The future of health IT innovation and informatics: a report from AMIA's 2010 policy meeting

Julie J McGowan,[1] Caitlin M Cusack,[2] Meryl Bloomrosen[3]

[1]Knowledge Informatics and Translation, Indiana University School of Medicine, Indianapolis, Indiana, USA
[2]Insight Informatics, Manchester, New Hampshire, USA
[3]AMIA, Bethesda, Maryland, USA

Correspondence to
Meryl Bloomrosen, Public Policy and Government Relations, AMIA, 4720 Montgomery Lane Suite 500, Bethesda, MD 20814, USA; meryl@amia.org

ABSTRACT

While much attention has been paid to the short-term impact that widespread adoption of health information technology (health IT) will have on the healthcare system, there is a corresponding need to look at the long-term effects that extant policies may have on health IT system resilience, innovation, and related ethical, social/legal issues. The American Medical Informatics Association's 2010 Health Policy Conference was convened to further the national discourse on the issues surrounding these longer-term considerations. Conference participants self-selected into three broad categories: resilience in healthcare and health IT; ethical, legal, and social challenges; and innovation, adoption, and sustainability. The discussions about problem areas lead to findings focusing on the lack of encouragement for long-term IT innovation that may result from current health IT policies; the potential impact of uneven adoption of health IT based on the exclusions of the current financial incentives; the weaknesses of contingency and risk mitigation planning that threaten system resilience; and evolving standards developed in response to challenges relating to the security, integrity, and availability of electronic health information. This paper discusses these findings and also offers recommendations that address the interwoven topics of innovation, resilience, and adoption. The goal of this paper is to encourage public and private sector organizations that have a role in shaping health information policy to increase attention to developing a national strategy that assures that health IT innovation and resilience are not impeded by shorter-term efforts to implement current approaches emphasizing adoption and meaningful use of electronic health records.

INTRODUCTION

Since 2006, the American Medical Informatics Association (AMIA) has convened an annual Invitational Health Policy Meeting to examine cutting-edge issues in healthcare and health-information technology (health IT) policy. The overarching objective of each meeting has been to identify potential future issues, especially those related to the convergence of health IT, clinical technologies, devices, innovations, and communications capabilities; identify areas for further study and research; and develop objective reports synthesizing conference outcomes to inform policymakers about the issues discussed and potential next steps. Previous meetings have focused on unintended consequences of health IT and policy; informatics-enabled evidence-based care; and development and advancing of a national framework for health data use. Outcomes of each meeting include a summary report with recommendations published in *JAMIA*, and a short-range action/research plan that can be pursued by the participants to address the issues discussed. As described in this paper, AMIA's 2010 Health Policy Meeting focused on several long-term challenges to healthcare and health IT resilience, innovation, and adoption that may result from current US policy initiatives.

BACKGROUND AND SIGNIFICANCE

In 2001, the Institute of Medicine outlined a vision of 21st-century healthcare, that is, safe, effective, patient-centered, timely, efficient, and equitable. Many aspects of this vision involve information technology, such as tools that collect and organize comprehensive data on patients, and systems that help providers integrate evidence into practice, and highlight problems as they arise.[1] A decade later, the healthcare environment and health IT continue to evolve. A national imperative exists to improve healthcare delivery and reduce related costs. The US government is investing considerable resources to broaden the reach of health IT in general and electronic health records (EHRs) in particular. The force behind much of this rapid change has been the health IT stimulus provisions of the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health (HITECH) legislation. These policy vehicles, which include financial incentives aimed at spurring broader health IT adoption, have the US healthcare sector poised on the brink of wide-scale implementation of health-information systems to support patient care. At the same time that health IT adoption and innovation are being widely promoted, new models for care delivery and financing, such as accountable care organizations (ACOs) and health insurance exchanges, have been proposed and are being debated.

Todd Park, Chief Technology Officer of the US Department of Health and Human Services (DHHS), said in a 2011 interview, 'There has never been a better time to be an entrepreneur—an innovator at the intersection of healthcare and IT.'[2] Isaac Kohane, one of the leaders of a project to encourage health IT innovation through the Office of the National Coordinator for Health Information Technology (ONC), noted that 'There is an enormous talent pool available in our country's developers and entrepreneurs to help drive new web and mobile health IT solutions that support healthcare functions.'[3]

Discussions about innovation, resilience, sustainability, and related ethical, legal, and social challenges, including those from public policy and technological perspectives, can be found in the

literature regarding the healthcare domain, as well as in other fields.[4–13] One of the drivers of current discussions is the abundant advances in science, technology, and medicine that hold promise for improved disease diagnosis and treatment. The mapping, sequencing, and analysis of the human genome are expected to allow us to identify which patients will respond to specific treatments; stem cells offer the possibility of regenerating tissues and organs; nanotechnology and new biomaterials are allowing the creation of smaller, more effective devices and implants; microelectronics, robotics, navigation techniques and new imaging modalities are offering more potent and focused approaches to diagnosis and treatment; and the convergence of devices, drugs, biologics, and diagnostics is creating new possibilities for prevention, treatment, and cure of chronic diseases. In the data-management sphere, an increasing number of businesses and organizations, including the federal government, are putting more data and processes online. With the continued emergence of next-generation web and wireless technologies, we are likely to see increasing levels of online collaboration and information sharing. However, technology innovations, medical discoveries and technical advances—from the networks themselves to the information stored in computer databases and other applications—are outpacing, and in some cases blurring the lines between, the technologies and the policies, rules, and regulations that address them.

In addition to technological breakthroughs, major new care delivery and payment initiatives under consideration are leading to questions about the US healthcare system's long-term ability to adapt to changes, maintain resilience under pressure, continue to foster innovation, and in general build a healthcare workforce and infrastructure that will be able to safely and ethically integrate these significant systemic changes. These concepts require further exploration and management of expectations.

