AMIA
INFORMATICS PROFESSIONALS. LEADING THE WAY.

AMIA PUBLIC POLICY PRINCIPLES AND POLICY POSITIONS

2019 – 2020 Priorities

(Updated with the AI Principles, 2022)

CONTENTS

PREFACE

Increasingly, the science and tools of informatics are being leveraged across all levels of healthcare delivery, public health and clinical research. The digitization of data across the health and research enterprise has thrust a traditionally academic pursuit more firmly into everyday application. Healthcare delivery now relies on electronic health records (EHRs); regulated medical devices and pharmaceutical drug development increasingly use a host of real-world data to demonstrate safety and effectiveness; epidemiologists have the capacity to leverage untold sources of data with the advent of the Internet of Things; and clinical research can now rely on vast databases as part of the Big Data revolution. Informatics is foundational to each and every one of these transformations.

Over the last nine months, AMIA's Public Policy Committee has considered the present and near-term policy landscape to develop Principles and Positions across select, priority domains, which are essential to the emergent realm of public policy referred to as Health Informatics Policy. Similar to Environmental Policy, Education Policy and Social Policy, Health Informatics Policy is a distinct policy domain which seeks to **optimize** care delivery & care experience, **improve** population and public health, and **advance** biomedical research through the collection, analysis and application of data.

AMIA Public Policy identified nine initial pillars as core to Health Informatics Policy, including: Patient Empowerment, Health IT Safety, Workforce and Education, Data Sharing in Research, Health IT Data Standards & Interoperability, Informatics-Driven Quality Measurement, Population & Public Health, Health Data Privacy, and AI Principles.

Each priority begins with a series of statements describing what AMIA *believes* – Principles that describe the values intrinsic to the pillar and viewed through an informatics lens. A series of Policy Positions are resultant from these Principles, and they are supported through evidence in peer-reviewed literature. We worked diligently to represent AMIA's Core Values by convening interdisciplinary sub-groups to develop each evidence-based position through a consensus process.

We are hopeful that these Principles and Positions will help AMIA articulate to its members, policymakers and other stakeholders those issues and conversations we hold with highest import. Over the next several months, the Public Policy Committee will continue its work to define the core of Health Informatics Policy, and we will continue our brand of evidence-based policy recommendations – supported by the latest research and reinforced through the literature – so that policymakers may benefit not just from what our members know, but from what they do.

PATIENT EMPOWERMENT

Individuals are central to the future of care and research, evermore so as consumer devices and applications persist through society. These Principles and Positions highlight the relationship between institutional informatics, consumer technology, and individuals' growing expectations for how technology should enable and empower their experiences, while articulating ways in which public policy must support this dynamic relationship.

AMIA Believes:

AMIA Policy Principles

Policies, programs, research and care delivery should seek to empower patients through access to, and control of, their personal health information.

Health informatics is a key to enabling delivery of patient-centered care.

Patients have a vital role to play in the development of public policy as well as publicly-funded programs & research.

Based on these Principles, AMIA Supports:

1. Efforts that enable patients to access and transmit all data contained in their electronic health record, rather than a limited or pre-defined set of data, to improve availability of data for care delivery,[1,2] biomedical discovery,[3] and in support of patients' own health and wellness.

2. Technology-enabled approaches that encourage patients to review and contribute directly to their record, which has been shown to improve their understanding of their own health information,[4] lead to improved self-care,[5] increase the likelihood of the patient's story being communicated accurately,[6] and improve trust within the doctor/patient relationship.[7]

3. Technologies and strategies that enable patients to have control over who accesses and uses their health data and biospecimens, and enable them to learn, who has accessed their health data, which has shown to improve patient autonomy and trust in their providers. [8,9]

4. Minimizing the burden patients experience when attempting to access and use their own health information through patient-facing informatics tools, such as usable and

accessible patient portals, HIE interfaces, and other aggregation tools.[10]

5. Use of tools to translate technical language and medical abbreviations to lay terms to facilitate improved communication and promote health literacy.[11, 12]

6. Using a wide range of technologies, (e.g., web-based portals, telemedicine, apps and APIs, mobile health, wearables and social media) to encourage and enhance patients' active participation in their health care, which has been shown to improve health outcomes such as medication adherence[13] and reduced urgent care utilization.[14]

7. Ongoing and enhanced efforts to fund research that contributes to and advances the design and evaluation of digital technologies that enable patients to manage their own health and that of their families.[15, 16]

8. Patients' efforts to design, test, and validate new technologies that help them manage their health and the health of their families.[17]

9. Transparent payment policies and other initiatives that promote patient-centered care coordination using a wide range of technologies to accommodate patient needs and preferences.[18]

[1] Klein D., Fix ., et al. (2015). Use of the Blue Button Online Tool for Sharing Health Information: Qualitative Interviews With Patients and Providers. *Journal of Medical Internet Research*. 2015 Aug; 17(8): e199.

[2] Mohsen, M., Aziz, H. (2015). The Blue Button Project: Engaging Patients in Healthcare by a Click of a Button *Perspectives in Health Information Management*. 2015 Spring; 12(Spring); 1d.

[3] Chisholm, R., Denny J., et al. (2015) Opportunities and Challenges Related to the use of Electronic Health Records Data for Research. *National Institutes of Health Precision Medicine Workshop (Invited White Paper)*. 2015 Feb.

