defensible health record. A (health, medical) record is not complete until all its parts are assembled and appropriate documents are authenticated according to medical staff bylaws. (AHIMA) Records and information comply with internal or external defined requirements for comprehensiveness, including clinical, business, and other operational needs (Task Force)

Data: basic facts and observations about people, processes, measurements, and conditions (e.g. dates, numbers, images, symbols, letters) (AHIMA)

Data Governance: the overall management of the availability, usability, integrity, and security of the data employed in an organization or enterprise (AHIMA)

Data Quality Attributes, Characteristics: accessibility, accuracy, comprehensiveness, consistency, currency, definition, granularity, precision, relevancy, timeliness. AHIMA includes Data Quality Characteristics in its "Data Quality Management Model (Updated)" available through the AHIMA Body of Knowledge (BOK). Data quality attributes includes but are not limited to:

- **Data Accuracy:** The extent to which the data are free of identifiable errors
- **Data Accessibility:** Data items that are easily obtainable and legal to access with strong protections and controls built into the process
- **Data Comprehensiveness:** All required data items are included—ensures that the entire scope of the data is collected with intentional limitations documented
- **Data Consistency:** The extent to which the healthcare data are reliable and the same across applications
- **Data Currency:** The extent to which data are up-to-date; a datum value is up-to-date if it is current for a specific point in time, and it is outdated if it was current at a preceding time but incorrect at a later time
- **Data Definition:** The specific meaning of a healthcare-related data element
- **Data Granularity:** The level of detail at which the attributes and values of healthcare data are defined
- **Data Precision:** Data values should be strictly stated to support the purpose
- **Data Relevancy:** The extent to which healthcare-related data are useful for the purposes for which they were collected
- **Data Timeliness:** Concept of data quality that involves whether the data are up-to-date and available within the expected time frame; timeliness is determined by manner and context in which the data are being used (AHIMA)

Ecosystem: everything that exists in a particular environment (M-W)

Healthcare Ecosystem: used in AHIMA's IGPHC ™ to reference the community of organizations, both healthcare provider and nonprovider, of all types, sizes, and settings, that are information intensive. Also referred to as in the IGPHC™ as healthcare industry and healthcare community (Task Force)

IGHPC™: the Information Governance Principles for Healthcare™. A set of governance principles adapted for use in provider and nonprovider organizations in the healthcare industry from ARMA International's Generally Accepted Recordkeeping Principles®. The IGPHC™ developed with multi-stakeholder and multi-discipline representation are the cornerstone of the AHIMA promulgated framework for the adoption and practice of information governance in healthcare. (Task Force)

Information Governance—AHIMA: an organization-wide framework for managing information throughout its lifecycle and supporting the organization's strategy, operations, regulatory, legal, risk, and environmental requirements

Information Governance—ARMA: a strategic framework composed of standards, processes, roles, and metrics that hold organizations and individuals accountable to create, organize, secure, maintain, use and dispose of information in ways that align with and contribute to the organization's goals

Information Governance—Gartner: the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving, and deletion of information

Information: data that have been collected, combined, analyzed, and/or interpreted to be used for a specific purpose or set of purposes. Data represent facts; information represents meaning (AHIMA)

Information Assets: information that has value for the organization. (AHIMA) The recognition that information must be recognized as a strategic asset by the organization is central to information governance principles (Task Force)

Information Lifecycle: the cycle of gathering, recording, processing, storing, sharing, transmitting, retrieving, and disposing of information (AHIMA)

Information Management: the generation, collection, organization, validation, analysis, storage, and integration of data as well as the dissemination, communication, presentation, utilization, transmission, and safeguarding of the information (AHIMA)

Interoperability: the ability of different systems to use and exchange information through a shared format (ARMA)