Resilience in healthcare and health IT
The US healthcare system is at a critical point, beset by increasing costs and pressures to improve healthcare quality and patient safety. The rapid deployment of health IT as currently mandated raises the possibility of unintended negative consequences and even implementation failures. To ensure continuity in the face of threats that could affect the stability of the overall healthcare system and, specifically, impact the viability of health IT implementations, it is essential to focus attention on those factors that bolster system resilience. Robust plans and policies are needed to facilitate preparedness and response, and roles for key stakeholders need to be defined to guide and enforce policies mitigating unintended consequences of such rapid deployment.

Ethical, legal, and social challenges
Such challenges will likely arise in response to changing technologies; for example, new technologies and information exchanges could affect ethical decision-making, either facilitating or reducing healthcare fraud. With the mandate for meaningful use (MU) of health IT by providers, there is ample opportunity for inappropriate and even fraudulent or illegal activities, ranging from lack of oversight to deliberate misrepresentations.

Innovation, adoption, and sustainability
Although a number of new funding models will exist to address the intersection of health IT and new forms of healthcare delivery, it is unclear what their impacts may be on the broader adoption and sustainability of health IT, especially among communities and stakeholders not reached by current funding models. Further, the desire by stakeholders to meet short-term requirements, such as those defined by regulations specifying MU requirements, may come at the expense of long-term innovation.

As stakeholders grapple with the daily challenges posed by a rapidly changing healthcare and health IT landscape, AMIA's 2010 Health Policy Meeting took a longer-term look at the situation to examine how close current plans and efforts can get us to the Institute of Medicine's vision of 21st-century care, and how, in fact, progress in adoption, system resilience, and innovation may be threatened by today's public-policy climate.

STRATEGY: AMIA'S 2010 HEALTH POLICY MEETING
AMIA's 2010 Health Policy Meeting explored the many facets of the tensions between shorter-term efforts to drive health IT adoption, supported largely by ARRA/HITECH legislation, and longer-term policy strategies needed to assure continuing innovation, resilience, and sustainability in health IT. Participants met on 1–2 September 2010, in the metropolitan Washington, DC area. In the months leading up to the meeting, a steering committee of a small group of AMIA members and subject-matter experts was convened. Led by the Chair of AMIA's Public Policy Committee, co-chaired by a member of the Public Policy Committee, and assisted by AMIA Policy Staff, the committee set goals, prepared the meeting agenda, and made suggestions about discussants, presenters, and attendees. The nearly 75 attendees included representatives from various segments of the health IT field including providers, technology vendors, pharmaceutical companies, consulting firms, researchers, government agencies, and consumer stakeholders. Background information, hypothetical scenarios, and discussion questions were provided to participants in advance of the meeting to help inform the discussions.

Plenary sessions laid out many of the key issues. John Glaser, Siemens Healthcare, and former consultant to the ONC, launched the meeting with the opening plenary, challenging participants to consider multiple factors in the future of health IT including technologies, financing options, and organizational issues. Linda Connell, Director of NASA's Aviation Safety Reporting System, drew parallels between the Aviation Safety Reporting System and evolving health IT patient safety and adverse-events reporting. Ethical and legal issues that could be by-products of rapid health IT implementation were raised in a presentation by Kenneth Goodman, director of the University of Miami Bioethics Program. A provocative presentation by William Barker, Chief Cybersecurity Advisor, NIST Information Technology Laboratory, focused on information-security issues in the healthcare field, outlining gaps in current research related to cybersecurity, particularly as related to cloud-computing applications.

Plenaries were followed by facilitated breakout discussions, designed to help participants focus ideas, summarize results, and formulate action items. Careful consideration of complex issues was encouraged by facilitators at these sessions, during which participants focused on resilience in healthcare and health IT; ethical, legal, and social challenges; and health IT adoption and innovation. A debate among senior health IT leaders, entitled 'Stifling of Health IT: Informatics Research and Innovation,' was a meeting highlight. Debaters included Drs John Halamka, Don Rucker, Don Detmer, and Randy Miller; they argued for and against the following statement: 'recent increases in HIT funding, public awareness, and federal policy, if sustained, are sufficient to enable vibrant informatics research and development efforts that will assure innovation and progress in clinical

informatics for the future of health and healthcare.' The side in favor of the proposition argued that momentum toward adoption would sustain and support innovation, while the opposing side argued that innovation would not be fostered through federal mandates, regardless of the good intentions of policies and funding priorities.

FINDINGS: IMPACTS OF POLICY AND FUNDING CLIMATE ON HEALTH IT AND THE HEALTHCARE SYSTEM

Conference participants focused on the ways in which current public policy, financing, and market trends are affecting the overall healthcare system and, specifically, their impact on health IT innovation, adoption, and resilience. Key discussion points that surfaced during plenaries and were debated in breakout sessions are briefly outlined below.

Failures and risk mitigation

Rapid deployment of any new technology is subject to a variety of unintended consequences. Funding under ARRA and earlier policies that have promoted health IT adoption have done so without identifying and mitigating a number of potential problems common to all health IT deployments. This lack of attention has laid the foundation for a number of possible minor and even major failures (eg, catastrophic EHR failures, floods or other natural disasters that cause infrastructure failures, or even health IT organizational failures that might result in death) that threaten to undermine the major benefits that health IT can provide. Recognition of these potential problems and development of plans to mitigate the impact were considered of paramount importance.

Managing expectations and potential loss of public trust

Former ONC Director, David Blumenthal, wrote in a 2010 article, 'The HITECH Act's programs strive to create an electronic circulatory system for health information that nourishes the practice of medicine, research, and public health, making healthcare professionals better at what they do and the American people healthier.'[14] The ONC website articulates numerous specific expectations for health IT.[15] Concern has been expressed that all of the expectations for health IT will not be realized as promised,[16] that the health IT community, including providers, vendors and patients, is not ready for the rapid and comprehensive nature of current regulatory requirements. Further, upcoming technology developments and transitions may cause disruptions in care and security challenges that could result in the loss of public trust, a loss that may extend beyond the government to healthcare institutions and even providers.