[4] Esch T., Mejilla R., et al. (2016). Engaging patients through open notes: an evaluation using mixed methods. *BMJ Open* 2016;6:e010034.

[5] Wright E., Darer J., et al. (2015). Sharing Physician Notes Through an Electronic Portal is Associated With Improved Medication Adherence: Quasi-Experimental Study. *Journal of Medical Internet Research,* 17(10)e:226

[6] Varpio, L., Rashotte, J., et al. (2015). The EHR and building the patient's story: A qualitative investigation of how EHR use obstructs a vital clinical activity. *International Journal of Medical Informatics, 84*(12), 1019-1028

[7] Bell S., Mejilla R., Anselmo M., et al. When doctors share visit notes with patients: a study of patient and doctor perceptions of documentation errors, safety opportunities, and the patient-doctor relationship. *BMJ Qual Saf* 2016

[8] Caine K., Hanania R. (2013) "Patients want granular privacy control over health information in electronic medical records." *Journal of the American Medical Informatics Association*. 2013;20:7–15.

[9] Weinfurt, K., Bollinger, J., et al. "Patients' views concerning research on medical practices: Implications for consent." *AJOB Empirical Bioethics*. 2016:7(2)

[10] De Lusignan, S., Mold, F., Sheikh, A., et al. (2014). Patients' online access to their electronic health records and linked online services: A systematic interpretative review. *BMJ Open,* **4**, e006021

[11] Ratanawongsa N, Barton J et al. Computer use, language, and literacy in safety net clinic communication. *Journal of the American Medical Informatics Association*. 2016; pii: ocw062. doi: 10.1093/jamia/ocw062.

[12] Brach C, Keller D. Ten attributes of health literate health care organizations. June 2012. Institute of Medicine. https://nam.edu/wp-content/uploads/2015/06/BPH_Ten_HLit_Attributes.pdf.

[13] Lyles, C., Sarkar, U. et al. (2016). Refilling medications through an online patient portal: consistent improvements in adherence across racial/ethnic groups. *Journal of the American Medical Informatics Association*. 2016;23:e28–e33

[14] Shimada SL, Hogan TP, et al. (2013) Patient-provider secure messaging in VA: variations in adoption and association with urgent care utilization. *Med Care. 2013 Mar; 51(3 Suppl 1):S21-8.*

[15] Parmanto B, Pramana G, et al. Development of mHealth system for supporting self-management and remote consultation of skincare. *BMC Medical Informatics and Decision Making*. 2015;15:114.

[16] Piette JD, List J, Rana GK, Townsend W, Striplin D, Heisler M. Mobile health devices as tools for worldwide cardiovascular risk reduction and disease management. Circulation. 2015;132(21):2012-2017.

[17] Lee JM, Hirschfeld E, Wedding J. A patient-designed do-it-yourself mobile technology system for diabetes: promise and challenges for a new era in medicine. *JAMA*. 2016:315(44):1447-1448.

[18] Demiris, G., Kneale, L., Informatics Systems and Tools to Facilitate Patient-centered Care Coordination. *Yearbook of Medical Informatics*. 2015; 10(1): 15–21.

HEALTH IT SAFETY

Health informatics is broader than simply the technology we use to digitally manage records of health and wellness. It includes the operational structures, the processes and practices, the agreed meanings, the people, the culture, and environment surrounding these elements. These Principles and Positions describe the factors that contribute to health IT safety and the actions necessary to prevent patient harm through health IT.

AMIA Believes:

AMIA Policy Principles

Design, implementation, maintenance, and evaluation of health IT can only be credibly carried out by a multidisciplinary team led by trained health informatics professionals.

Assuring the safe use and general safety of health IT is a shared responsibility among oversight bodies, developers, implementers, organizations, hospitals, practices, users, and patients.

Health IT and the practice of clinical informatics play a vital role in identifying more effective medical interventions, preventing errors, improving patient safety, and enabling learning healthcare systems; however, health IT can also introduce new and novel errors and risks to patient safety.

Identifying and mitigating risks introduced by health IT in a coordinated, non-punitive environment, both at the local/organizational and national/systems level, is an essential component for fulfilling the promise of a highly functional health IT ecosystem.

Sharing information about harm enables system improvement. There needs to be a safe place to share cases of health IT that caused harm to patients, whether related to the technology, people, or operational processes in place, alone or in combination.

Based on these Principles, AMIA Supports:

1. The establishment of a national public/private center, or collaborative, on health IT safety meant to convene, analyze and disseminate information to improve the safety and safe use of health IT.[1]

2. The use of standardized reporting mechanisms[2] and patient safety organizations[3] to aggregate, analyze and share information on health IT-related patient safety events across the care continuum.

3. The development of prioritized health IT-related safety measures to ensure (1) that clinicians and patients have a baseline understanding of safe health IT and potential risks; (2) that health IT is properly integrated and used within healthcare organizations to deliver safe care; and (3) that health IT is part of continuous improvement processes to make care safer and more effective.[4]

4. Efforts to fund research that contributes to and advances health IT safety, including research that develops new IT to improve safety, as well as evaluates the safety of live health IT systems *as used in practice,* so that a robust evidence base can inform the total health IT lifecycle and identify ways to remediate risks.

