2017-2018 Public Policy Principles

Approved by the HIMSS North America Board of Directors on December 15, 2016

Introduction:

HIMSS is a global, cause-based, not-for-profit organization focused on better health through information technology (IT). In North America, HIMSS focuses on health IT thought leadership, education, market research, and media services. Founded in 1961, HIMSS North America encompasses more than 64,000 individuals, of which more than two-thirds work in healthcare provider, governmental, and not-for-profit organizations, plus over 640 corporations and 450 not-for-profit partner organizations, that share this cause.

Our nation's healthcare system is in a critical phase, transitioning ***from*** wide-spread implementation of health IT based, in part, on the requirements of the HITECH Act ***to*** IT-driven improvements in care delivery, access to care, health outcomes, and costs. As federal and state policymakers realize the promise of IT to support health policy goals, the growing divide between the rapid speed of innovation and the measured pace of government regulation increases the complexity of the health policy landscape.

Realizing the full value and potential of health IT can result in advances in biomedical research, improved care delivery and access, wellness through disease prevention, early detection of disease, cost effectiveness, and economic opportunity. Fundamental to achieving these advances is the Office of the National Coordinator for Health IT's (ONC) role in in aligning federal health IT policy and coordinating activities across government agencies, with States, and the private sector.

HIMSS's Public Policy Principles[1] ("Policy Principles") serve as guidance for federal and state legislative and regulatory policy. Through this framework, the HIMSS North America Board of Directors articulates our policy expectations of practical solutions being harnessed to achieve better health through the best use of IT. The Policy Principles provide policy-makers, our chapters, and our members with well-articulated solutions to inform and shape public discourse on the policy issues of the day, and understanding of how today's decisions may impact, and be impacted by, the future.

---

[1] Policy Principles are formally reassessed bi-annually through a process that includes review by HIMSS Committees and subject matter experts, and approval by the Board of Directors. Proposed changes may be submitted by any HIMSS member. HIMSS's Policy Principles are updated by the Board of Directors on an as-needed basis.

HIMSS believes, to the extent possible, federal, state and regional policy should be harmonized to minimize conflicting requirements, support alignment of goals and objectives, and enable private sector innovation.

To that end, HIMSS maintains the following overarching principle: Government program requirements must: a) justify benefits based on evidence that considers costs, cumulative burdens, finite resources, and competing priorities; (b) not conflict or overlap; and, (c) acknowledge a reasonable amount of time ***and*** resources needed for implementation of new policies or program requirements, and where applicable, a reasonable amount of time to innovate and/or implement health IT solutions.

For 2017 - 2018, the HIMSS Public Policy Principles address the following components of the Value of Health IT:

Supporting Care Transformation

1. Quality, Safety and Outcomes
2. Clinical & Administrative Efficiency
3. Interoperability, Health Information Exchange & Infrastructure
4. Innovation & Research
5. Information Privacy and Security
6. Patient Activation and Engagement

Expanding Access to High Quality Care

1. Connected Health
2. Equity

Increasing Economic Opportunity

1. Workforce Development
2. Economic Growth

Making Communities Healthier

1. Population Health Management
2. Public Health

Supporting Care Transformation

1. Clinical Quality, Patient Safety & Outcomes

A.) Continuous quality improvement of the provision of care must be supported by a scientific approach and standards determined to be industry best practices to the development, reporting, and continued use of clinical quality measures supported by health IT.

B.) Quality measures must reflect current evidence and clinical guidelines with consideration of the following factors: appropriateness, availability, continuity, effectiveness, efficiency, safety, timeliness, patient satisfaction, patient empowerment, health improvement, and consistency with technical standards and value.

C.) Integrated health IT systems should embrace reporting capabilities to define and capture data to fulfill public payer, private payer, and government health agency requirements.

D.) The development, implementation, and use of health IT systems should involve full consideration of related patient safety issues.