Uneven adoption of health IT

Concerns were raised that inconsistency of health IT adoption, in part based on lack of implementation funds available to subsets of providers, may lead to implementation silos, polarization of the healthcare environment, and inability of some stakeholders to participate in future health information exchanges (HIEs). With its focus on hospitals and selected eligible providers, ARRA legislation excludes incentive funding for medical specialties that serve targeted patient groups (eg, pediatrics) and for those whose focus is population health, public-health infrastructure, community health, and health education. Thus, important population-based and chronic conditions that pose serious health challenges, such as obesity, may not be successfully addressed, resulting in missed opportunities to address health problems that drive up costs.

Organizational/workforce issues

If human-resources issues related to health IT implementation are not addressed, the systems will not work. This applies to training, workforce support, organizational resilience, and user-centric software. Health IT adoption impacts operational workflow in situations where heathcare organizations are already overstressed. Training is critical to support the workforce; current ONC-sponsored training efforts[17] aimed at adoption and MU of EHRs, may be inadequate. Core competencies of EHR users across various settings are currently poorly defined, thus making it difficult to set up robust training programs, and it is unclear how these training and workforce development programs will be implemented, monitored, and evaluated. Nor is it clear how projected workforce shortages will be addressed. Approaches to provide continuing education for training-program graduates and for the current workforce are inadequate.

Concerns about implementation speed and interoperability

The rapidity of health IT implementation under ARRA/HITECH is another challenge to the overall healthcare system. Health IT acquisition, implementation, and maintenance costs are high, and investments must be made very quickly in order to receive federal incentive payments. This could provide fertile ground for both fraud and failures. Obstacles impede implementation of widespread system interoperability. For example, current market structure discourages cooperation among various stakeholders with perverse incentives arguing against the interoperability. Market reform is needed to strengthen the overall healthcare system. Further, initial DHHS certification requirements for EHRs did not include the explicit criteria for interoperability that could help propel forward movement in this challenging area.[18]

Lack of encouragement for long-term IT innovation

Current and contemplated models for financing health IT in the US primarily take the form of MU incentives and subsidies for new forms of healthcare delivery. There is the potential that current DHHS efforts, largely focused on short-term adoption, could be putting innovation and further advancements in health IT at risk. This is possible because vendors are likely to focus on assuring that their EHRs meet MU criteria, putting aside other types of research and product development; and because the increase in those adopting EHRs will put more strain on an already-stretched implementation workforce[19] resulting in the redirection of funding to meet these pressing workforce needs. On our current trajectory, the ARRA/HITECH funding incentives may have the unintended effect of impeding true technological innovation in healthcare and health IT.

Tension between federal and state roles

Clarity and coordination are lacking regarding state and federal roles in the area of health IT implementation, with tension existing between state and federal governments as to responsibilities, regulations, and funding. The federal government has awarded major contracts to the states to ensure continuity of linking health IT systems. However, without explicit guidelines, proprietary state systems may be created, with many not being able to connect to the national health information infrastructure and some not acknowledging the healthcare systems that cross state lines. These issues are magnified by different state requirements for protected health information and other macro issues resulting from complexities of healthcare delivery across state boundaries.

DISCUSSION: RECOMMENDATIONS

The meeting was organized around three major topics: resilience in healthcare and health IT; ethical, legal, and social challenges; and innovation, adoption, and sustainability. Specific recommendations on these topics that resulted from the meeting discussions and were subsequently enhanced by postmeeting review, analysis, and syntheses are outlined below. However, some discussions either crossed the three topic areas or could not be categorized into one of them; recommendations from these discussions are listed at the end.

Resilience in healthcare and health IT

Current contingency plans are insufficient to serve as the basis for rapid, effective responses in the event of a major health IT infrastructure disaster or a natural or man-made catastrophic event.

Healthcare is a complex socio-technical system, and it is the nature of such systems that failures and other undesirable outcomes may be unavoidable.[20–22] Resilience has been defined as the 'intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances so that it can sustain required operations, even after a major mishap or in the presence of continuous stress.'[23] It is an attribute that should be on the minds of all stakeholders in the US healthcare system—providers, researchers, thought leaders, policymakers, and consumers—especially as billions of dollars begin to flow into the healthcare sector for the purpose of speeding the adoption of EHRs, HIEs, and other forms of health IT.

The Gulf oil spill, Hurricane Katrina, and the 2011 earthquake/tsunami in Japan provide stark reminders that major disasters are always possible, even if the risk of occurrence is small. A recent US Government Accountability Office report emphasized the ongoing need for efficient sharing of real-time information to help prevent or mitigate the consequences of public-health emergencies. The report cites concerns about DHHS progress in formulating a strategic plan for the establishment and evaluation of a nationwide, electronic, public-health situational awareness capability collaboration with state, local, and tribal public-health officials, noting that a catastrophic public-health event could threaten our national security and cause hundreds of thousands of casualties.[24]

Meeting participants discussed the potential for, and ramifications of, inadequacies or failures of current contingency planning approaches to health IT, along with ways to support more robust plans and policies focused on preparedness and response. As the public and private sectors move forward to adopt health IT, comprehensive national strategic plans and programs *beyond* those for public-health emergencies and initiatives will also be needed.

In general, state and federal budgets fail to provide funds to support the ongoing maintenance and growth of health IT and the overall health-system infrastructure. The return on investment on these efforts is not always well understood and thus difficult to demonstrate. New funding models need to be created and disseminated to address these issues. Health-system stakeholders can play key roles in recognizing the importance of contingency planning to ensure the ability of systems to rebound after a catastrophe, and in establishing, following, and enforcing the policies needed to support resilient health IT systems.

Specific recommendations include:

► Risks of new technologies should be identified on an ongoing basis and mitigated. Risks and shortcomings of new and evolving technological approaches such as cloud computing need to be acknowledged and explored. Methods of addressing and mitigating those risks need to be implemented before such approaches are widely adopted as part of health IT implementation.