Integrity: 1. the state of being whole or unimpaired. 2. the ability of data to maintain its structure and attributes, including protection against modification or corruption during transmission, storage, or at rest. Maintenance of data integrity is a key aspect of data quality management and security. (AHIMA) *Integrity* of information is directly related to the organization's ability to prove that information is *authentic, timely, accurate, and complete*. (Task Force)

Metadata: descriptive data that characterize other data to create a clearer understanding of meaning, and to achieve greater reliability and quality of information. Metadata consist of indexing terms and attributes. Data about data. For example, dates of creation, sending, receipt, last access, last modified. (AHIMA). The structured information that describe, explain, locate, or otherwise make it easier to retrieve, use, or manage information resources. **Note:** Metadata are typically broken into broad types that include but are not limited to: administrative, content, descriptive, preservation, and structural. (ARMA)

Program: a plan of action to achieve a specified end (M-W)

Provider (of healthcare): physician, clinic, hospital, nursing home, or other healthcare entity that delivers healthcare services (AHIMA). Nonprovider: in context of the IGPHC™, means organizations within and service provider organizations or consumers that do not provide direct medical or healthcare services (Task Force)

Record: any recorded information, regardless of medium or characteristics, made or received and retained by an organization in pursuance of legal obligations or in the transaction of business (ARMA)

- **Health Record:** information related to the physical or mental health or condition of an individual as made by or on behalf of a health professional in connection with the care ascribed that individual (AHIMA)
- **Legal Health Record:** documents and data elements that a healthcare provider may include in response to legally permissible requests for patient information (AHIMA)
- **Business Record:** a record that is made and kept in the usual course of business, at or near the time of the event recorded (AHIMA)

Reliability: (of information) information is managed in the usual and ordinary course of business, and in a manner which ensures integrity and compliance with accepted industry standards for quality (Task Force)

Retention: Mechanisms for storing records, providing for timely retrieval, and establishing the lengths of time that various records (and/or) information (sets) will be retained by the healthcare organization (AHIMA)

Retention Schedule: a time line for various records/information retention based on factors such as laws, statutes of limitation, age of patient, competency of patient, standards, AHIMA recommendations, operational needs, and role and mission of the organization (AHIMA, Taskforce)

Timely, Timeliness: the time between an event and the availability of data and/or information about the event. The completion of a business or health record within timelines established by external or internal requirements, medical and/or professional staff bylaws, or organization policy (Task Force)

Transparency: transparency of use of health information: open and transparent definition of uses and sharing of identified and de-identified, individual, or aggregate healthcare information (Task Force)

Workforce: human resources, employed, contracted, and where applicable, nonemployed members of medical and professional staff granted practice privileges. All members of the workforce of the healthcare organization are accountable for their responsible and ethical handling of information (Task Force)

Bibliography

American Health Information Management Association. *Pocket Glossary of Health Information Management and Technology*, 4th Edition. Chicago, IL AHIMA Press, 2014.

ARMA International. *Glossary of Records and Information Management Terms*, 4th Edition. Overland Park, KS. ARMA International. 2012

ARMA International. "Generally Accepted Recordkeeping Principles®." 2013 Overland Park, KS ARMA International. 2013

M-W–Merriam-Webster On-Line Dictionary and Thesaurus http://www.merriam-webster.com/ (terms searched 2014)

Suggested Reading:

Cohasset Associates and AHIMA. "A Call to Adopt Information Governance Practices." 2014 *Information Governance in Healthcare*. Minneapolis, MN. Cohasset Associates, 2014.

The Joint Commission. "Information Management (IM) Chapter", *Comprehensive Accreditation Manual for Hospitals*, 2014, Oakbrook Terrace, IL: The Joint Commission, 2014, pp.IM-1–IM-10.

The Information Governance Initiative. "The Information Governance Initiative Annual Report." 2014. New York, NY. www.IGinitiative.com

The Sedona Conference. "Commentary on Information Governance" The Sedona Conference® Working Group Series. A project of The Sedona Conference® Working Group on Electronic Document Retention and Production (WGI)

ACKNOWLEDGEMENTS

AHIMA acknowledges the following individuals and organizations for their valued contributions to the AHIMA Information Governance Principles for Healthcare (IGPHC)™.

