Testimony of David C Classen, MD, MS

Before the
Subcommittee on Health
Committee on Energy and Commerce

U.S. House of Representatives

Hearing on:
"Health Information Technologies: How Innovation Benefits Patients"
March 20, 2013

Chairman Pitts and Ranking Member Pallone, Members of the Subcommittee, thank you for the opportunity to testify on this very important issue.

I am a practicing infectious disease physician at the University of Utah School of Medicine and I am also the Chief Medical Informatics Officer at Pascal Metrics, a federally certified Patient Safety Organization (PSO). I am also Co-Chair of the AHRQ Common Formats Committee at the National Quality Forum.

I am trained as an infectious disease physician and a medical informaticist and also I am a patient safety researcher focused on ways to measure and improve patient safety with health information technology (health IT). Furthermore I have been a member of several Institute of Medicine Committees on patient safety, most recently (2010-11) the one whose report I will touch on today, *Health IT and Patient Safety: Building Safer Systems For Better Care*. Indeed much of my testimony is drawn directly from this IOM report.

More than a decade ago, the Institute of Medicine (IOM) report, *To Err Is Human,* estimated that 44,000-98,000 lives are lost every year due to medical errors in hospitals and led to the widespread recognition that health care is not safe enough, catalyzing a revolution to improve the quality of care. Despite considerable effort, patient safety has not yet improved to the degree hoped for in that IOM report. In the most recent IOM report on *Health IT and Patient Safety*, the estimates of patient safety problems in hospitals are much higher than the original estimates more than a decade ago, similar studies of ambulatory patient safety issues from the American Medical Association and others cited in this IOM report also suggest that original estimates of safety problems in the outpatient arena may also be low as well.

One strategy the nation has turned to for safer, more effective care is the widespread use of health IT. The U.S. government is investing billions of dollars toward meaningful use of effective health IT so that all Americans can benefit from the use of electronic health records (EHRs). Health IT is playing an ever-larger role in the care of patients, and some components of health IT have significantly improved the quality of health care and reduced medical errors. Continuing to use paper records can place patients at unnecessary risk for harm and substantially constrain the country's ability to reform health care, However, concerns about harm from the use of health IT have emerged.

In this IOM report on *Health IT and Patient Safety*, health IT is defined broadly to include a broad range of products, including EHRs, patient engagement tools (e.g., personal health records [PHRs] and secure patient portals), and health information exchanges (HIEs). Included in this definition of HEALTH IT were mobile applications of any of these tools listed above.

Practicing clinicians such as myself expect health IT to support delivery of high-quality care in several ways, including storing comprehensive health data, providing clinical decision support, facilitating communication, and reducing medical errors.

It is widely believed that health IT, when designed, implemented, and used appropriately, can be a positive enabler to transform the way care is delivered. Designed and applied inappropriately, health IT can add complexity to the already complex delivery of health care, which can lead to unintended adverse consequences, for example dosing errors, failing to detect fatal illnesses, and delaying treatment due to poor human-to-computer interactions or loss of data.

Software-related safety issues are often ascribed narrowly to software coding errors or human errors in using the software. It is rarely that simple. Many problems with health IT relate to usability, implementation, and how software fits with clinical workflow. Focusing on coding or human errors alone often leads to neglect of other important factors (e.g., usability, workflow, interoperability, human factors for example) that may increase the likelihood a patient safety event will occur. Safety is an emergent property of a larger system that takes into account not just the software but also how it is used by clinicians. That larger system – often called a sociotechnical system – includes technology (e.g., software, hardware), people (e.g., clinicians, patients), processes (e.g., workflow), organization (e.g., capacity, decisions about how health IT is applied, incentives), and the external environment (e.g., regulations, public opinion). Adopting a sociotechnical perspective acknowledges that safety emerges from the interaction among these various factors.

Merely installing health IT in health care organizations will not result in improved care or safety. Taken together, the design, implementation, and use of health IT affects its safety performance. Safe implementation and safe use of health IT is a complex, dynamic process that requires a shared responsibility among vendors, healthcare workers, and health care organizations. Safely functioning health IT should provide easy entry and retrieval of data, have simple and intuitive displays, and allow data to be easily transferred and shared among health professionals.

Many features of software contribute to its safe use, including usability and interoperability. The committee believes poor user-interface design, poor workflow, and complex data interfaces are threats to patient safety. The lack of system interoperability is a barrier to improving clinical decisions and patient safety, as it can limit data available for clinical decision-making. Laboratory data have been relatively easy to exchange because good standards exist such as Logical Observation Identifiers Names and Codes (LOINC) and are widely accepted.