5. Efforts to train and credential health informatics experts at all levels, such as physicians, nurses, pharmacists and researchers, to identify and address health IT safety issues.

6. Regulatory and oversight frameworks that are designed to be proportional to the risk of the activity, and reflective of clinicians' ability to intervene in the activity being informed by health IT.[5]

7. Policies, strategies and technical standards that facilitate health IT-related patient safety event reporting by front-line clinicians and patients.[6]

8. Development and refinement of best practices meant to enable healthcare organizations to address health IT safety within and across organizations, such as ECRI's Copy & Paste Toolkit[7] and ONC's SAFER Guides.[8]

9. Contracts and practices that promote safety, disclosure of errors, bugs, design issues, and software-related hazards, while permitting protection of intellectual property.[9]

10. The application of quality principles and risk management processes – across the health IT lifecycle of design & development, implementation & use, optimization and decommissioning – to improve health IT safety.[10]

[1] Office of the National Coordinator for Health IT, "Health IT Safety Center Roadmap," RTI International. July 2015. Available: http://www.healthitsafety.org/

[2] Agency for Healthcare Research and Quality, "Common Formats," Available: https://pso.ahrq.gov/common

[3] Agency for Healthcare Research and Quality, "Patient Safety Organization (PSO) Program," Available: https://pso.ahrq.gov

[4] National Quality Forum, "Identification and Prioritization of Health IT Patient Safety Measures," Feb. 2016. Available: http://bit.ly/297AWDV

[5] Bipartisan Policy Center Health Innovation Initiative, "An Oversight Framework for Assuring Patient Safety in Health Information Technology," Feb. 2013. Available: http://bit.ly/297Ardb

[6] Huerta T., Walker C., Murray K., et al "Patient Safety Errors: Leveraging Health Information Technology to Facilitate Patient Reporting." *Journal for Healthcare Quality*, 2016 Jan-Feb; 38(1): 17-23

[7] ECRI Partnership for Health IT Patient Safety, "Health IT Safe Practices: Toolkit for the Safe Use of Copy and Paste," ECRI Institute, Feb. 2016. Available: http://bit.ly/297z7qo

[8] Sittig, D.; Ash, J.; Singh, H. "ONC Issues Guides for SAFER EHRs" *Journal of AHIMA* 85, no.4 (April 2014): 50-52.

[9] Goodman, K., Berner, E., Dente, M., et al "Challenges in ethics, safety, best practices, and oversight regarding HIT vendors, their customers, and patients: a report of an AMIA special task force," *Journal of the American Medical Informatics Association,* 2011 18: 77-81

[10] "AAMI Launches Health IT Standards Initiative," AAMI. Aug. 2015. Available: http://bit.ly/297AHbY

WORKFORCE & EDUCATION

A trained informatics workforce, qualified to make systems-level improvements in care delivery using health IT, is necessary to the future of our healthcare system and research enterprise. These Principles and Positions articulate the importance of a well-funded education and training pipeline for informatics professionals, and they identify key policy levers necessary to integrate such professionals within existing workforce structures.

AMIA Believes:

AMIA Policy Principles

The digitization of care delivery is transforming the health and research enterprise; the workforce and educational skills needed to optimize this transformation must include both basic informatics literacy for all health professionals and the option to receive more advanced applied informatics training.

Such a workforce will only be realized with financial support for educational professionals, who advance the science of informatics and train the next generation of informatics professionals.

Based on these Principles, AMIA Supports:

1. Efforts to develop and recognize standardized curricula for health informatics training in specific domains. Ideally, such curricula should be overseen by one or more accreditation bodies, where applicable accreditation bodies exist, so that the current and future healthcare delivery and research workforce has the necessary skillset to advance the learning health system. [1,2,3]

2. Educational and training programs that emphasize the transdisciplinary and socio-technical nature of health IT-enabled care through adequate in-the-field training options for more rigorous programs, to ensure the healthcare workforce is exposed to the cultural and role relationships within and across teams.

3. Efforts to develop basic health informatics training and education for baccalaureate, associate and high school students, so they are exposed to health informatics as a discipline earlier in their academic careers.

4. Federal and state-dedicated funding for informatics training, internships, and apprenticeships, so our health and research enterprises will be supported with a competent workforce.[4,5]

5. Ways to enlarge and sustain advanced formal training for physicians, nurses and other healthcare professionals, such as federal funding for ACGME-accredited Clinical Informatics training programs and advanced degrees in Nursing Informatics, so anticipated shortfalls in workforce are avoided and clinical settings have the experts they need. [6,7]

6. The creation of a designated health informatics Standard Occupational Classification code by the federal government, so accurate employment data can inform public sector decision-making, private sector investment and academic programming.[8]

7. The creation of a designated informatics "expertise code" for NIH consultant files.

[1] Safran C, Shabot MM, Munger BS, Holmes JH, Steen EB, Lumpkin JR, et al. Program Requirements for Fellowship Education in the Subspecialty of Clinical Informatics. *Journal of the American Medical Informatics Association*. 2009;16(2):158-66.

[2] Gardner RM, Overhage JM, Steen EB, Munger BS, Holmes JH, Williamson JJ, et al. Core Content for the Subspecialty of Clinical Informatics. *Journal of the American Medical Informatics Association*. 2009;16(2):153-7.