Information Governance Taskforce

Deborah Bass, Chief Executive Director, Nebraska Health Information Exchange, AHIMA Practice Council Member on HIEs

Brent Bigelow, CISSP, Senior Security Architect, Cardinal Health

Galina Datskovsky, PhD, IGP-CRM, CRM, Consultant and Facilitator, CEO Covertix North America, VP Information Governance, HP Autonomy, Past President ARMA International

Sofia Empel, PhD, MLIS, **CRM, CDIA+**—InfoCentric Strategies

Deborah K. Green, MBA, RHIA, AHIMA. Executive Vice President and Chief Operating Officer, AHIMA EVP/COO, AHIMA National Visionary Award, 2000

Anupam Goel, MD, MBA, VP Clinical Information Advocate (ACO) UCSD, Beacon Communities, Malcolm Baldridge Examiner, Boarded in Informatics

Lee Hamilton, JD, MBA, RN, CPHQ, FNAHQ, PCMH CCE, International Executive and Consultant in Health Leadership, Policy and Quality/Risk. Past President of NAHQ

Melissa Martin, RHIA, CCS, CHTS-IM, Chief Privacy Officer and HIM Director at West Virginia University Hospitals, AHIMA Board, Third Year Director. Past President and Distinguished Member of WVHIMA

Gretchen Tegethoff, MS, CHCIO, CPHIMS, FHIMSS, FCHIME, CIO and CHIME Representative, CIO George Washington University, Athens Regional Health System

Mary G. Reeves, RHIA, Past AHIMA Chair EHRs Practice Council, Past Director AHIMA Board, AVP HIM Ops and CDI Regional HealthCare Partners. Former Admin HIM Director Vanderbilt

Lydia M. Washington, MPH, RHIA, CPHIMS, AHIMA Senior Director HIMPE, Former HIM Director MD Anderson

Sandra Wolfskill, CPA, FHFMA, HFMA, Director Revenue Cycle MAP

IG Expert Advisory Group

Bennett Borden, JD, Partner Commercial Litigation Practice Group-Co Chair IG and eDiscovery Group at Drinker Biddle and Reath, Sedona Conference, ARMA, Co-Founder IG Initiative, globally recognized authority on the legal, technology, and policy implications of digital information

Dee Cantrell, MS, RN, BSN, CP, Chief Information Officer, Emory Healthcare Associate Director for Enterprise Clinical Informatics for Emory's Center for Clinical Informatics and the Deputy CIO for the Office of Information Technology for Emory University

Todd Cooper, EVP, Center for Medical Interoperability, Principle Breakthrough Technologies Foundry, Chairman US Technical Advisory Group to ISO TC 215, Head of US Delegation ISO TC 215-Informatics, Board IHE, Co-Chair HL7 Medical Device, Chair IEEE

Ron Hale, PhD, CISM, Acting CEO and Chief Knowledge Officer for ISACA, Former Practice Director Enterprise Risk Management Division, Deloitte & Touche

Ronald J. Hedges, JD, Former US Magistrate Judge, Adjunct Professor Georgetown Law, eDiscovery Expert, Author, Sedona Conference, ARMA

Pamela Lane, MS, RHIA, CPHIMS, CA. DHHS, Deputy Section Health Information, Director Office of Health Information Integrity, Consulting and Hospital Ops Experience, US Navy Veteran

John Mache, **MS**, Chief Information Officer and Enterprise Security Officer, The Joint Commission

Fred Pulzello, MBA, CRM, IGP, President ARMA International

Don Rosen, MS, Director Policy and Enforcement, Officer of the Chief Records Officer, National Archives and Records Administration (NARA)

