American Hospital Association

800 10th Street, NW
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100 Phone
www.aha.org

July 7, 2014

Submitted Electronically

Jeffrey E. Shuren, M.D.
Director, Center for Devices and Radiological Health
Food and Drug Administration
Division of Dockets Management (HFA-305)
5630 Fishers Lane
Room 1061
Rockville, MD 20852

Re: Proposed Risk-Based Regulatory Framework and Strategy for Health Information Technology Report; Request for Comments (Docket No. FDA–2014–N–0339).

Dear Dr. Shuren:

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, and our 43,000 individual members, the American Hospital Association (AHA) appreciates the opportunity to comment on the *Proposed Risk-Based Regulatory Framework and Strategy for Health Information Technology Report* developed jointly by the Food and Drug Administration (FDA), Federal Communications Commission (FCC) and Office of the National Coordinator (ONC) for Health Information Technology (IT).

America's hospitals are committed to ensuring the highest level of patient safety and are eager to utilize health IT as one of many tools to continuously ensure and improve the safety of health care. The AHA believes the report is a good first step in the development of a risk-based framework for health IT and is encouraged by the report's recognition of both the opportunities and risks inherent in using IT systems and its emphasis on increased learning about the safe development, installation and use of health IT. To further this emphasis, **we recommend that the proposed risk-based regulatory framework and strategy for health IT leverage and support existing safety reporting requirements and initiatives and not create a new incident reporting silo labeled "Health IT Safety." We recommend a framework that emphasizes:**

- **Increased analysis of existing data sources for safety incidents involving health IT;**
- **Continued collaboration with private and public-sector stakeholders that expands access to sources of information about the role of health IT in safety incidents; and**

- **More transparency and communication about safety and health IT to educate all stakeholders with a role in advancing the culture of safety and quality in health care**.

Our comments focus on the following elements of the report:

- The proposed categories of health IT function by level of risk and approaches to ensure safety.
- The four identified strategies for addressing safety:
  - Identification, development and adoption of standards and best practices;
  - The value and role of conformity assessment tools;
  - The creation of an environment of learning and continual improvement in the public and private sectors; and
  - Special considerations for clinical decision support tools.
- The proposed public-private Health IT Safety Center.

CATEGORIES OF HEALTH IT FUNCTIONALITY BY LEVEL OF RISK

The report proposes a framework for health IT that describes a risk-based approach that describes the function of the health IT and places the health IT in a category based upon the described technology function. The three categories are administrative, health management and medical device. Rather than the FDA developing formal regulatory oversight for technology in the health management category, the report proposes to rely on a limited, narrowly tailored approach that primarily relies on ONC-coordinated activities, such as the public-private Health IT Safety Center and private-sector capabilities that support testing to validate interoperability and conformance to standards.

The AHA appreciates the attempt to balance the need for safety assurance with promoting innovation. However, we are concerned that the categories used to distinguish one type of health IT from another are based on descriptions of the technology as it is currently used. This approach will be difficult to manage in the future, as IT functionality and use expand and do not fit neatly into one category. The administrative function technology, supporting activities such as admissions and scheduling, would be classified as limited or low risk to patient safety. This type of technology provides information important for the initiation, continuation or conclusion of care. The health IT management function technology, supporting activities such as some clinical decision support (CDS), medication management, provider order entry and electronic access to clinical results, would be classified as generally low risk for patient safety compared to the potential benefit. Technology in this category supports time-sensitive information for health care decision-making. As we understand the proposed framework, technology in the administrative or health IT management categories would not be subject to oversight.

Further, the typology presented does not fully explain how it captures key factors that determine risk: the potential for harm, the extent of harm and the extent to which software is automating clinical decision-making. Nor does it look at a known vulnerability in health management

information systems that could affect safety – that is, the extent to which a product can alter data (such as laboratory values or drug dosages) used to guide clinical decision-making and treatment.

The AHA recommends a categorization for health IT, including:

- The urgency of the technology in support of a clinical intervention or decision;
- The potential for harm if the technology fails;
- The probability of technology failure;
- The scope or severity of patient harm that might occur if the technology fails; and
- The ability to remediate any patient harm that might occur.

The AHA also is concerned that the functional approach presented in the draft report does not sufficiently capture three important facets of health IT that have significant potential safety ramifications and, therefore, should influence the development of categories of health IT based upon risk: interoperability of information across data sources; usability of products; and accurate patient matching. We recommend that the final report include all three of these factors as considerations in the assessment of health IT by level of risk:

- *Interoperability of health information*, or the lack of interoperability, is a key factor in the assessment of safety of health IT. As hospitals connect disparate systems and medical devices to bring data into the electronic health record (EHR), they often must establish multiple interfaces; these also may introduce safety risks. Additionally, the federal government could play an important role in furthering interoperability and addressing this aspect of risk by funding the establishment of robust reference implementations and test beds.
- *Usability of health IT*, which includes how information is presented and accessed, influences the ability of individuals to use health IT products to safely provide care.
- *Accurate patient matching*, or the use of a single, national approach by all parties to accurately and efficiently match patients to their records, is a critical safety issue in the use health IT. The inability to match patients across silos raises safety concerns about mismatches – incorrectly matching patients, or missing a match that should have been made. In addition, without a single, national approach to patient matching, hospitals and health systems are forced to expend significant resources on expensive, proprietary solutions to develop master patient indexes that apply only to that particular hospital or health system's patients. The issue of how to match patients with their medical records needs to be solved as we accelerate information exchange on regional and national levels.