► System performance and software need to be monitored for unintended consequences, and problems should be reported. Healthcare organizations are not currently sharing information about system performance and software reliability or shortcomings, nor lessons learned with regard to health IT implementations. Transparency, quality assurance, oversight control, and ongoing technical support for users are needed to identify and remedy software problems that arise. There is also an ongoing need to identify mechanisms to encourage users to collect and share these lessons. To help meet that need, the National Quality Forum, under contract to the Agency for Healthcare Research and Quality (AHRQ), has released a new Common Format designed to help healthcare providers collect information about adverse events related to health IT.[25] Payment-oriented demonstration projects sponsored by the Centers for Medicare and Medicaid Services (CMS), such as patient-centered advanced primary care practices[26] and/or medical homes, as well as efforts to establish ACOs must consider and address unanticipated and unintended consequences of health IT related to such new models of care.[27–29]

► Planning for risk mitigation, interoperability, and lifecycle funding needs to be a high priority. Plans for disaster management/preparedness by healthcare systems are inadequate. Lessons from recent events such as Hurricane Katrina and the Haiti earthquake need to be reviewed. The success of health IT, particularly in times of system stress such as disasters, is in part dependent on the availability and resilience of available sources of power and telephone systems. Backup systems need to be robust and immediately available to maintain a 'paperless' health-system environment. Linkages among hospitals need to be strengthened or created to promote effective disaster management, particularly in terms of health IT systems. HIEs could potentially provide some solutions for backup capacity; policies are needed to promote interoperability to support system resilience and emergency response.[30–32] Research is needed to examine existing risk mitigation and disaster-planning approaches in general, and specifically to determine to what extent such plans consider health IT needs (eg, the role of EHRs). Key federal agencies such as the Centers for Disease Control and Prevention (CDC) and AHRQ, and private sector organizations such as the American Hospital Association and the American Group Practice Management Association should make recommendations to all stakeholders for ensuring that their disaster plans adequately support EHRs and health IT. Beyond specific risk-mitigation planning, lifecycle funding as an essential component of system sustainability needs to be addressed with new funding models created to ensure that health IT remains a viable component in supporting improved quality of care and patient safety.

► New approaches are needed to predict system failures. The increasing complexity in highly technological systems such as aviation/air traffic control, maritime, telecommunications, nuclear power plants, space missions, and the chemical and petroleum industry, as well as healthcare and patient safety, is leading to potentially disastrous failure modes and new kinds of safety issues. Traditional accident modeling approaches are not adequate to analyze accidents that occur in modern socio-technical systems such as healthcare, where

accident causation is not the result of an individual component failure or single human error.[33–37] Additional research is needed to further develop risk-mitigation approaches to deal with system failures. DHHS and other agencies should accelerate existing efforts to identify and apply approaches for anticipating and mitigating risks from large-scale failures including those due to technical, natural, or man-made disasters. While there is an increasing body of literature on the role of health-information systems and technology in terms of assisting during disasters, there seems to be less known about how health systems can prepare for the disasters themselves.[38 39]

Ethical, legal, and social challenges

There are new and evolving legal, social, and ethical challenges and risks from more widespread adoption and use of health IT, especially involving EHRs, personal health record, wireless and mobile devices, and telehealth applications.

Changing technology is affecting ethical decision-making, with a growing array of ethical, legal, and social considerations confronting clinicians, patients, providers, and policymakers. There is a heightened need to address how these issues should be approached by policymakers. The AMIA Board of Directors appointed a Task Force on the topic whose recommendations include the following:

> patient safety should trump all other values; corporate concerns about liability and intellectual property ownership may be valid but should not over-ride all other considerations; transparency and a commitment to patient safety should govern vendor contracts; institutions are duty-bound to provide ethics education to purchasers and users, and should commit publicly to standards of corporate conduct; and vendors, system purchasers, and users should encourage and assist in each others' efforts to adopt best practices. Finally, the Task Force concluded that the HIT community should re-examine whether, and how, regulation of electronic health applications could foster improved care, public health, and patient safety.[40]

Policymakers believe that the Patient Protection and Affordable Care Act[41] will help improve and expand consumer protections, strengthen Medicare, and reduce healthcare costs—for example, by improving government-wide efforts to fight fraud and waste. The law contains some important new tools (eg, Health Care Fraud and Abuse Control Account) to improve the federal government's efforts to prevent, detect, and take strong enforcement action against fraud in Medicare, Medicaid, and the Children's Health Insurance Program, as well as in private insurance. The Patient Protection and Affordable Care Act also allows these funds to support the hiring of new officials and agents that can help prevent and identify fraud.

However, it is not clear that the status quo will be able to keep up with new developments. For example, there may be new liability exposures that result from current MU incentives for greater and more widespread adoption of health IT. It is possible that new or revised regulations may be needed to address potential shortcomings as the industry witnesses ongoing convergence of previously disparate technologies and data sources. It may be important to reconcile ethical practices with the increasingly digital and technology-supported delivery of healthcare. Additionally, the increasing and more direct role of consumers in their healthcare (eg, through home monitoring and disease-management programs) may increase risks and challenges not yet foreseen or addressed by existing legal, ethical or moral practices, rules, or guidances.

Specific recommendations include:

▶ Meaningful use (MU) should require formal attestation. New or revised monitoring and auditing requirements are needed to track appropriate attestation of MU. Given the initial reliance on self-reported MU compliance, it appears that guidelines to assure accurate interpretation of reporting requirements are needed. Ongoing monitoring of the validity of MU compliance seems prudent. Such processes could be incorporated into existing fraud and abuse compliance and monitoring activities such as those performed by CMS for coding and billing accuracy (Recovery Audit Contractor audits) and the Office of Civil Rights for HIPAA privacy, security, and confidentiality requirements.

▶ Unforeseen challenges involved with technology use, new healthcare delivery approaches, and changes in roles should be envisioned and addressed. Consideration should be given to possible challenges and risks resulting from the increasing role of broadband and wireless technologies in supporting health-care delivery. Other issues may result from the implementation of new or refined provider organizations, such as ACOs. In addition, potential problems may arise resulting from the direct role consumers could play in medical monitoring and chronic disease management.

