233 N. Michigan Ave.,21st Fl.
Chicago, IL 60601-5800

phone » (312) 233-1100
fax » (312) 233-1090
web » www.ahima.org

AHIMA
American Health Information Management Association®

2018 Public Policy Principles

Introduction

The American Health Information Management Association (AHIMA) is the national non-profit association of health information management (HIM) professionals. Representing over 103,000 HIM professionals, AHIMA's mission is to transform healthcare by leading in health information management, informatics, and information governance.

In 2017, AHIMA's Board of Directors identified four strategic objectives to realize AHIMA's vision of improving health through trusted information. These strategic objectives are:

(1) Lead in Informatics
(2) Lead in Data Analytics
(3) Champion Information Governance
(4) Prepare Health Information Professionals for the Future

While the healthcare landscape continues to evolve, the foundational principles of the HIM profession remain the same—ensuring that health data is confidential, complete, accurate, reliable, timely and useful "regardless of medium or format," to reduce costs, provide better care, and improve health.[1] There is no question that the healthcare ecosystem is undergoing transformation as the industry adopts new and emerging technologies and continues to shift toward and adapt to value-based care.[2] Along these lines, while the needs of the industry will shift from translating data to transforming data into knowledge to fuel improved decision-making, AHIMA is committed to its core mission and values by improving health through trusted information.

Over the past nine months, AHIMA's Advocacy and Policy Council has evaluated the current and near-term policy landscape to develop public policy principles that align with the aforementioned strategic objectives and AHIMA's organizational strategy. It is important to note that some of the principles in this document are germane to more than one strategic objective and should not be viewed as exclusive to a specific strategic objective. Rather, the principles serve as a framework to guide AHIMA's public policy activities at the state and federal level throughout the year.

[1] Abrams KJ, Gibson CJ, editors. (editors). Fundamentals of health information management, 2nd ed Ottawa, ON: Canadian Healthcare Association; 2013. Pg. 1
[2] PwC Health Research Institute. "Top Health Industry Issues of 2017: A Year of Uncertainty and Opportunity/" Available at: https://www.pwc.com/us/en/health-industries/pdf/pwc-hri-top-healthcare-issues-2017.pdf

Informatics

The Commission on Certification for Health Informatics and Information Management (CCHIIM), an AHIMA commission dedicated to assuring the competency of professionals practicing health informatics and information management, defines informatics as "a collaborative activity that involves people, processes, and technologies to produce and use trusted data for better decision making."[3]

AHIMA believes it is important to break down the different aspects of the definition of informatics to understand the public policy principles below. The technical component of informatics focuses on how information is entered into the record and/or system. In contrast, the people and processes aspects of informatics as defined above focus on what information is included in the record as well as the quality and integrity of the data in building trusted information.

HIM professionals have traditionally had expertise in data quality and integrity, data standards, and management of data throughout its lifecycle to maximize utilization of the health information by a provider or health system. To date, we have seen a convergence of health information management and informatics competencies due to a number of trends and market forces including, but not limited to: meaningful use, value-based payment reform, personalized medicine and population health management.[4] With such changes, new roles requiring "specialized skills in the use, maintenance, protection, retrieval . . . analysis," and retention of health information will emerge.[5] The principles below are essential to effective informatics practices and ensuring that HIM professionals are prepared to assume these new roles and responsibilities.

1. Health information technology systems should support workflow processes and user-centered design principles that enhance the ability to collect and document quality data.

2. Policies and procedures should be in place to ensure the accuracy, accessibility, completeness, consistency, currency, granularity, precision, relevancy, reproducibility, and timeliness of the data needed to facilitate improved decision-making and care.[6]

3. The integrity of coded clinical data and the ability to turn it into useable information requires all users to consistently apply the same coding standards including: rules, conventions, guidelines, and definitions. Consistent promotion and uniform application of medical coding standards across sites of service will enhance data quality and integrity and facilitate improved decision-making and delivery overall.