[3] Silverman H, Lehmann CU, Munger B. Milestones: Critical Elements in Clinical Informatics Fellowship Programs. *Journal of Applied Clinical Informatics*. 2016;7(1):177-90.

[4] Kannry J, Sengstack P, Thyvalikakath TP, Poikonen J, Middleton B, Payne T, et al. The Chief Clinical Informatics Officer (CCIO): AMIA Task Force Report on CCIO Knowledge, Education, and Skillset Requirements. *Journal of Applied Clinical Informatics*. 2016;7(1):143-76

[5] Kannry J, Fridsma D. The Chief Clinical Informatics Officer (CCIO). *Journal of the American Medical Informatics Association*. 2016;23(2):435.

[6] Lehmann CU, Longhurst CA, Hersh W, Mohan V, Levy BP, Embi PJ, et al. Clinical Informatics Fellowship Programs: In Search of a Viable Financial Model: An open letter to the Centers for Medicare and Medicaid Services. *Journal of Applied Clinical Informatics*. 2015;6(2):267-70.

[7] Detmer DE, Munger BS, Lehmann CU. Clinical informatics board certification: history, current status, and predicted impact on the clinical informatics workforce. *Journal of Applied Clinical Informatics*. 2010;1(1):11-8.

[8] Bureau of Labor Statistics, U.S. Department of Labor, "Standard Occupational Classification System" http://1.usa.gov/29003at

DATA SHARING IN RESEARCH

The rapid digitization of care and clinical research has ushered in a new era of data-drive research. These Principles and Positions articulate the role informatics plays in data sharing, and describes the cultural dynamics, institutional support systems, and policy levers necessary to this new era's ongoing evolution.

AMIA Believes:

AMIA Policy Principles

Data sharing among stakeholders is critical to: advance scientific discovery; improve benefit / risk assessments; conduct comparative effectiveness research; improve patient safety; and promote biomedical research rigor, transparency, and reproducibility.

Data sharing should preserve and protect patient and consumer privacy and autonomy.

The science and application of informatics facilitates and improves knowledge gained through data sharing, and should foster a culture of trust and transparency among patients, consumers, researchers, providers, health care organizations, and the vendors and business associates that handle patient and consumer data.

The advantages of data sharing can only be realized with appropriate levels of investment in underlying infrastructure, including tools for managing, storing, and indexing increasingly large and diverse data sets, as well as, human resources for curating shared data.

Based on these Principles, AMIA Supports:

1. Activities that provide, promote and harmonize robust data sharing infrastructures, including hardware, software and data standards so that data sharing efforts are optimized to achieve their stated goals.[1]

2. The implementation of data standards that can be used for consumer- and patient-generated data, electronic health records, and other data that could be useful to informatics researchers to convey summary data in a usable format, individual participant data and

metadata for different types of research to help amplify scientific knowledge while minimizing risks to privacy.[2]

3. Dedicated funding from research sponsors for data curation and sharing efforts so there are sufficient incentives to share, collaborate, and advance data sharing capabilities.[3]

4. Institutional rewards for those who create and/or contribute to public datasets and software that others find useful so that incentives exist for those who create as well as those who analyze data.[4]

5. The creation of harmonized regulatory and/or policy frameworks for data sharing, including: data use agreements; data sharing plans; human-subjects reviews and federal, state and local privacy requirements to minimize barriers to sharing data.[5]

6. Investment in innovative approaches to data sharing involving a range of technical approaches, including sharing of computational resources that might enable computation over data sets that cannot be shared directly due to regulatory or other concerns.[6,7]

7. Data sharing across the translational spectrum, from animal model bioinformatics to human health outcome data.[8]

8. The incorporation of the FAIR data principles (findable, accessible, interoperable and reusable) to optimize the use of resources and data.[9]

9. Efforts to develop evaluation frameworks that assess the value of data sharing and curation.

[1] Examples include: BD2K, CTSA, PCORnet, and BioCADDIE (biocaddie.org)

[2] National Academy of Medicine (formerly Institute of Medicine) "Sharing Clinical Trial Data: Maximizing Benefits, Minimizing Risk," Jan. 2015 http://bit.ly/1Vwtnbi

[3] Borne, P., Lorsch, J., Green, E., "Perspective: Sustaining the big-data ecosystem," *Nature.* November 2015. 527, S16–S17

[4] Piwowar, H., Vision, T., "Data reuse and the open data citation advantage," *Peer J.* 2013. 1:e175

[5] Taichman, D., Backus, J., Baethge, C., et al. "Sharing Clinical Trial Data: A Proposal From the International Committee of Medical Journal Editors," *Annals of Internal Medicine.* 2016. doi:10.7326/M15-2928

[6] Hrynszkiewicz, I., Khodiyar, V., Hufton, A., Sanson, S., "Publishing descriptions of non-public clinical datasets: proposed guidance for researchers, repositories, editors and funding organizations," *Research Integrity and Peer Review.* 2016. 1:6

[7] Examples include: Yale Open Data Access (YODA; http://yoda.yale.edu/); Clinical Study Data Request (CSDR; http://clinicalstudydatarequest.com); and Vivli (http://www.vivli.org)

[8] Velsko, S., Bates, T. "A Conceptual Architecture for National Biosurveillance: Moving Beyond Situational Awareness to Enable Digital Detection of Emerging Threats." *Health Security.* 2016 May-Jun; 14(3):189-201.