▶ Review of existing security regulations is needed. The Office for Civil Rights, responsible for issuing periodic guidance on the HIPAA Security Rule provisions (45 C.F.R. §§ 164.302–318), has issued a series of guidance documents to assist organizations in identifying and implementing administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic health information. The extent to which these guidances have been adopted or are sufficiently effective is unclear, particularly in light of new technologies and evolving security and privacy standards. With the increasing array of devices and technologies available for use, it is unclear how or if entities that are not currently covered under HIPAA can be held accountable to the evolving standards.[42 43]

▶ Identity management and authentication issues need to be addressed. New electronic medical devices used by or implanted in patients are among the technologies increasing the urgency in work related to identity management, authentication, and cybersecurity. For example, wireless pacemakers can now transmit data to a smart phone or computer system and directly into an electronic health record. While there is a growing marketplace of vendor solutions and methods dealing with identity management and authentication issues, it is not clear what the longer-term risks and solutions may be in this multidisciplinary area involving technical, legal, privacy, security, and organizational factors.[44] Recent federal efforts to explore these issues include a 2010 report of the President's Council of Advisors on Science and Technology, *Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward*.[30] Authentication technologies, rules, standards, services, and policies should be in place across the public and private sectors. Additional research is needed to help stakeholders identify and solve future problems in this arena.

Innovation, adoption and sustainability

The current state of adoption and use of available EHR systems is not adequate to assure the long-term, successful attainment of high-quality care throughout the US, much less support the innovation, that is needed to ensure the next generation of health IT.

The rapid growth of health IT is transforming the delivery of healthcare, and more health information than ever is available today for use by providers, payers, researchers, and patients. Fueled largely by aggressive public and private health IT initiatives and supported by targeted federal and state funding, this evolution holds much promise for improvements in healthcare quality and outcomes. But the transformation also brings with it numerous new challenges. Gaps and disparities in adoption along provider and geographic lines exist. In the implementation of health IT, for example, there is an uneven distribution due to a lack of incentives for certain specialties and provider types not covered by ARRA. Many believe that, despite regional extension centers and other federal efforts, emphasis has been placed on larger, more 'advanced' practices. Currently, available health IT models and tools may be less well suited for providers in rural areas, where access to broadband, needed to facilitate health IT adoption and use, may be limited or prohibitively expensive. Other factors leading to implementation issues include the rapid pace of the ARRA implementation schedule and the lack of demand for health IT applications by patients due to their lack of awareness of their benefits.

With respect to the overall healthcare system, several payment initiatives are under way to address new forms of care delivery, such as ACOs and Patient-Centered Medical Homes. There are uncertainties about how future financing options can accommodate these and other evolving forms of healthcare practice and delivery, sites of care and/or technologies.[45–47] It is not clear what impacts new models of care may ultimately have on the broader adoption of health IT, especially among communities and stakeholders that the current funding models do not reach. Payment and coverage policies as well as efforts to establish health IT-related performance or quality measures also need to be in sync. To drive gains in quality and efficiency, simply adopting EHRs is unlikely to be sufficient. Instead, policies are needed that encourage the use of EHRs in ways that will lead to improvement.[48]

Specific recommendations include:

▶ Incentives for HITECH implementation should be broadened beyond the current recipients, and the implementation schedule lengthened. The federal government should accelerate the consideration of financial incentives for eligible providers and organizations not currently identified for MU incentive payments (eg, other medical specialties). Also, consideration should be given to lengthening the timeline for the federal implementation schedule to allow for additional providers to come on board, as well as to ensure that systems are viable and that users are adequately trained. Evaluation and monitoring of early stages of MU implementation should be considered as later stages are rolled out.

▶ Innovation in health IT needs to be driven by optimum healthcare. Quality care delivery needs should be the primary driver of innovation in health IT rather than the pursuit of incremental advances in technology or broader adoption alone. Current health IT applications have focused on automating medical care as practiced and may be too limited in supporting innovations in care that could promote improvements in outcomes and efficiencies. Innovation should also be driven by changes in federal and state reimbursement policies such as new pay for performance models, as well as customer expectations. CMS is examining new ways of delivering healthcare and paying providers that can save money for Medicare and Medicaid, while improving the quality of care. CMS demonstration projects that support efforts to better coordinate care and improve health outcomes

should more explicitly consider health IT and related technologies and solutions.

▶ Patients should be involved in promoting the use of health IT as a critical component of healthcare delivery. Engaging patients in the health IT value/benefit discussion could contribute to consumer-driven demand as expectations grow for the healthcare system to provide the automated convenience offered by other consumer services. Patient education and awareness programs regarding the potential benefits of health IT should be implemented to help generate this demand.

OTHER FOCUSED RECOMMENDATIONS
Health IT terminology
The federal government should facilitate the development of standardized terminologies that will promote interoperable health IT.

As health IT continues to play an increasing role in healthcare planning and delivery, it is becoming increasingly important that stakeholders (including consumers) have a shared understanding of what key terms mean. As noted in a 2008 report by the National Alliance for Health Information Technology to the ONC:

> The ambiguity of meaning created by not having a shared understanding of what these key terms signify becomes an obstacle to progress in health IT adoption when questions about a term's definition and application complicate important policy expectations or directives, contractual matters, and product features.[49]

Specific recommendation:

▶ Health IT terminology needs to be refined and standardized. There is a need to harmonize the various terms used to describe health IT to clarify their application by research and practice communities. The widespread use of terms such as e-health, m-health, EHRs, personal health records, telehealth, and mobile health, among others, is increasingly confusing to stakeholders. There are various approaches to defining and using the terms. Public and private sector organizations should collaborate to build consensus around working definitions of key terms related to evidence-based medical computing. As appropriate, DHHS agencies should refine and adjudicate definitions and terms related to health IT and their use in federal rules and regulations.