E.) Clinical and business intelligence - the use and analysis of data captured in, and outside of, a care setting - should directly inform decision-making. It has the power to positively impact patients' care, health outcomes, and economic wellness, as well as improving business operations of the system itself.

2. Clinical & Administrative Efficiency

A.) The control of soaring care-related costs, sustainability of our nation's health system, and ensuring the broadest access to care, must be coordinated among public and private-sector entities, across clinical care and public health, and between government and the private sector. Harmonization and simplification of IT systems across all entities is essential.

B.) Administration and overhead adds significantly to nationwide and individual health-related costs; this must be addressed through the effective use of health IT.

C.) Administrative simplification must be an integral part of all health IT systems' development.

D.) Health IT systems must support enhanced workflow processes and user-centered design principles to enable the delivery of efficient, cost effective, and high quality care, and to efficiently coordinate high-quality care benefitting the patient.

E.) Reduce resource waste by establishing efficient practices that automate and support clinical and business intelligence, and compliance practices.

F.) Use health IT for data mining not only for retroactive utilization such as reporting and performance review, but for proactive identification of inefficient, suboptimal or wasteful use of resources.

3. Interoperability, Health Information Exchange & Infrastructure

A.) All individuals, their families, and healthcare providers should be able to send, receive, find and use electronic health information in a manner that is appropriate, secure, timely and reliable to support their health and wellness.[2]

B.) Health information must be accessible[3] and able to follow the individual. The ability to efficiently and securely exchange health information among healthcare stakeholders, in a form that also allows for the data to be consumed discretely and in a manner that enables clinical decision support, is fundamental to promoting patient safety, achieving quality outcomes, facilitating care coordination and transitions of care, and controlling costs.

C.) Interoperability should support the combination of administrative and clinical data to enhance transparency and enable value-based payment.[4]

D.) Achieving nationwide interoperability across the health IT ecosystem will require stakeholders to agree to and follow a common set of standards, services, policies and practices that facilitate the appropriate exchange and use of health information nationwide. Nationwide interoperability should not limit competition.

E.) Testing and certification programs, such as ConCert by HIMSS™ and IHE' Conformity Assessment, can increase market confidence in the interoperability and safety of health IT products, accelerate the development and commercialization of technology, and enable standards developers, technology developers and users to evaluate technical implementations for inconsistencies and unexpected behaviors among other issues.

F.) The ONC Health IT certification criteria development process should be enhanced, expanded, and applied openly and transparently, with extensive provider and vendor input.

G.) Healthcare is one of the sixteen critical infrastructure sectors identified by federal, state, and local governments. Policy advancements and program development should reflect that IT is the backbone of the U.S. healthcare infrastructure supporting medical research, care delivery, public health, and a number of other national priority areas. Investments in health infrastructure should ensure all communities have access to the economic and technology advantages of health IT.

4. Innovation & Research

A.) Legislation and regulation must be balanced with the need to encourage technological innovation which is essential to improving quality of care and health outcomes, controlling costs, engaging/activating consumers/patients/caregivers, and increasing access to care.

---

[2] Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap, October, 2015
[3] HIMSS Board Approved Definition of Interoperability, April 5, 2013
[4] Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap, October, 2015

B.) Legislation and regulation can play a role in supporting patient safety and must be balanced with the need to encourage technological innovation, which is also essential to improving quality of care and health outcomes, controlling costs, engaging and activating consumers/patients and their caregivers, as well as improving access to care.

C.) Technology-enabled delivery systems must engender a "Learning Health System" which supports continuous clinical quality improvement by utilizing evidence-based clinical decision support, market and syndromic surveillance, which in turn, refines the learning of an organization and advances quality outcomes.

D.) Health IT plays a critical role in the advancement of health research. Health IT must leverage automation, advanced health-related artificial intelligence tools, partnerships with universities, medical institutions, and healthcare data warehouses, and utilize real-time information exchanges to accelerate ideation of clinical delivery pathways.