Sunil Sinha, MD, MBA, FACHE, FACP, Boarded: ABIM, ACPE, ABQUAR, Senior Malcolm Baldridge Examiner, Juror NQF National Quality Award, Johns Hopkins, Former Sr. Medical Officer CMS, Pfizer, Jencare Market Medical Director—Virginia

Rita Vann, RN, SVP Clinical Services Brookdale Senior Living, Long Term Care Nurse Executive Council

Charlotte Weaver, PhD, RN, Chief Clinical Officer and SVP Clinical Services Gentiva, VP & ED Nursing Research-Cerner, AMIA-Nursing Informatics Pioneer

Paul Wester, MA, MLS, Chief Records Officer, US Government National Archives and Records Administration (NARA)

AHIMA-Appointed IG Review Group

Kimberly A. Baldwin-Stried Reich, MBA, MJ, RHIA, PBCI, CPHQ, FAHIMA

Ellen Berkowitz, RHIT, CHDA, CPHQ

Patty Buttner, RHIA, CCS

Jill S. Clark, MBA, RHIA, CHDA, FAHIMA

Angie Comfort, RHIA, CDIP, CCS

Julie A. Dooling, RHIA, CHDA

Elizabeth A. Dunagan, RHIA

Melanie Endicott, MBA/HCM, RHIA, CDIP, CCS, CCS-P, FAHIMA

Louis Galterio, MBA, CHIME, CP, FHIMSS

Barb Glondys, RHIA

Pamela Heller, RHIA, CCS-P

Sandra A. Huyck, RHIT, CCS-P, CPC/H

Beth H. Just, MBA, RHIA, FAHIMA

Lesley R. Kadlec, MA, RHIA

Elisa Stamm Kogan, MS, MHA, CDIP, CCS-P

Susan Lucci, RHIA, CHPS, CHDS, AHDI-F

Katherine G. Lusk, MHSM, RHIA

Ann M. Meehan, RHIA

Deborah L. Neville, RHIA, CCS-P, PCS

Alice Noblin, PhD, RHIA, CCS

Brenda S. Olson, MEd, RHIA, CHP

Anna Orlova, PhD

Erik Pupo, MBA, CPHIMS, FHIMSS

Harry Rhodes, MBA, RHIA, CHPS, CDIP, CPHIMS, FAHIMA

Lisa A. Roat, RHIT, CCS, CCDS

Angela Rose, MHA, RHIA, CHPS, FAHIMA

Sharon K. Slivochka, RHIA

Patrice L. Spath, MA, RHIT, CHTS-IM

Diana Warner, MS, RHIA, CHPS, FAHIMA

Susan White, PhD, RHIA, CHDA

Lou Ann Wiedemann, MS, RHIA, CDIP, CHDA, CPEHR, FAHIMA

AHIMA Board of Directors 2014

Angela Kennedy, EdD, MBA, RHIA, President/Chair

Ann Chenoweth, MBA, RHIA

Cassi Birnbaum, MS, RHIA, CPHQ, FAHIMA, President/Chair-elect

Cindy Zak, MS, RHIA, PMP, FAHIMA

Colleen A. Goethals, MS, RHIA, FAHIMA

Dana C. McWay, JD, RHIA, Secretary

David Muntz, CHCIO, FCHIME, LCHIME, FHIMSS, Advisor

Dwayne M. Lewis, RHIT, CCS

Jennifer McManis, RHIT, Speaker of the House

Melissa M. Martin, RHIA, CCS, CHTS-IM, Treasurer

Lynne Thomas Gordon, MBA, RHIA, CAE, FACHE, FAHIMA, Chief Executive Officer

Virginia E. Evans, MBA, RHIA, FAHIMA

Susan J. Carey, RHIT, PMP

Zinethia L. Clemmons, MBA, MHA, RHIA, PMP

American Health Information Management Association
233 N. Michigan Ave., 21st Floor | Chicago, IL 60601
ahima.org | (800) 335-5535

AHIMA
American Health Information
Management Association®