Evaluation of health IT implementations
The federal government should allocate resources to evaluate health IT implementation strategies as well as the overall safety of systems purchased with or reimbursed by federal funds.

Achieving 'safe use of health IT' will require not only the provision of opportunities for health IT users to report events related to health IT use, but also the training of users for full and effective use of these systems. It will require developing the clerical, administrative, clinical, and technical expertise and workforce necessary to support a healthcare enterprise built on, and supported by, electronic platforms. Additional efforts will be needed to address issues of design safety, change implementation, and error monitoring and reduction. Safe use of EHRs depends on a professional and clinical workforce, that is, increasingly attuned to the potential of health IT in clinical care, health promotion, and public-health monitoring as well as the potential challenges and pitfalls of its expanded use. Clarity with regard to federal versus state roles in fostering and monitoring health IT implementations is also needed.

Specific recommendations include:

- Use evidence to guide implementation. Implementation of health IT and relevant federal initiatives should be based on the evidence base. Comparative effectiveness research of various health IT alternatives, technologies, and approaches should be conducted. Health IT implementations should be monitored to identify barriers, challenges, and risks. Key organizations such as AHRQ and the National Library of Medicine need additional resources to assess whether the promise of health IT adoption and MU is being achieved, and to disseminate the results of such studies.

- Attention needs to be given to human—computer interaction (HCI). Additional research is needed to improve the human—computer interaction aspects of existing and new systems and applications, in order to ensure the safe and successful implementation and use of health IT. Although there are some recent federally sponsored efforts addressing usability issues,[50] such efforts must reflect the most current research and science about usability to ensure that providers attempting to achieve MU have effective systems that support their efforts.

- Trained healthcare workforce is essential to implementation success. A nationwide approach to help assure the ongoing sustainability of the healthcare workforce and the incorporation of the requisite knowledge, skills, and experience to maintain and support EHR systems once deployed is essential.[51–53]

- Clarity is needed on federal/state roles. Within DHHS, a coordinating effort needs to be established to ensure that health IT initiatives that cross federal and state government initiatives are in concert, and not competing against each other or overlapping, resulting in unwise spending of funds. More study is also needed to better understand the impediments to innovation (eg, limits to information sharing, certification requirements, etc) that may exist in current federal and state policies.

CONCLUSION

AMIA's 2010 Health Policy Meeting focused on three major health IT concepts: resilience in healthcare and health IT; ethical, legal, and social challenges; and innovation, adoption, and sustainability. These concepts were clarified by national experts in plenary addresses and discussed in breakout sessions by invited participants over a 2-day period. The overarching concern growing out of the findings of the meeting is that current US funding and public policy priorities may have an unintended negative effect on broader health IT innovation and research, and concomitantly the future of healthcare as it is supported by health IT.

US funding and policy priorities, aimed at rapid health IT deployment and a relatively short-term focus on 'meaningful use,' may distract policymakers and industry from supporting and pursuing continued innovations in health IT as aggressively as needed. Because vendors are likely to focus attention on short-term implementation issues to ensure that their EHRs meet MU criteria, and set aside other types of development, true innovation in health IT could falter. Thus, federal initiatives[54] may result in ossification of current mediocre software by failing to push the industry to move to the next level in terms of functions supporting clinical practice (eg, user-centered clinical decision support, computerized provider order entry). These concerns are consistent with general concerns about the ability of the US to remain technologically competitive, and are

supported by studies and publications suggesting that the federal government and industry may be letting crucial strategic issues of US competitiveness slip below the surface.[55–59]

However, rather than thinking of health IT as a fertile ground for failures, fraud, and financial sustainability challenges, targeted policy initiatives can preclude most, if not all, of the potential problems. The recommendations outlined in this paper address many of these issues. The ultimate goal is to recognize the creative vision necessary to take health IT to its next level of innovation and enable it to both drive and support major improvements in healthcare quality and outcomes.

AMIA board of directors response and action

By convening this meeting and disseminating this report, AMIA has identified resilience and innovation as critical issues for the continued widespread adoption of health IT. The AMIA Board of Directors reviewed the paper and endorsed the authors' recommendations. The Board of Directors anticipates committing additional organizational resources to continue to advance the work of the Meeting and will encourage other organizations to work collaboratively to pursue the recommendations and to continue this important public discourse.

REFERENCES

1. **Committee on Quality of Health Care in America, Institute of Medicine.** *Crossing the Quality Chasm: A New Health System for the 21st Century.* Washington, DC: National Academies Press, 2001.
2. **Suehle R.** *Todd Park, CTO of Health and Human Services, on Improving Healthcare with Open Data.* Opensource.com, 2011. http://opensource.com/life/11/3/todd-park-cto-health-and-human-services-improving-healthcare-open-data (accessed 24 Mar 2011).
3. *The SMART Apps Challenge is Live!* SMARTPlatforms. http://www.smartplatforms.org/2011/03/the-smart-apps-challenge-is-live/ (accessed 24 Mar 2011).
4. **Tenner E.** *Why things Bite Back: Technology and the Revenge of Unintended Consequences.* New York: Vintage Books, 1996.
5. **Dorner D.** *The Logic of Failure: Recognizing and Avoiding Error in Complex Situations.* New York: Basic Books, 1997.
6. **Goldfinch S.** Pessimism, computer failure, and information systems development in the public sector. *Public Adm Rev* 2007;**67**:917–29.
7. **Johnson CW.** Why did that happen? Exploring the proliferation of barely usable software in healthcare systems. *Qual Saf Health Care* 2006;**15**(Suppl 1):i76–81.
8. **Posner RA.** *From the Oil Spill to the Financial Crisis, Why We Don't Plan for the Worst.* Washington, DC:The Washington Post, 2010:B01.
9. **Bernstein WS,** Pfister HR, Ingargiola SR. *HITECH revisited.* California HealthCare Foundation. 2010. http://www.manatt.com/uploadedFiles/News_and_Events/Newsletters/HealthLaw@Manatt/HITECH%20Revisited_Final%20May%2031,%202010.pdf (accessed 9 May 2011).
10. **Hoffman S,** Podgurski A. Finding a cure: the case for regulation and oversight of electronic health record systems. *Harv J Law Technol* 2008;**22**:103–64.
11. **Macilwan C.** Science economics: what science is really worth. *Nature* 2010;**465**:682–4. http://www.nature.com/news/2010/100609/full/465682a.html (accessed 24 Mar 2011).
12. **Van der Schaff TW.** Development of a near miss management system at a chemical process plant. In: Van der Schaff TW, Hale AR, Lucas DA, eds. *Near Miss Reporting as a Safety Tool.* Oxford: Butterworth-Heinemann, 1991.
13. **National Research Council, Assembly of Engineering, Committee on Flight Airworthiness Certification Procedures.** *Improving Aircraft Safety: FAA Certification of Commercial Passenger Aircraft.* Washington, DC: National Academy of Sciences, 1980.