E.) Health IT, like all technologies, brings about innovative solutions, but often creates new legal issues. As new technologies develop, clear enforcement principles should be defined. Clarity, transparency and predictability of the regulatory environment allows for innovation in health IT.

F.) Current user experience policy addresses usability testing related to the software development cycle for electronic health records (EHRs). Research and policy should address user-centered design principles for ***all*** health IT products through their complete product life cycle, including evaluation, selection, implementation, optimization, operational decisions, and governance. Finally, in an effort to improve patient safety, drive better clinical outcomes, lower costs, and improve the patient's experience, realistic solutions that align regulatory and product development timelines must be sought.

5. Information Privacy & Security

A.) A well-functioning health system requires the development and maintenance of a trust framework through recognition, management, and enforcement of privacy principles and risk-based security practices which, consistent with data stewardship, also allows for appropriate access and use, appropriate information flow in care delivery, and appropriate secondary uses to promote a learning health system.

B.) A unified approach to health sector security is necessary. It can be achieved through the creation and adoption of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes for the adoption of a common set of voluntary, universal information privacy and security framework with use cases and implementation guidance—scalable for a wide range of healthcare organizations and inclusive of small, medium, and large providers.

C.) Workforce development for health information privacy and cybersecurity requirements must be supported and prioritized across the health sector.

D.) Security and resilience of the health sector should be supported through means which include the following: (1) intelligence and information sharing intra-sector and cross-sector with government and private sector stakeholders, (2) identification of threats, vulnerabilities, and hazards, (3) defense in depth, (4) strong multi-factor authentication and strong passwords, (5) encryption, (6) supply chain integrity and security, (7) vendor and third party management, (8) situational awareness, (9) information superiority, (10) education and training, (11) detection, response, mitigation, and interdiction of threats and hazards--internal and external to health stakeholders, (12) risk assessments and risk management, (13) business continuity, (14) disaster recovery, (15) emergency preparedness, (16) organizational policies, procedures, standards, baselines, and guidelines (17) authorized penetration testing, (18) mock exercises, (19) fault tolerance of IT infrastructure and assets, and (20) security research.

E.) Advancing the state of the art for cybersecurity and other types of security across the health sector, and sectors upon which the health sector depends, should be supported to: (1) protect the confidentiality, integrity, and availability of patient information and other sensitive information and assets of stakeholders, (2) ensure the continued delivery of patient care and coordination of care, and (3) protect patient safety.

F.) Manufacturers, vendors, and others in the supply chain should be encouraged to proactively address the security of products and services (including, but not limited to, medical devices, mobile applications, software applications, web applications, cloud service providers, EHR vendors, etc.) throughout the product/service lifecycle, including during the design, development, production, distribution, deployment, and maintenance of such products and services.

G.) Timely and proactive information sharing should be facilitated among security researchers, manufacturers, vendors, service providers (and other relevant parties in the supply chain), their customers, and government agencies (such as FDA & DHS), on potential threats, vulnerabilities, and mitigation information, inclusive of hardware, software, operating systems, databases, mobile applications, medical devices, wearable devices, implantable devices, embeddable devices, ingestibles (e.g., IoT sensors), operating systems, web applications, firmware, hardware components, Internet and network stability and security, software libraries, application programming interfaces (APIs), and other objects.

H.) Barriers to exchanging information in health and healthcare should be minimized through harmonization of federal and state privacy and security laws, regulations, and policies.

6. Patient/Consumer Activation & Engagement

A.) Health IT systems must be designed to ensure patients, caregivers, consumers and communities are the center of the system by way of the following:

(i) ensure that they obtain the right information at the right time to enable them to make accurate decisions about the delivery and coordination of their care;
(ii) ensure that they can, easily and efficiently, communicate with their providers, including in view of the objectives as set forth in (i).

B.) Patients and caregivers - empowered and active participants - lead to improved quality, reduced costs, higher patient satisfaction, responsibility for health-related decisions and aligned provider and patient goals.

