Recommendation

The introduction of health IT applications to healthcare delivery has unambiguously improved patient safety and saved lives. However, health IT has also introduced new, novel and complex threats to patient safety, resulting in extensive harm. AMIA urges Congress to support the development of a national-level strategy for health IT safety. Such a strategy must include a centralized public-private partnership meant to provide a trusted space where stakeholders can convene to review evidence and jointly develop solutions to critical health IT safety issues.

Background

Congress has long understood the important role public policy can play in promoting patient safety. The Patient Safety and Quality Improvement Act of 2005 created a national network of distributed patient safety organizations (PSOs) whose primary purpose is to collect, analyze and disseminate information on patient safety missteps. These PSOs provide a non-punitive environment for hospitals and physicians to learn from their mistakes and share best-practices on how to improve care. Currently, 82 PSOs serve various regions of the country, but only a handful have the expertise to review health IT-related patient safety events. No PSO has such expertise with a national reach.

The introduction of health IT applications to healthcare delivery has improved patient safety and saved lives. Evidence for improved patient safety due to health IT is widespread. Findings from 2014 literature review demonstrated benefits in medication safety and dosing, increased adherence to clinical guidelines and protocols (including screenings and vaccinations), and the efficiency of care. However, health IT has also introduced new, novel and complex threats to patient safety.

Evidence gathered through experience in the last six years of health IT adoption confirms that software design, implementation decisions, user training and maintenance processes can all have a material impact on the safety of health IT. From 2010 to 2013, 120 health IT-related Sentinel Events (SEs) – an event that has resulted in an unanticipated death or major permanent loss of function – were reported to the Joint Commission. Further, the Journal of Patient Safety reviewed a medical malpractice claims database from 2012 to 2013 and found that while less than one percent of claims involved health IT, a total of 248 cases demonstrated that “Adverse events associated with health IT vulnerabilities can cause extensive harm and are encountered across the continuum of health care settings and sociotechnical factors.” Lastly, a recent spate of high-profile ransomware attacks involving twelve hospitals’ EHR data has added a new dimension of concern for those focused on health IT safety: without access to digital information, clinicians are “flying blind” causing patients to be relocated and high-risk surgeries to be cancelled. In all instances, experts believe reported problems represent a small fraction of the total number of adverse events that go unreported and unanalyzed.

The Path Forward

Multiple efforts, led by the private sector and supported by public sector participation, are working to improve the safe use and safety of health IT. The National Quality Forum has recently developed a set of new quality measures focused on health IT safety; the Agency for Healthcare Research & Quality is working to update and harmonize standardized reporting methods to share data on health
IT-related patient safety events across the care continuum; a multistakeholder group convened by the Association for the Advancement of Medical Instrumentation (AAMI) is working to develop process standards for the development, implementation and use of health IT; and multiple federal agencies from the Veterans Administration and the Food & Drug Administration to the Department of Homeland Security are developing programs and policies to identify and mitigate health IT safety risks. However, none of these activities are being coordinated by a single entity or single group of stakeholders. Each activity is, at best, loosely informed by other, similar activities. Such a landscape is ripe for Congressional leadership.

**Congressional Ask**

AMIA urges Congress to support development of a national health IT safety strategy, as reflected in the Office of the National Coordinator’ Health IT Safety Roadmap, which includes:

- A national public/private partnership on health IT safety meant to convene, analyze and disseminate information to improve the safety and safe use of health IT.
- A national infrastructure to collect and monitor health IT-related patient safety events; and
- Coordinated federal policies to identify and mitigate health IT-related safety risks.

Health IT safety is a responsibility shared among developers, healthcare organizations, clinicians, patients and government stakeholders. Through the creation of a national strategy and public/private partnership focused on health IT safety, empowered to collect information on, evaluate, and report on the overall safety of health IT, AMIA believes that event reporting, education, data aggregation, and the creation of best practices can improve patient safety, better engender patient engagement and fulfill the potential of health IT.

---

6 Gruber et al
7 Simonite, T., “With Hospital Ransomware Infections, the Patients Are at Risk,” MIT Technology Review. April 1, 2016