14. **Blumenthal D.** Launching HITECH. *N Engl J Med* 2010;**362**:382—5. http://www.nejm.org/doi/full/10.1056/NEJMp0912825?query=current&rss=1 (accessed 2 Apr 2011).

15. *Office of the National Coordinator of Health Information Technology*. http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__home/1204 (accessed 6 Apr 2011).

16. **Avram S.** *Managing Expectations: A View from the Field from Calif.'s REC*. iHealthBeat, California HealthCare Foundation. http://www.ihealthbeat.org/perspectives/2010/managing-expectations-a-view-from-the-field-from-califs-rec.aspx (accessed 2 Apr 2011).

17. **Office of National Coordinator for Health Information Technology.** *Get the Facts about Health IT Workforce Development Program*. http://healthit.hhs.gov/portal/server.pt?open=512&objID=1432&mode=2 (accessed 2 Feb 2011).

18. **Office of the National Coordinator for Health Information Technology, Department of Health and Human Services.** Health Information Technology: initial set of standards, implementation specifications, and certification criteria for electronic health record technology; interim final rule. *Fed Regist* 2010;**57**:2014—47. http://edocket.access.gpo.gov/2010/pdf/E9-31216.pdf (accessed 4 Apr 2011).

19. *The Full Potential of University Research. A Model for Cultivating New Technologies and Innovation Ecosystems*. 2010. http://www.scienceprogress.org/2010/06/the-full-potential-of-university-research/ (accessed 6 Apr 2011).

20. **Perrow C.** *Normal Accidents: Living with High Risk Technologies*. Princeton, NJ: Princeton University Press, 1999.

21. *Ultra-Large-Scale Systems: The Software Challenge of the Future*. Pittsburgh, PA: Software Engineering Institute Carnegie Mellon, 2006.

22. **Kranz G.** *Failure is not an Option: Mission Control from Mercury to Apollo 13 and Beyond*. Simon & Schuster, 2000.

23. **Nemeth C,** Wears R, Woods D, et al. Minding the gaps: creating resilience in health care. In: Henriksen K, Battles JB, Keyes MA, et al, eds. *Advances in Patient Safety: New Directions and Alternative Approaches (Vol. 3: Performance and Tools)*. Rockville (MD): Agency for Healthcare Research and Quality, 2008:259. http://www.ctlab.org/documents/Minding%20the%20Gaps-AHRQ%20AIPS%20Sep08.pdf (accessed 4 Apr 2011).

24. **The Government Accountability Office (GAO).** *Public Health Information Technology: Additional Strategic Planning Needed to Guide HHS's Efforts to Establish Electronic Situational Awareness Capabilities*. 2010. GAO-11-99. http://www.gao.gov/new.items/d1199.pdf (accessed 4 Apr 2011).

25. **PSO Privacy Protection Center.** *AHRQ Common Formats Device or Medical/Surgical Supply, Including HIT Device (Beta)*. https://www.psoppc.org/web/patientsafety/device-or-medical/surgical-supply-including-hit-device-beta#DeviceHIT (accessed 4 Apr 2011).

26. **Centers for Medicare & Medicaid Services.** *Medicare Demonstrations. Details for Multi-Payer Advanced Primary Care Initiative*. http://www.cms.gov/DemoProjectsEvalRpts/MD/itemdetail.asp?itemID=CMS1230016 (accessed 4 Apr 2011).

27. **Bloomrosen M,** Starren J, Lorenzi NM, et al. Anticipating and addressing the unintended consequences of health IT and policy: a report from the AMIA 2009 Health Policy Meeting. *J Am Med Inform Assoc* 2011;**18**:82—90.

28. **Barach P,** Small SD. Reporting and preventing medical mishaps: lessons from non-medical near miss reporting systems. *BMJ* 2000;**320**:759—63. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1117768/pdf/759.pdf (accessed 4 Apr 2011).

29. **Woolf SH,** Kuzel AJ, Dovey SM, et al. A string of mistakes: the importance of cascade analysis in describing, counting, and preventing medical errors. *Ann Fam Med* 2004;**2**:317—26.

30. **Executive Office of the President.** *President's Council of Advisors on Science and Technology. Report to the President. Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward*. 2010. http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf (accessed 4 Apr 2011).

31. **Dolin RH,** Jaffe C. *Health Level Seven® International. Comments re RIN 0991-AB59: Proposed Rule: Proposed Establishment of Certification Programs for Health Information Technology*. 2010. http://www.hl7.org/documentcenter/public_temp_78D65C16-1C23-BA17-0C4C202F095FCC8C/newsroom/HL7%20Response%20to%20the%20ONC%20Certification%20NPRM.pdf (accessed 4 April 2011).

32. **US Department of Homeland Security.** *National Emergency Response Interoperability Framework and Resilient Communication System of Systems*. 2009. http://www.hsdl.org/?view&doc=119204&coll=limited (accessed 4 Apr 2011).