C.) Ensure that health IT infrastructure supports the belief that patients are at the center of the care team, and are accountable members of the care team, by providing education and clear messaging about clinical and wellness data, how to access and direct their data, costs and quality. Information literacy should be prioritized to facilitate effective use of information from valid and reliable sources.

D.) Health IT including EHRs, personal health records (PHRs), patient portals, electronic health information (EHI), APIs, mobile applications and medical devices, patient-generated health data and data infrastructure are critical to enabling bi-directional communication that empowers consumers, patients, and caregivers.

Expanding Access to High Quality Care

1. Connected Health

A.) Connected Health, and integrated wired, mobile and wireless technologies have the potential to empower patients through remote monitoring, telehealth, and the expansion of access to care for underserved and remotely-located patient populations. Connected Health allows for a continuum of support and access to information between locations of care (e.g. from hospital, to skilled nursing facility, to the home). The use and innovation of mobile technologies must be encouraged and not be over-regulated to further enable measureable outcomes of successful planning and transitions of care activities.

B.) The safe, effective, secure, and integrated application of wired, mobile, and wireless technologies must play a central role in advancing individual, population, and public health and facilitate care regardless of location.

C.) Payment system reform is necessary to promote Connected Health through telemedicine/ telehealth services and remote patient monitoring.

2. Equity

A.) Consumers, patients, caregivers, and providers should have equitable access to health IT regardless of race, ethnicity, age, gender, geography, education, sexual orientation, or socioeconomic status.

Increasing Economic Opportunity

1. Workforce Development

A.) A robust, diverse health IT workforce is essential to transformation of the nation's health system through best use of science, evidence, knowledge, innovation, technology and informatics.

2. Economic Growth

A.) Health IT through advancement of interoperability and innovation offers great potential as American exports and should be cultivated as an export industry through innovation labs and makerspace environments.

Making Communities Healthier

1. Population Health Management

A.) Integrated Health IT Systems are essential to assess and track utilization, quality, and cost metrics for specific populations.

B.) Health IT has a role in promoting coordination and transitions of care across all settings, all specialties and types of providers.

C.) Value-based care models and population health management are innovation drivers for health systems to design interventions that take into account health needs with the unmet social and economic needs of populations.

D.) Data is the foundation for improving decision-making in a world of value-driven care and payment. Access to social determinates of health data and community vital signs data will further enrich population health management programs.

2. Public Health

A.) Electronic health information collected near real-time (as a by-product of care delivery) can support coordination of public health. Primary and urgent care can enable enabling population level syndromic surveillance, better management of outbreaks and disasters, and disease prevention and control.

Conclusion:

These HIMSS Public Policy Principles serve as guidance for federal and state policy issues involving health IT. HIMSS is prepared to assist and support other stakeholders to ensure that

these policy principles are reflected in laws and regulations aimed at positively transforming our health system through the best use of IT. These principles are formally revisited biannually, and as necessary in the interim, to ensure their relevance in this rapidly changing environment. Please contact HIMSS for clarification or to make recommendations.

Appendix A: Examples of 2017-2018 HIMSS-Supported Policies[5]