[9] "FAIR data principles," The Future of Research Communications and e-Scholarship. Available at https://www.force11.org/group/fairgroup/fairprinciples

HEALTH IT DATA STANDARDS & INTEROPERABILITY

Technical standards enable disparate systems to communicate and are prerequisite for our health IT ecosystem to interoperate. These Principles and Positions describe the desired characteristics of IT standards for care and research. They also articulate the importance of governance, testing, and multistakeholder standards development.

AMIA Believes:

AMIA Policy Principles

Clinical, research and health information technology (HIT) systems must be able to exchange biomedical, clinical, and health data consistently and reliably using computable formats while preserving the intended meaning and relationships.

Access to and reliable use of these electronic data at scale requires that established, consistent, well-published, and openly available HIT standards be used to specify the formats and values for biomedical, clinical, and health data.

To ensure the consistency and comparability of biomedical and clinical data, HIT standards must have coordinated development, open participation, and transparent governance.

Whenever possible, one canonical specification should be designated as the preferred representation for each biomedical, clinical, and health data standard that are required for defined use-cases related to optimizing health and healthcare.

Testing of HIT systems should test both conformance to the standard and interoperability of the standard to ensure data consistency and reliability across implementations.

Based on these Principles, AMIA Supports:

1. The development and management of HIT standards as a public good, operated in a non-profit, non-proprietary basis, with low barriers to review, reference, or use.

2. HIT standards that leverage existing information technology stacks, such as the Internet Protocol Suite,[1] to greatly expand the functionality of existing information systems, and increase the use of HIT standards by disparate systems.

3. HIT standards that are modular and substitutable, having clear boundaries for use and application, with specifications for automated access, use, and integration with relevant data.

4. HIT standards that are simple, parsimonious, and include documentation that is complete, comprehensible, readily available, and timely.

5. HIT standards that are fit for purpose within a declared domain, and clearly recognized and identifiable as the preferred standard. [2]

6. HIT standards that leverage prevailing security practices to protect and preserve privacy and confidentiality.

7. Efforts to recognize and address stakeholder motivations, aims, activities, business models, and information needs in the specification of HIT standards so as to increase the value of their adoption by users and improve ease of implementation.

8. Standards development that incorporates implementation experience and feedback loops from real-world settings to better support an adoption pathway for HIT standards.

9. New modalities of biomedical data, use cases, and information technology that can evolve and mature through implementation experience before canonical specifications can be identified as the standard.

10. Interoperability testing, which tests both the sending of data using a specific standard(s) as well as receipt of data using such standard(s), and tests adherence to Postel's Principle.[3]

11. Adequate funding for the development, management and maintenance of HIT standards, and the SDOs that create them, due to the enormous positive impact on society HIT interoperability can have.

[1] Also known as TCP/IP (https://www.ietf.org/)

[2] This criterion implies being comprehensive within a declared domain of information, purpose and context, and generating verifiable content, preserving provenance, and computer interpretable.

[3] Also known as Postel's Robustness Principle, stating: Be conservative in what you do, be liberal in what you accept from others (often reworded as "Be conservative in what you send, be liberal in what you accept"). Postel, Jon, ed. (January 1980). Transmission Control Protocol. IETF. RFC 761. Retrieved June, 2017.

INFORMATICS-DRIVEN QUALITY MEASUREMENT

The ability to accurately and consistently measure quality and safety of care delivery underlies our national healthcare system. These Principles and Positions describe the characteristics of quality measures in an electronic environment, the governance processes needed to develop such measures, and the public policies needed to ensure that modern quality measures are meaningful to all stakeholders.

AMIA Believes:

AMIA Policy Principles

The purpose of measurement is to improve the quality and safety of care, identify areas for care delivery improvement, and maximize value for patients, for populations, and for the US healthcare system as a whole.

Electronic quality measures should emphasize the use of data available in EHRs, gathered in the routine process of care. Data from other health IT systems may also be required to augment EHR data. Further, data used to compile quality measures should able to be queried in its native environment in a computable and semantically interoperable fashion.

It is not enough that a measure be deemed clinically appropriate for endorsement; the measure should also be demonstrably implementable in the clinical setting, balancing value with provider time required during visits, so that the measure can be collected, reported, and submitted automatically.

Consensus measurement governance and processes must include informatics professionals who are uniquely qualified to ensure that quality measures are clinically meaningful, efficiently integrated in workflow, implementable in an electronic environment, and scalable to address different patient population needs.

Based on these Principles, AMIA Supports:

1. Development of evidence-based quality measures that are aligned with existing data in the care record and can be captured through routine practice without impairing patient-provider communication.

2. Development of evidence-based quality measures that are clinically relevant to providers and meaningful to patients.[4]

3. Clinicians' ability to select among consensus measures that they feel best represent their specialty and patient populations.

4. Evidence-based quality measures that support individualized care, and are flexible enough to facilitate reporting of unique patient experiences as well as patient populations.[5,6,7]

5. A measure development process that is transparent, consistent, inclusive, and includes a parallel quality assurance mechanism to ensure all measures developed through the process are aligned with a holistic strategy.