33. **Qureshi ZH.** A review of accident modelling approaches for complex socio-technical systems. *SCS '07 Proceedings of the Twelfth Australian Workshop on Safety Critical Systems and Software and Safety-Related Programmable Systems*. **Vol. 86**. https://portal.acm.org//citation.cfm?id=1387046&dl=ACM&coll=DL&CFID=3432312&CFTOKEN=96600816 (accessed 4 Apr 2011).

34. **Leveson N.** White paper on approaches to safety engineering. 2003. http://sunnyday.mit.edu/caib/concepts.pdf (accessed 4 Apr 2011).

35. **Leveson N.** A new accident model for engineering safer systems. *Saf Sci* 2004;**42**:237—70. http://sunnyday.mit.edu/accidents/esd.pdf (accessed 4 Apr 2011).

36. **Carayon P.** Human factors of complex sociotechnical systems. *Appl Ergon* 2006;**37**:525—35.

37. **Lowy J.** Cascading failures followed Qantas A380 engine blowout. *USA Today* 18 November 2010. http://www.usatoday.com/travel/flights/2010-11-18-qantas-a380-engine_N.htm (accessed 4 Apr 2011).

38. **Miyamoto M,** Sako M, Kimura M, et al. Great earthquakes and medical information systems, with special reference to telecommunications. *J Am Med Inform Assoc* 1999;**6**:252—8. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC61365/pdf/0060252.pdf (accessed 6 May 2011).

39. **Levy G,** Blumberg N, Kreiss Y, et al. Application of information technology within a field hospital deployment following the January 1010 Haiti earthquake disaster. *J Am Med Inform Assoc* 2010;**17**:626—30.

40. **Goodman KW,** Berner ES, Dente MA, et al; for the AMIA Board of Directors, AMIA Board Position Paper. Challenges in ethics, safety, best practices, and oversight regarding HIT vendors, their customers, and patients: a report of an AMIA special task force. *J Am Med Inform Assoc* 2011;**18**:77—81. http://jamia.bmj.com/content/early/2010/11/10/jamia.2010.008946.full.pdf (accessed 4 Apr 2011).

41. **Healthcare.gov.** *Understanding the Affordable Care Act*. http://www.healthcare.gov/law/introduction/index.html (accessed 4 Apr 2011).

42. **US Department of Health & Human Services.** *Health Information Privacy. Security Rule Guidance Material*. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html (accessed 4 Apr 2011).

43. **US Department of Health & Human Services.** *Guidance on Risk Analysis Requirements Under the HIPAA Security Rule*. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf (accessed 4 Apr 2011).

44. **NIST Information Technology Laboratory.** *Identity Management Systems Program*. 2010. http://www.nist.gov/itl/idms/ (accessed 6 May 2011).

45. **McCullough JS,** Casey M, Moscovice I, et al. The effect of health information technology on quality in US hospitals. *Health Aff (Millwood)* 2010;**29**:647—54.

46. **Vest J,** Gamm L. Health information exchange: persistent challenges and new strategies. *J Am Med Inform Assoc* 2010;**17**:288—94.

47. **National Rural Health Association.** *Issue Paper. Rural Health Information Technology*. http://www.ruralhealthweb.org/go/left/policy-and-advocacy/policy-documents-and-statements/issue-papers-and-policy-briefs/ (accessed 5 Apr 2011).

48. **DesRoches CM,** Campbell EG, Vogeli C, et al. Electronic health records' limited successes suggest more targeted uses. *Health Aff (Millwood)* 2010;**29**:639—46.

49. **National Alliance for Health Information Technology.** *Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology terms*. Chicago, IL: National Alliance for Health Information Technology, 2008:4.

50. **McDonnell C,** Werner K, Wendel L; James Bell Associates, The Altarum Institute. *Electronic Health Record Usability: Vendor Practices and Perspectives*. AHRQ Publication, 2010. No. 09(10)-0091-3-EF. http://healthit.ahrq.gov/portal/server.pt/community/ahrq_national_resource_center_for_health_it/650 (accessed 6 May 2011).

51. **Association of Academic Health Centers.** *Out of Order, Out of Time: The State of the Nation's Health Workforce*. 2008. http://www.aahcdc.org/policy/AAHC_OutofTime_4WEB.pdf (accessed 4 Apr 2011).

52. **American Medical Informatics Association and American Health Information Management Association.** *Building the Workforce for Health Information Transformation*. 2006. https://www.amia.org/files/shared/Workforce_web.pdf (accessed 4 Apr 2011).

53. **American Medical Informatics Association and American Health Information Management Association.** *Joint Work Force Task Report. Health Information Management and Informatics Core Competencies for Individuals Working with Electronic Health Records*. 2008. https://www.amia.org/files/shared/Workforce_2008.pdf (accessed 4 Apr 2011).

54. **Blumenthal D,** Tavenner M. The 'meaningful use' regulation for electronic health records. *N Engl J Med* 2010;**363**:501—4. http://www.nejm.org/doi/pdf/10.1056/NEJMp1006114 (accessed 4 Apr 2011).

55. **Augustine NR.** *Is America Falling off the Flat Earth? Rising Above the Gathering Storm Committee, National Academy of Sciences, National Academy of Engineering, and Institute of Medicine of the National Academies*. Washington, DC: The National Academies Press, 2007.

56. **National Science Board (NSB).** *Science and Engineering Indicators 2010*. Arlington, VA: National Science Foundation (NSB 10-01). http://www.nsf.gov/statistics/seind10/ (accessed 4 Apr 2011).

57. **US Government Accountability Office.** *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*. 2010. http://www.gao.gov/new.items/d10338.pdf (accessed 4 Apr 2011).

58. **US Government Accountability Office.** *Cybersecurity: Key Challenges Need to be Addressed to Improve Research and Development*. 2010. http://www.gao.gov/new.items/d10466.pdf (accessed 4 Apr 2011).

59. **National Security Council (NSC) and Homeland Security Council.** *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. 2009. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed 4 Apr 2011).