However, important information such as problem lists and medication lists are not easily transmitted and understood by the receiving health IT product because existing standards have not been uniformly adopted. Interoperability must extend throughout the continuum of care; standards need to be developed and implemented to support interaction between health IT products that contain disparate data.

Safety considerations need to be embedded throughout the whole health IT implementation process, including the stages of planning and goal setting, deployment, stabilization, optimization, and transformation. Selecting the right software requires a comprehensive understanding of the data and information needs of the organization and the capabilities of the system. Vendors take primary responsibility for the design and development of technologies, ideally with iterative feedback from users. Users assume responsibility for safe implementation and work with vendors throughout the health IT implementation process. The partnership to develop, implement, and optimize systems is a shared responsibility where vendors and users help each other achieve the safest possible applications of health IT.

It is important to recognize that health IT products generally cannot be installed out of the box. Users often need to ensure that products appropriately match their needs and capabilities— in both functionality and complexity of operation. The process of implementing and supporting software is critical to optimizing value and mitigating patient safety risks. A constant, ongoing commitment to safety—from acquisition to implementation and maintenance—is needed to achieve safer, more effective care. Testing at each of these stages is needed to ensure successful and safe use of health IT.

Ongoing safe use of health IT requires diligent surveillance of evolving needs, gaps, performance issues, and mismatches between user needs and system performance, unsafe conditions, and adverse events. The committee believes certain actions are required by private and public entities to monitor safety in order to protect the public's health and provides the following recommendations to improve health IT safety nationwide—optimizing their use to achieve national health goals, while reducing the risks of their use resulting in inadvertent harm.

Building on this background, the IOM report on *Health IT and Patient Safety* made a series of recommendations summarized as follows:

Recommendation 1: The Secretary of Health and Human Services (HHS) should publish an action and surveillance plan within 12 months that includes a schedule for working with the private sector to assess the impact of health IT on patient safety and minimizing the risk of its implementation and use.

Recommendation 2: The Secretary of HHS should ensure insofar as possible that health IT vendors support the free exchange of information about health IT experiences and issues and not prohibit sharing of such information, including details (e.g., screenshots) relating to patient safety.

Recommendation 3: The Office of The National Coordinator for Health IT (ONC) should work with the private and public sectors to make comparative user experiences across vendors publicly available.

Recommendation 4: The Secretary of HHS should fund a new Health IT Safety Council to evaluate criteria for assessing and monitoring the safe use of health IT and the use of health IT to enhance safety. This Council should operate within an existing voluntary consensus standards organization.

Recommendation 5: All health IT vendors should be required to publicly register and list their products with ONC, initially beginning with EHRs certified for the meaningful use program.

Recommendation 6: The Secretary of HHS should specify the quality and risk management process requirements that health IT vendors must adopt, with a particular focus on human factors, safety culture, and usability.

Recommendation 7: The Secretary of HHS should establish a mechanism for both vendors and users to report health IT–related deaths, serious injuries, or unsafe conditions.

Recommendation 8: The Secretary of HHS should recommend that Congress establish an independent federal entity for investigating patient safety deaths, serious injuries, or potentially unsafe conditions associated with health IT. This entity should also monitor and analyze data and publicly report results of these activities.

Recommendation 9a: The Secretary of HHS should monitor and publicly report on the progress of health IT safety annually beginning in 2012. If progress toward safety and reliability is not sufficient as determined by the Secretary, the Secretary should direct the FDA to exercise all available authority to regulate EHRs, health information exchanges, and PHRs.

Recommendation 9b: The Secretary should immediately direct the FDA to begin developing the necessary framework for regulation. Such a framework should be in place if and when the Secretary decides the state of health IT safety requires FDA regulation as stipulated in Recommendation 9a above.

Recommendation 10: HHS, in collaboration with other research groups, should support cross-disciplinary research toward the use of health IT as part of a learning health care system. Products of this research should be used to inform the design, testing, and use of health IT. Specific areas of research include
a. User-centered design and human factors applied to health IT;
b. Safe implementation and use of health IT by all users;
c. Sociotechnical systems associated with health IT; and
d. Impact of policy decisions on health IT use in clinical practice.

Thank you and I look forward to answering your questions.

References

Institute of Medicine. *To Err Is Human: Building a Safer Health System.* Washington, DC: National Academy Press, 2000.

Institute of Medicine. Health IT and patient safety: Building safer systems for better care. 2011. http://www.iom.edu/Reports/2011/Health-IT-and-Patient-Safety-Building-Safer-Systems-for-Better-Care.aspx