[3] AHIMA. "Informatics and Data Analytics." http://www.ahima.org/topics/Informatics/informatics?tabid=overview.
[4] Gibson, C. J., Dixon, B. E., & Abrams, K. (2015). Convergent Evolution of Health Information Management and Health Informatics: A Perspective on the Future of Information Professionals in Health Care. Applied Clinical Informatics, 6(1), 163–184. http://doi.org/10.4338/ACI-2014-09-RA-0077.
[5] Ibid.
[6] AHIMA. "Informatics Toolkit for Health Informatics and Information Management Professionals." http://bok.ahima.org/PdfView?oid=302342.

Data Analytics

As the demand for data in healthcare continues to flourish, organizations are becoming more data driven in making healthcare and business decisions in such areas as revenue cycle management, quality improvement, resource utilization, and population health management. HIM professionals are uniquely qualified to analyze data given their knowledge and expertise in translating data into meaningful, timely and relevant information for decision-making purposes. The public policy principles below are crucial to ensuring effective data analytics and practices.

1. The use of structured data including the use of a common set of standards, policies, and practices should be promoted to minimize inconsistent data formats and ensure the capture and sharing of meaningful, accurate, quality data.[7]

2. Data sharing policies that encourage the sharing of protected health information (PHI) for reasons other than treatment, payment or health care operations (or otherwise permitted or required under the Health Insurance Portability and Accountability Act (HIPAA), should protect an individual's privacy and security, including a person's right to withdraw authorization to share their health information.

3. Common data standards and policies should be adopted broadly to ensure semantic, technical, and functional interoperability in order to facilitate data analytics within and across organizations and providers. Data standards should be selected based on their maturity, level of adoption, compatibility and interoperability.[8]

4. Solutions should be implemented to address patient identification matching problems nationwide. The solutions should be 100 percent accurate, interoperable, scalable, secure, safe, and capable of being implemented across different care settings.

[7] AHIMA. "Health Data Analysis Toolkit." http://bok.ahima.org/PdfView?oid=302359.
[8] AHIMA. "Data Standards, Data Quality, and Interoperability." http://bok.ahima.org/doc?oid=107104#.WfNL8FuPKpo.

Information Governance

Ensuring accurate and trustworthy information from the data to the medical record and business systems level, whether it be in electronic or paper format, is of critical importance to AHIMA and its members.

AHIMA has developed an information governance organizational framework for managing information throughout its lifecycle that supports an organization's strategy and operations including regulatory, legal, risk, and environmental requirements. This framework is a critical organizational initiative that healthcare organizations must embrace to thrive in healthcare today. AHIMA's Information Governance Adoption Model (IGAM)™ consists of 10 IG organizational competencies. The public policy principles below are representative of a number of these competencies and are critical to a robust information governance organizational framework.

Privacy and Security

1. The confidentiality of protected health information (PHI) should be protected to the fullest extent prescribed under the Health Insurance Portability and Accountability Act (HIPAA), regardless of the medium in which it is stored and where it travels and/or whether the organization is a covered entity or business associate as defined by HIPAA. Organizations and their employees should comply with HIPAA, state laws, and the policies and procedures put in place to protect PHI.[9]

2. Federal and state privacy and security laws, regulations, guidance, and policies should be harmonized to improve the electronic and/or physical movement and sharing of health information.

3. Treatment of health information, including information related to mental health and substance use disorder treatment should be aligned with the requirements of HIPAA to ensure consistency in the access, use, and disclosure of such information to improve care coordination and produce quality outcomes.

4. Privacy and security processes, best practices, and guidelines should be in place to ensure appropriate access is granted when and where it is needed by authorized users so that the correct information gets to the right person at the right time in the proper setting.

5. Guidance should be provided to ensure that small and medium-sized organizations and providers, including vendors and business associates, have the resources necessary to meet the privacy and security requirements of HIPAA.