Supporting Care Transformation

1. Clinical Quality, Patient Safety and Outcomes
   - A.) The Secretary of Health and Human Services (HHS) should review and evaluate a five-year roadmap of all mandated health program requirements and changes administered by HHS that impact the operations of providers, payers, and health information technology vendors.
   - B.) Substantive changes to federal reporting requirements (for example, a new CQM or a change in a current CQM that requires a workflow/system change) should be published in rulemaking. Data collection, reporting, and performance should not be required for new measures that have been changed resulting in significant workflow changes until 18 months following the publication of the final rulemaking. *[6]
   - C.) HHS should require CMS and the Office of the National Coordinator for Health IT (ONC) to implement an aggressive and thorough quality measures testing program to ensure that measures have been adequately specified and tested before requiring them for Meaningful Use, Inpatient Quality Reporting (IQR), MIPS e-Reporting, as well as in use in any Medicare Advanced Alternative Payment Model. All selected eCQMs should meet the following criteria:
     i. The eMeasures specifications are tested and piloted to confirm they are accurate, with the correct clinical category defined and mapped to the correct vocabulary standards (taxonomy) and codes, along with the correct attributes and state(s).
     ii. The eMeasures are validated by the measure steward and tested for validity and reliability against the measures intent.
     iii. Required data elements can be efficiently and accurately gathered in the healthcare provider workflow, if at all possible using data elements that are already collected as a byproduct of the care process and stored in the EHR and other certified business information systems.
     iv. CQM reports based on eMeasures accurately reflect the care given by the applicable healthcare provider(s).
     v. The testing evaluates the output from translation of the measure to established standards in the health quality measure format (HQMF) and successful transport using the quality reporting document architecture format to CMS.
     vi. Selected CQMs should present a clear pathway to value and fit into an analytics capability for use by health care professionals and hospitals as a meaningful scorecard on performance. HIMSS urges policymakers to engage with developers, in a voluntary and collaborative manner, on

[5] This list is intended to provide examples of polices that align with the 2017-2018 HIMSS Public Policy Principles. It is not intended to be a comprehensive list of all policies that fit within the policy principles.
[6] * Indicates HIMSS North America Board Approved Positions

identifying and implementing the most promising ways to present visualize data and quality results for action.

2. Clinical & Administrative Efficiency
   A.) Align federal policy and healthcare stakeholders in order to facilitate electronic business processes to reduce inefficiency in the healthcare financial infrastructure and support real time information management.
   B.) Coordinate and harmonize data standards to facilitate more cost-effective private sector compliance with diverse federal program requirements.
   C.) Encourage a strong partnership between government and private sectors to encourage further innovation, transparency in price and quality, and facilitate the implementation and operation of health IT systems through strategic planning, resource management, and both public and private investments.
   D.) Improve patient safety, privacy and information security by promoting zero tolerance for fraud and abuse in the billing and claims process through the appropriate use of EHR technologies and related business practices.

3. Interoperability and Health Information Exchange
   A.) Congress should clarify the Labor-HHS UPI rider and immediately direct HHS to study patient data matching solutions; such study must include the impact of: implementing a national-level UPI; how a national-level solution might impact locally-based solutions currently underway; and how various levers (federal-mandates, public-private collaboration, etc.) impact progress towards solution. *
   B.) Direct all federally-funded national and state government agencies to have the functionality to exchange data with healthcare institutions through means of standards-based interfaces, e-data exchange & access, and health information exchanges.
   C.) Maintain prioritization of the Departments of Defense and Veterans Affairs' EHR modernization efforts resulting in interoperable systems that ensure connectivity to each other as well as civilian entities providing care for military service members, veterans, their families, and other beneficiaries by engaging in private sector-led interoperability efforts.
   D.) Support private sector efforts for accelerating the adoption of consensus-based standards, interoperability specifications, and guidelines, such as IHE Integration Profiles and Continua Guidelines.
   E.) Support frameworks which promote the safe and secure transmission of health information via the Internet and any other mode; and, continue to work with the public and private sectors to achieve that goal. *

4. Innovation & Research
   A.) For regulatory purposes, "medical device" should not be defined to include software or hardware if it is not integral to the functioning of a traditional diagnostic, therapeutic, or surgical device. "Medical device" should not cover software or hardware that provides clinical decision support (with very limited

exception), technology that, simply transmits or allows other parties to read information originally sent from a medical device, EHRs, or technologies that are widely used in other industries. Congress should work with HHS to develop a risk-based oversight framework for such software or hardware that takes into account factors such as risk relative to intended use and cost/benefit of any proposed oversight, with the intent of ensuring patient safety. *

B.) Support the creation of criteria for high quality, patient generated (and attributed) health data to be accommodated within EHRs, other health IT systems, and data aggregation systems, for use in making better decision-making towards improved outcomes.