6. Efforts to simplify quality measure development and streamline quality measure approval processes, including a firm set of selection criteria and strict endorsement processes.[8]

7. Efforts to bring measure developers together with health IT developers, the clinical community, and informatics professionals so that implementation guidelines and best practices accompany quality measures.

8. Efforts to test both the accuracy of the measure calculation, and the feasibility of the data collection requirements, impact on patient-provider communication during visits, to improve the ability to consistently implement the measures.

9. Efforts to leverage quality measure data in ways that are communicated back to the clinician and patients.

10. Programs and policies that increase and prioritize the development of outcome measures, to enable a shift away from process measures.

11. Gradual implementation of reporting requirements to allow for alignment with workflow processes and time requirements.

[4] In a survey reported in Health Affairs, only 27 percent of responding physicians believed that current measures were moderately or very representative of the quality of care they provided. The report also stated that US physician practices are spending $14.5 billion dollars annually – on average about $40,000 per physician to report quality measures that may not have a large impact on health. (Casalino LP, Gans D, Weber R, Cea M, Tuchovsky A, Bishop TF, Miranda Y, Frankel BA, Ziehler KB, Wong MM, Evenson TB. US Physician Practices Spend More Than $15.4 Billion Annually To Report Quality Measures. Health Aff (Millwood). 2016 Mar; 35:401-6.)

[5] Reimagining Quality Measurement. Elizabeth A. McGlynn, Ph.D., Eric C. Schneider, M.D., and Eve A. Kerr, M.D., M.P.H. N Engl J Med 2014; 371:2150-2153December 4, 2014DOI: 10.1056/NEJMp1407883

[6] Patient-Centered Performance Management - Enhancing Value for Patients and Health Care Systems. Eve A. Kerr, MD, MPH1,2; Rodney A. Hayward, MD1,2,3 JAMA. 2013;310(2):137-138. doi:10.1001/jama.2013.6828

[7] Goal-Oriented Patient Care — An Alternative Health Outcomes Paradigm. David B. Reuben, M.D., and Mary E. Tinetti, M.D. N Engl J Med 2012; 366:777-779March 1, 2012DOI: 10.1056/NEJMp1113631

[8] See the NCQA: http://www.ncqa.org/Portals/0/HEDISQM/Measure_Development.pdf

12. Rigorous ongoing monitoring of effectiveness of measures, so that measures remain relevant to practice and patients.[9]

13. The creation of a "safe harbor" status for organizations that utilize their own vetted measurement systems, to advance performance measure development.[10]

[9] The NCQA provides a good model: http://www.ncqa.org/tabid/425/Default.aspx

[10] McGlynn EA, Kerr EA. Creating safe harbors for quality measurement innovation and improvement. JAMA. 2016;315(2):129-30.

POPULATION & PUBLIC HEALTH

As our understanding of health expands beyond the four walls of hospitals, and our conception of what impacts individuals' health grows to include various geographical and social determinants, the need to view populations and public health differently becomes more pronounced. These Principles and Positions are meant to articulate the role of informatics in better understanding the health of populations and facilitate the merging of traditional care delivery with public health.

AMIA Believes:

AMIA Policy Principles

Everyone should have equitable opportunities to live a healthy/healthier life, regardless of who they are, where they live, or socioeconomic circumstances.

When medical, social services, and public health entities work together, everyone benefits.

All U.S. health system stakeholders should be accountable to their communities to assure conditions for a healthy life.

A balance between health care and public health investments should consider the value of preventive community-based services to support individuals to live healthy lives.

A systems- and standards-based approach for addressing social determinants of health and other factors that influence health should be integrated into health system workflows to support improved health outcomes.

Based on these Principles, AMIA Supports:

1. Better (1) integration, (2) interoperability, and (3) bi-directional sharing of data, information, and knowledge across care delivery, public health agencies, and community-based organizations to inform policy, drive prevention and disease management efforts, and support community resource information sharing.

2. Work to develop nationally scalable, multi-jurisdictional approaches to common public health work flows (e.g., electronic case reporting) for broad dissemination.[11]
3. A research agenda focused on (1) developing real-time public health-primary care information loops; (2) improving strategies to engage individuals to assess and promote health (e.g., mobile or virtual technologies); and (3) developing tools to assess social determinants of, and other factors that influence, health.[12]
4. Development of more sophisticated approaches for protecting individual's confidentially while implementing strategies to improve population health outcomes.
5. Investment in public health informatics workforce training to build competencies and capacity at every level where information is generated, managed, and used for population health.[13]
6. The establishment and sustainability of Centers of Excellence for public health informatics to serve as models of best practice for the nation.[14]
7. Dedicated funding for training of public health informatics professionals analogous to NIH funding to ensure the continued evolution of the field.[15]

[11] Digital Bridge Project. Available at: http://www.digitalbridge.us/

[12] Massoudi, B., Goodman, K., Gotham I., et al "An informatics agenda for public health: summarized recommendations from the 2011 AMIA PHI Conference," J Am Med Inform Assoc 2012;19:688e695. doi:10.1136/amiajnl-2011-000507

[13] LaVenture M, Baker B. Developing an Informatics-Savvy Health Department: From Discrete Projects to a Coordinating Program Part II: Creating a Skilled Workforce. J Public Health Manag Pract. 2017 Nov/Dec;23(6):638-640.