[9] AHIMA. "Guidelines for a Compliant Business Associate Agreement." http://bok.ahima.org/doc?oid=301918#.WfNKLFuPKpp.

6. Policies and procedures should be developed, including training and education, to reduce the risk of security threats to information technology infrastructure and minimize security risks related to user-related behavior.[10]

7. Resources should be dedicated to improving cyber literacy and awareness of cyber risks among stakeholders, including within organizational leadership and across the healthcare continuum.

8. Continued enhancement and improvement of information sharing of cyber threats, risks and mitigations in real time between the federal government and private sector stakeholders should be supported and aligned with cross-sector information sharing activities in a manner that is consistent with protecting privacy and security to maintain appropriate legal protections.

Legal and Regulatory

1. Paper and electronic health record (EHR) systems should have the capability to create, manage, preserve, and disclose records that meet evidentiary legal requirements and can serve as official business records.[11]

2. Policies should be promoted to ensure consumers have timely access to their health information in the form and format requested by the consumer as required by HIPAA.[12]

Data Governance

1. Standards-based documentation and documentation integrity practices should be broadly adopted to generate reliable and trusted information for care continuity, quality improvement, research, population health, reimbursement, and other administrative purposes.

2. Implementation of new technologies should align with documentation integrity practices to ensure the data is accurate, reliable, and trusted no matter where it flows within the healthcare ecosystem.

3. Clinical documentation improvement (CDI) practices should be utilized when necessary to ensure high quality documentation within a patient's health record which can assist in: accurate capture of severity of illness and risk of mortality, measurement of intensity of care, improved data for outcomes and quality measures, improved regulatory compliance, more accurate reimbursement and preparation for future payment methodologies.[13]

4. Coding professionals and clinical documentation improvement professionals should adhere to ethical coding guidelines and practices, including AHIMA's Standards of Ethical Coding and Ethical Standards for CDI professionals to ensure the production of high quality healthcare data and prevent coding and documentation practices intended to increase payment

[10] AHIMA. "Understanding Cybersecurity: A Primer for HIM Professionals." http://bok.ahima.org/doc?oid=301408#.WfNGcVuPKpo.
[11] AHIMA. "EHRs Serving as the Business and Legal Records of Healthcare Organizations." http://bok.ahima.org/doc?oid=301443#.WfNCVFuPKpo.
[12] AHIMA. "Consumer Engagement Toolkit." http://bok.ahima.org/PdfView?oid=301404.
[13] AHIMA. "Clinical Documentation Improvement Toolkit." http://bok.ahima.org/PdfView?oid=301829.

inappropriately, qualify for insurance policy coverage or skew data by means that do not comply with federal and state statutes, regulations, rules, and guidelines.[14]

Information Technology Governance

1. Connected health and the expansion of such technologies, including telehealth and remote patient monitoring services, have tremendous potential to lower healthcare costs while improving access and quality of care. Connected health technologies should include reasonable and appropriate controls to not only protect the privacy and security of a patient's health information but ensure that the health information collected and associated with the connected health technology is accurate, reliable, trusted, and actionable.[15]

2. Patient portals and application program interfaces (APIs[16]) should be enhanced to allow consumers to access their complete medical record in a secure environment and to foster bidirectional exchange of health information between providers and consumers (including caregivers and individuals designated by the patient.)[17]

Enterprise Information Management

1. Identity proofing, credentialing, authentication and authorization controls and/or processes should be in place to ensure that the consumer and/or individual authorized to access such information is accurately identified and verified when accessing an individual's health information.