STRATEGIES AND RECOMMENDATIONS FOR ADDRESSING SAFETY

Identification, Development and Adoption of Standards and Best Practices. Hospitals and physicians bear ultimate responsibility for the delivery of care to the patient and must be assured that health IT tools are safe as developed and installed. Hospitals also must have assurance that some of the standards and best practices used in support of health IT are applicable at the product level and others are applicable at the hospital system level. This will call attention to the need

for awareness of a health IT product interaction with other products, devices or systems and awareness of the effects of health IT in their environment:

- The federal government should ensure that health IT vendors are committed to proven standards and processes that promote safety in the complex hospital environment. Attributes such as safe design, use of quality management principles, user-centered design and human factors assessments have been shown to improve safety, and data should be available to affirm to providers what is meant by the best practice associated with health IT products. Transparency about the intended use of the health IT product and the relationship of the product to the rest of the complex hospital IT environment should be an element of required best practices for health IT.
- For the vendor community, safety begins in the requirements stage, and cannot be "reverse engineered" during implementation. Health IT vendors must commit to supporting safe use of their products before and after they are sold. It should not be permissible for vendor agreements to include nondisclosure language or other types of provisions that act to limit or restrict identification, discussion or reporting of safety concerns solely to the health IT vendor.
- Ongoing development and dissemination of best practices in the deployment and use of health IT would be helpful. It is essential that the increased use of EHRs be accompanied by freely available guidance on how to achieve safe implementation and information that communicates all of the steps required to achieve what is deemed to be a successful practice. Consistent with the culture of safety, we believe positive guidance will be more effective than punitive measures.

The Value and Role of Conformity Assessment Tools. The variation in health IT products and changes due to configuration and post-implementation upgrades make the development of conformity assessment tools challenging yet vitally important. Hospitals are particularly attuned to the safety risks associated with health IT because product non-conformity, introduced by a modification to a health IT tool or a modification to other devices or systems, can inadvertently and negatively impact the previously safe use of a health IT tool. The AHA recommends the development and rigorous testing of conformity assessment tools. We also recommend using the evidence collected from safety reports to support updates to the conformity assessment tools:

- Conformity assessment tools for interoperability may be the most important area for improving the usability and safety of health IT systems, particularly as providers seek to share data across settings to support the highest quality of care and the coordination of care.
- It is important to develop conformity assessment tools that can be used with live systems, to ensure that decisions made during implementation and configuration have not had unintended consequences.
- Vendor attention to factors such as use of quality management systems, usability of products and interoperability must be assured.

The Creation of an Environment of Learning and Continual Improvement in the Public and Private Sectors. America's hospitals are prepared to participate in efforts to improve the safe use

of health IT, as well as sharing of best practices and learning from safety events. The private or public-sector initiatives created to examine health IT and patient safety must remember that hospitals embrace the "culture of safety" as the best approach to prioritizing patient safety and identifying and correcting safety concerns:

- Patient safety issues must be considered in a holistic manner. Health IT is most appropriately considered as one of many factors affecting safety, rather than as a freestanding topic. Hospitals participate in a variety of state, federal and private safety reporting and improvement activities, such as The Joint Commission Sentinel Event monitoring and voluntary participation with Patient Safety Organizations (PSOs). In general, ensuring that these existing channels have the knowledge needed to address health IT safety issues would be more productive than establishing new efforts specifically targeted to health IT.

Special Considerations for Clinical Decision Support Tools. There is significant variation in the technology referred to as CDS. Some CDS is within the medical device functionality category and regulated by the FDA. The report distinguishes the regulated from the CDS technology that is within the health management category. The AHA recommends close study of the role of health management CDS in the complex hospital environment to ensure that it meets expectations for the automated delivery of accurate, timely and trusted information in support of safe, rapid decision-making and care delivery in inpatient settings:

- CDS must be transparent so that providers know what information is being used and when the information is updated.
- Ongoing stakeholder discussions are needed to continually refine the definition of CDS as the interoperability of technology advances and the data sources supporting CDS become more complex.
- Insight from functionality and usability testing of CDS and testing of the interoperability of CDS with other systems will be useful in developing and refining best practices and standards applicable to CDS. Electronic data distant from the data source is presumed to be accurate and that presumption of trustworthiness requires validation.

A PUBLIC-PRIVATE HEALTH IT SAFETY CENTER

The draft report proposes the creation of a Health IT Safety Center that will largely focus on oversight of products in the health management category, overseen by ONC and with private sector participation. The AHA supports the concept of a Health IT Safety Center that focuses on engaging all health IT stakeholders, leverages existing sources of evidence to analyze all aspects of health IT – product development through end user experience – and shares study results to educate all stakeholders. Duplicate efforts will slow progress necessary to understand health IT within the larger construct of patient safety. The AHA urges the federal government to support and collaborate with private-sector initiatives underway, such as the ECRI Partnership for Promoting Health IT Patient Safety, that bring multiple stakeholders together to identify and reduce risk and promote patient safety and quality. The federal government's continued

engagement on standardization of terminology, reporting forms and submission methods will help support the usability of existing safety incident information for root cause analysis:

Bringing existing federal government health and safety initiatives into collaboration with a health IT Safety Center will underscore the need to address patient safety holistically. While we need to develop capacity to ensure safety of health IT, it cannot be done in isolation. A safety event, whether a near miss or an adverse event, rarely has a single cause. A separate reporting structure for health IT safety events, for example, would run counter to the culture of safety adopted by hospitals because hospitals want to look at all of the possible contributing factors in order to maintain patient safety plans that effectively remediate and prevent events.

America's hospitals are committed to providing the safest possible care. Thank you for the opportunity to comment on the risk-based regulatory framework for health IT. If you have questions about our comments or would like more information, please contact me or Diane Jones, senior associate director of policy, at djones@aha.org.

Sincerely,

/s/

Linda E. Fishman
Senior Vice President
Public Policy Analysis & Development