[14] Husting EL, Gadsden-Knowles K. The Centers of Excellence in Public Health Informatics: Improving Public Health through Innovation, Collaboration, Dissemination, and Translation. Online J Public Health Inform. 2011; 3(3): ojphi.v3i3.3897.

[15] SHINE Fellows. Available at: http://www.shinefellows.org/

HEALTH DATA PRIVACY

Note: AMIA defines "Health Data" as data collected about an individual – including genetic, phenotypical, physiological, and behavioral data – which provide, or have the potential to provide, information about the physical or mental state of the individual.

The volume, variety, and velocity of health data are rapidly growing across care delivery, research, community, and commercial settings. These Principles and Positions reflect a set of beliefs and actions necessary to support individual privacy within the context of health informatics policy. These Principles and Positions apply wherever and whenever health data exist, including within contexts of health care delivery, clinical research, public health, social/community services, and consumer applications.

AMIA Believes:

AMIA Policy Principles

Health data must be protected to reduce the risks of harm to individuals.

Individuals may benefit themselves and others when they share health data for care and research.

The threat of communicable risk, contaminant risk, and other threats to public health necessitates broad access to health data with severe penalties for misuse.

An individual's privacy protections must be consistently maintained, and their privacy preferences respected across clinical, research, community services, and commercial use of their health data.

Informed consent requires clearly worded, understandable explanations of how an individual's health data will be used and the circumstances in which it will be disclosed; a commercial application Terms of Service agreement is not equivalent to, nor a substitute for, informed consent.

Health data must always be collected, managed, and shared in ways that minimize the risk of reidentification of individuals.

Based on these Principles, AMIA Supports:

1. The regular review and harmonization of federal, state, and tribal privacy policy as technology and society evolve, especially given the expanding use of artificial intelligence (AI) and increasing capacity for data aggregation from diverse sources.

2. Federal privacy policy that lays a foundation for (1) individual data rights and protections; (2) obligations and custodial duties for data owners, managers, and users; and (3) data use prohibitions across jurisdictional and geographic boundaries, while also establishing a process for jurisdictions to address local needs and norms.

3. Federal protections from harassment, targeting, unwanted marketing, bias, discrimination, stigma, and exploitation resulting from use, disclosure, or reidentification of health data.

4. Uniformity of health data access policy, empowering individuals to have complete access to their health data, in machine- and human-readable formats, regardless of covered entity, business associate, or other commercial status.

5. Transparency in how an individual's health data are used or disclosed once collected or generated through clear, easily accessible, and readable explanation of permitted uses.

6. Permissions or consents for data use and disclosure that are accurate, granular, timely, presented in formats that support accessibility by all, understandable across target education levels, revocable, and that are collected from individuals without duress or misleading statements.

7. Development of data standards that can represent and enact privacy policy, such as through tagging (e.g. Security Labels)[16] and metadata (e.g. provenance).[17]

8. Publicly funded research programs that promote responsible data sharing and that seek to be broadly inclusive of diverse and under-represented populations.

9. Explicit accommodation for data access, aggregation, and sharing for purposes of public health.

10. Computable audit trails and accounting of disclosures so individuals can determine who accessed their data, when, and for which purposes.

11. Security systems and controls that protect data in transit and at rest.

[16] A security label is a concept attached to a resource or bundle that provides specific security metadata about the information it is fixed to. See more at: https://www.hl7.org/fhir/security-labels.html

[17] Provenance of data is a record that describes entities and processes involved in producing and delivering or otherwise influencing that data. Provenance provides a critical foundation for assessing authenticity, enabling trust, and allowing reproducibility. Provenance assertions are a form of contextual metadata and can themselves become important records with their own provenance. See more at: https://www.hl7.org/fhir/provenance.html

12. Authentication of individuals and entities and verification of authorization to receive health data before data are shared.

13. Adequate funding for investigation and enforcement of privacy laws, with consequential penalties for individuals and businesses that violate laws and regulations, and with individual redress for harm.

14. Policies that provide individuals the opportunity to securely dispose of, or transmit or download their health data in the event of a transfer of ownership or in the case of a company ending or selling its business.

15. Policies that confer health data protections to non-health data, when non-health data are applied to represent an individual's health and wellness, or when such data are used for purposes of health care delivery, medical research or public health.

16. Ongoing funding for research to develop tools and strategies necessary to minimize the risk of reidentification, increase data privacy and security, and promote data literacy.

ARTIFICIAL INTELLIGENCE PRINCIPLES FOR HEALTHCARE

Artificial Intelligence (AI) refers to an array of computer technologies such as machine learning, deep learning, natural language processing and other mathematical and statistical techniques that simulate human intelligence in order to address highly complex problems, often involving vast quantities of information.

In healthcare, AI systems are generally intended to derive new knowledge, make recommendations or trigger actions via the development of complex algorithms, or processes, that analyze data, often in real or near-real-time, and can sometimes adapt to changes over time. Such systems have the potential to advance medical knowledge and make healthcare safer, more effective, less costly, and even more equitable. There are, however, well documented risks associated with all aspects of the design, deployment and maintenance of AI systems, particularly with respect to the potential for bias in many forms, including algorithmic bias.

As growing numbers of AI systems are deployed in healthcare, the need for ethical principles and governance has become increasingly urgent to assure that AI is introduced judiciously, in the appropriate environments, with appropriate training and maintenance and in accordance with core principles that ensure respect, safety and equity for patients, providers, institutions, and society.