2. Consumers should be able to share all types of data with their providers as to give a complete and holistic view of their health status. Policies and standards should be developed to support the secure capture, validation, integration, use, and sharing of patient-generated health data (PGHD).[18]

Awareness and Adherence

1. Education, training, and assistance should be provided by health information professionals to assist individuals and providers in understanding an individual's right of access under HIPAA including the use of patient portals or third party applications via APIs. Such education should

---

[14] AHIMA. "American Health Information Management Association Standards of Ethical Coding." http://bok.ahima.org/doc?oid=302237#.WfNUbFuPKpo, AHIMA. "Ethical Standard for Clinical Documentation Improvement (CDI) Professionals." http://bok.ahima.org/doc?oid=301868#.WfNVrVuPKpo.

[15] AHIMA. "Telemedicine Toolkit." http://bok.ahima.org/PdfView?oid=302358.

[16]'An API is a set of programming protocols established for multiple purposes. APIs may be enabled by a provider or provider organization to provide the patient with access to their health information through a third-party application with more flexibility than is often found in many current "patient portals."' *Federal Register* 80, no. 200, October 16, 2015; p. 62842. Available at https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25595.pdf.

[17] AHIMA. "Patient Portal Toolkit." http://bok.ahima.org/PdfView?oid=301419.

[18] AHIMA. "Consumer Engagement Toolkit." http://bok.ahima.org/PdfView?oid=301404., AHIMA. "Including Patient-Generated Health Data in Electronic Health Records." http://bok.ahima.org/doc?oid=107560#.WfNJwFuPKpo.

include best practices for requesting and providing a patient with their health information as well as a process for addressing patient requests for correction to their medical record.[19]

2. Partnerships between providers, health information exchanges, networks, health plans, HIM professionals, and other vested stakeholders should be encouraged to provide consumers access to their health information in a single, longitudinal format that is easy to understand, secure, and may be updated automatically.

[19]AHIMA. "Patient Request for Health Information Model Form." http://www.ahima.org/about/advocacy/efforts., AHIMA. "Making Amendments to Health Records." http://bok.ahima.org/doc?oid=302080#.WfM_ZluPKpo.

Prepare Health Information Professionals for the Future

The HIM profession has long been recognized for its expertise and leadership in medical coding, medical record standards, documentation integrity and privacy-related matters in healthcare. Because of this expertise, the HIM profession often serves as a bridge between clinical, financial, technological, and administrative fields in healthcare.[20]

However, as the landscape of the healthcare ecosystem continues to evolve, the overall role of the HIM profession must transform as well—requiring HIM professionals to take on emerging roles in various fields including but not limited to data analytics and informatics. The public policy principles below align with the recommendations set forth in AHIMA's white paper, *HIM Reimagined: Transformation Starts with You*, and are critical to preparing the HIM profession for the future.

1. Federal and state funding should be dedicated to promoting health informatics and the practice of information management including training and apprenticeships to strengthen the current workforce and generate pathways for career advancement in the field of health informatics and health information management.

2. Appropriate resources should be dedicated to the recruitment and retention of academic professionals with advanced degrees in the HIM profession and/or related disciplines to meet the evolving workforce demands of the HIM profession and the healthcare industry.

3. Resources should be dedicated to supporting the value of HIM skills and the need for data analytics to manage data for strategic business and population health purposes.

4. A designated Standard Occupational Classification code for Health Information Technology, Health Information Management, and Health Informatics Specialists and Analysts should be created by the federal government to reflect the expanded roles of health information professionals related to the implementation of informatics solutions including data analytics, clinical decision support, and machine-human interface to support and enhance patient care.

[20] American Health Information Management Association. *HIM Reimagined: Transformation Starts with You*. Chicago, IL: American Health Information Management Association, 2017.

Conclusion

AHIMA's Public Policy Principles serve as a roadmap for federal and state policy issues affecting the health information management profession. AHIMA seeks to ensure that these public policy principles are reflected in the laws, regulations, and guidance that impact the HIM profession with the goal of improving health through trusted information. The principles will be revisited annually by AHIMA's Advocacy and Policy Council and approved by AHIMA's Board of Directors to ensure their continued relevance and applicability to the policy landscape as well as AHIMA's strategic objectives and organizational strategy.