C.) Support the design of systems, usability and workflows that enhance patient safety, facilitate decision making, consumer access, and improve provider efficiency

D.) Encourage the expansion and permanence of the Stark exemptions (exemptions from anti-trust laws) and anti-kickback safe harbors for EHRs to cover additional healthcare software. The Secretary of HHS should implement necessary measures to protect against conflicts of interest and improper relationships among providers.

5. Information Privacy and Security

A.) Eliminate any expansion of accounting of disclosure requirements unless proven to justify the burden through actual evidence of benefit.

B.) Elevate the HHS Chief Information Security Officer and expand the office's portfolio to include an external focus and development of a sector specific plan.

C.) Federal agencies and entities should engage in outreach efforts with state agencies and entities (e.g., meetings, conferences, workshops, or other means) that may establish, maintain, or contribute to privacy and security regulatory or legal schemes to facilitate harmonization of requirements.

6. Patient Activation and Engagement

A.) Promote public and private incentives to encourage patient/caregiver and provider utilization of EHI, while also protecting the privacy and security of individual health information.

B.) Fund studies that promote patient health and technology literacy, identify effective patient engagement strategies and techniques, and promote self-management and point-of-care decision-making tools for patients and consumers.

Expanding Access to High Quality Care

1. Connected Health

A.) Eliminate the geographic restrictions on telehealth (i.e., currently limited only to Health Professional Shortage Areas and not in metropolitan statistical areas)

B.) Amend the allowable originating sites of care beyond those currently stipulated by CMS to include interactions with patients from wherever the patient is located, including the home, where cost effective and medically appropriate

C.) Expand modalities beyond live (real-time) voice and video to include active monitoring between clinicians, patients and care providers.

D.) Support the integration of mobile technologies into the design and deployment of alternative payment models and MIPS.

2. Equity
   A.) Ensure the robust implementation by all relevant federal, state, territory, tribal, and local entities of broadband-enabled healthcare technologies to build the infrastructure needed to improve access to healthcare in rural and underserved communities.
   B.) Federal programs should include provisions focused on assisting the smallest medical practices to ensure their ability to implement and use certified technology in a meaningful manner.
   C.) Ensure adequate public funding for culturally, linguistically, and age appropriate public awareness programs to inform patients/caregivers about the benefits of health IT.

Increasing Economic Opportunity

1. Workforce Development
   A.) Support the addition of health informatics education in accredited schools, develop competency-based continuing education programs, and improve specialty training programs.
   B.) Promote the development of a diverse workforce of health IT professionals, clinicians, and educators that understand the requirements of clinical informatics and technology principles through various avenues of career development, professional certification and levels of education.
   C.) Continue to authorize and appropriate adequate funding for the Health Resources and Services Administration (HRSA) to promote the proficiency of nursing, clinical, and other healthcare professionals in healthcare technology.

Making Communities Healthier

1. Population Health Management
   A.) Support the development/enhancement of standard methods for attributing a patient population to a provider/health system consistently.
   B.) Develop, in conjunction with innovative care models, the use of data and information from EHRs and health IT to improve population health outcomes through analytics and the informed development of proven models, pilots, and innovative strategies
   C.) Encourage the recording of demographic and social determinants of health data for the benefit of healthcare quality improvement and population health management to identify local, regional, and national trends.

2. Public Health
   A.) Support the use of health information facilitated by EHRs, and health IT inside and outside of direct healthcare delivery to enable rapid detection and on-going

monitoring of public health events for the purpose of triggering appropriate early response, including syndromic surveillance, resource management, community-based planning and modeling, and improvement of public health, de-identified when appropriate while protecting and minimizing the impact on patient privacy

B.) Fund initiatives that facilitate the exchange of health information, immunization integration and reporting from trusted sources among population health, school and clinical care systems to protect and improve public health.