AMIA Believes:

Due diligence is required to address the risk of bias and safety in the use of AI in healthcare, which includes:

- A set of core principles should govern all aspects of design, development, testing, deployment and maintenance of biomedical AI systems, products and services intended to be used in healthcare, as well as in more consumer-oriented health and wellness applications.
- Organizations that deploy or develop AI systems for healthcare should also be governed by a set of principles intended to assure that issues related to the context of use, maintenance over time, and other implementation issues are addressed.
- Development and deployment of AI systems in healthcare should proactively seek to mitigate the potential un-intended socio-cultural impact of such systems with particular emphasis on education, research, and the impact on vulnerable populations, including groups that have been economically/socially marginalized.
- Guidelines for implementation of the principles outlined herein should offer appropriate mechanisms to assess the degree to which an AI system adheres to them, with particular emphasis on principles that may represent or require a value judgement.

Based on these Principles, AMIA Supports:

AI Systems Principles

1. Autonomy - AI must protect the autonomy of all people and treat them with courtesy and respect including facilitating informed consent.
2. Beneficence - AI must be helpful to people modeled after compassionate, kind, and considerate human behavior.
3. Non-maleficence - AI shall "do no harm" by avoiding, preventing, and minimizing harm or damage to any stakeholder.
4. Justice - AI includes equity for people in representation and access to AI, its data, and its benefits. AI must support social justice.
5. Explainability - Scope, proper application, and limitations of AI must be understandable and provided in context appropriate language.
6. Interpretability - Plausible reasoning for decisions or advice in accessible language must be provided.
7. Fairness – AI must be free of bias and must be non-discriminatory.
8. Dependability - AI must be robust, safe, secure, and resilient. Failure must not leave any system in an unsafe or insecure state.
9. Auditability - AI must provide and preserve a performance "audit trail" including internal changes, model state, input variables, and output for any system decision or recommendation.
10. Knowledge Management - AI systems must be maintained including retraining of algorithms. AI models need listed creation, re-validation, and expiration dates.

Principles for Organizations Deploying or Developing AI

11. Benevolence - Organizations must be committed to use AI systems for positive purposes.
12. Transparency - AI must be recognizable as such or must announce its nature. AI systems do not incorporate or conceal any special interests and deal even-handedly and fairly with all good faith actors.
13. Accountability - attributed to AI must be reported, assessed, monitored, measured, and mitigated as needed. Complaints and redress must be guaranteed.

Principles to Address Special Considerations

14. Vulnerable Populations – AI applied to vulnerable populations requires increased scrutiny and appropriate community involvement to avoid worsening the power differential among groups
15. AI Research – continued research into AI is required
16. User Education - Developers of AI have a responsibility to educate healthcare providers and consumers on machine learning and AI systems.

Selected References

Solomonides AE, Koski E, Atabaki SM, Weinberg S, McGreevey JD, Kannry JL, Petersen C, Lehmann CU. Defining AMIA's artificial intelligence principles. J Am Med Inform Assoc. 2022 Mar 15;29(4):585-591. doi: 10.1093/jamia/ocac006. PMID: 35190824; PMCID: PMC8922174.

Embi PJ. Algorithmovigilance—Advancing Methods to Analyze and Monitor Artificial Intelligence–Driven Health Care for Effectiveness and Equity. *JAMA Netw Open*. 2021;4(4):e214622. doi:10.1001/jamanetworkopen.2021.4622

Buolamwini J, GebruT. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Available online at https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Last accessed 8/27/2021.

Hogan NR, Davidge EQ, Corabian G. On the Ethics and Practicalities of Artificial Intelligence, Risk Assessment, and Race. J Am Acad Psychiatry Law. 2021 Jun 3:JAAPL.200116-20. doi: 10.29158/JAAPL.200116-20. Epub ahead of print. PMID: 34083423.

Matheny ME, Whicher D, Thadaney Israni S. Artificial Intelligence in Health Care: A Report From the National Academy of Medicine. JAMA. 2020 Feb 11;323(6):509-510. doi: 10.1001/jama.2019.21579. PMID: 31845963.

McGreevey JD 3rd, Hanson CW 3rd, Koppel R. Clinical, Legal, and Ethical Aspects of Artificial Intelligence-Assisted Conversational Agents in Health Care. JAMA. 2020 Aug 11;324(6):552-553. doi: 10.1001/jama.2020.2724. PMID: 32706386.

Nordling L. A fairer way forward for AI in health care. Nature. 2019 Sep;573(7775):S103-S105. doi: 10.1038/d41586-019-02872-2. PMID: 31554993.

Obermeyer Z, Powers B, Vogeli C, Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019 Oct 25;366(6464):447-453. doi: 10.1126/science.aax2342. PMID: 31649194.

Petersen C, Smith J, Freimuth RR, Goodman KW, Jackson GP, Kannry J, Liu H, Madhavan S, Sittig DF, Wright A. Recommendations for the safe, effective use of adaptive CDS in the US healthcare system: an AMIA position paper. J Am Med Inform Assoc. 2021 Mar 18;28(4):677-684. doi: 10.1093/jamia/ocaa319. PMID: 33447854.

World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. Geneva: 2021. Licence: CC BY-NC-SA 3.0 IGO.