TEXAS MEDICAL
ASSOCIATION

Physicians Caring for Texans

July 7, 2014

Leslie Kux
Assistant Commissioner for Policy
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

RE: Proposed Risk-Based Regulatory Framework and Strategy for Health Information Technology Report. Docket No. FDA-2014-N-0339

Dear Assistant Commissioner Kux:

The Texas Medical Association (TMA) is a private, voluntary, nonprofit association of more than 47,000 Texas physicians and medical students. Founded in 1853 to serve the people of Texas in matters of medical care, prevention and cure of disease, and improvement of public health, our charge today is little changed. We represent physician members practicing in all fields of medical specialization.

TMA appreciates the efforts of the FDA, FCC, and ONC in producing a report with a key focus on patient safety when using health technologies. TMA is strongly committed to improving patient safety in all aspects of health information technology, not just electronic health records.

TMA offers the following comments on the Proposed Risk-Based Regulatory Framework and Strategy for Health Information Technology Report.

Page 17 of the report: *The Agencies seek input on the following questions related to promoting the use of quality management principles in health IT:*

• What essential quality management principles should apply to health IT? How should they apply to different stakeholders and at different stages of the health IT product lifecycle?

TMA supports the use of quality management principles in health IT. The medical device industry successfully uses the "Good Manufacturing Principles (GMP)." The one important distinction between the medical device industry and the health IT is that following GMP is mandatory for device manufacturers, and modification of the GMP-manufactured devices is not permitted. TMA believes that GMP-equivalent requirements should be developed for all three proposed classes of Health Information Technology (HIT) development. HIT vendors should be required to follow these GMP-equivalent requirements, and their work should be audited regularly. In order to promote compliance, failure to follow or adhere to the principles may result in some form of corrective action, which may include penalties.

At this time, TMA does not support the extension of these mandatory GMP-equivalent requirements to physician offices as the degree of HIT modification is usually very limited.

Page 20 of the report: *The Agencies seek input on the following questions related to identification, development, and adoption of standards and best practices in health IT:*

• Are the identified priority areas for standards and best practices the proper areas of focus? If not, what areas should be prioritized?

TMA believes that these are the appropriate areas but would add "Downtime and Downtime Recovery" to the list. Downtime and recovery are periods of extreme danger, and systems are rarely built to support safety during downtime (e.g., through the use of a read-only" system) and downtime recovery (e.g., through the use of a shadow system whose entries can be "played back"). It would be helpful to have standardized guidance and best practices for downtime and recovery.

• How can the private sector help facilitate the development and adoption of applicable health IT standards and best practices? Is there a role for a non-governmental, independent program to assess product and stakeholder adherence to standards and best practices? Is there a role for government?

TMA supports the development of GMP-equivalent mandatory requirements for vendors in these areas, with regular auditing and authority to impose penalties for non-compliance. These areas of standards and best practices should be built into the GMP-equivalent requirements.

Page 25 of the report: *Agencies seek public input on the following questions related to creating an environment of learning and continual improvement:*

• What should be the governance structure and functions of the Health IT Safety Center, in order for it to serve as a central point for a learning environment, complement existing systems, facilitate reporting, and promote transparent sharing of adverse events, near misses, lessons learned, and best practices?

TMA strongly believes that the Health IT Safety Center should have the authority outlined by Singh et al in "Creating an Oversight Infrastructure for Electronic Health Record-Related Patient Safety Hazards" (J Patient Saf. 2011 December; 7(4): 169–174). All organizations using HIT should be required to report near-misses and incidents to local Patient Safety Organizations (PSOs). The Health IT Safety Center should have the authority to aggregate these reports. To be effective, the Safety Center also must have the power to investigate incidents with patient harm and require vendor changes, much like the National Transportation Safety Board.

This entity would be charged by Congress to oversee HIT patient safety and coordinate with other agencies that can contribute to improvement in patient safety such as the Office of the National Coordinator, the Federal Drug Administration, the National Institute of Standards and Technology, the Agency for Healthcare Research and Quality, the Center for Medicare and Medicaid Services, the National Quality Forum, PSOs, local health care organizations that collect patient safety data, other local EHR patient safety reporting entities and industrial (EHR and HIT) trade associations. All of these entities need to function cooperatively to effectively identify and manage patient safety risks.

Although many government agencies and private entities can contribute to patient safety surveillance and improvements, none has the expertise and assets necessary to coordinate a national effort.

When patient safety risks or actual adverse events occur, the evaluation and resolution processes currently are nontransparent and managed in a nontransparent manner between the individual physician office and the individual EHR vendor. EHR vendors are not required, nor are they externally incentivized, to identify whether the same issue exists in the same EHR product they support in other physician offices. As a result, patients remain at risks in other offices even if the issue is resolved at the office that reported the issue. Patient safety events are locally reported and managed across the state through mechanisms established within individual health care institutions and by local PSOs. However, the collected data remains within each institution and PSO. Even with a central or statewide reporting point for this data to roll up to for analysis, it would be beneficial to establish governance at a national level. It is practical for patient safety risks to continue to be monitored and managed by these local entities, but the data needs to be collected, aggregated and analyzed through a national central point to identify and manage potentially dangerous trends and patterns that cannot be found and managed locally.

In addition to the complexity involved with collecting and analyzing data from hundreds of institutions and PSOs, hundreds of unrelated EHR vendor products are being used. There is no available registry of these EHR products, many of which are subdivided into multiple versions that sometimes vary widely in their functionality. Although a number of government agencies will need to be involved in a national patient safety program, no single government agency or other entity exists today with the expertise and assets needed to perform these functions.

The primary focus of the national Health IT Safety Center should be on the dedicated surveillance of HIT-related safety risks and on promoting learning from identified issues, potential adverse events (“close calls”) and adverse events. We believe the Health IT Safety Center’s infrastructure should leverage local organizations as a primary source of HIT-related hazard reports, and provide a mechanism by which the data rolls up to the national level. Other functions that a national Health IT Safety Center would or could perform include:

- developing a method for the public to report HIT-related safety concerns;
- investigating HIT-related patient safety deaths and adverse events that are reported;
- disseminating educational information based on findings;
- developing the legal and regulatory infrastructure needed to effectively collect, analyze, and manage HIT-related patient safety issues;

- creating a non-punitive environment that promotes the transparent, free exchange of information regarding safety issues (require vendors to report issues, encourage physicians and providers to report issues, but protect everyone from liability when issues are reported);[1]
- creating an environment of where improving patient safety is seen as a shared responsibility among providers, vendors, and the patient safety infrastructure;
- developing standardized testing of EHRs and performing post-deployment safety testing of EHR products using those standards;
- developing best practices for selection, implementation, and use of EHRs, and disseminating information on best practices;
- developing methods for measuring how HIT product use affects patient safety (use deidentified, aggregated data to provide reports on EHR patient safety to assess the current state of patient safety and to monitor improvements in the safe use of health IT products);
- developing methods to collect data, including the confidential reports of events and safety risks from vendors (required) and physicians and providers (voluntary) as well as automated methods that analyze EHR data to identify potential risks; and
- developing a method for the public to report patient safety events or potential risks.

We also believe the Health IT Patient Safety Center could help repair the fragmentation of the electronic record that is occurring today. The current meaningful use incentives require providers to provide a “portal” through which patients can electronically access their health record information. This means patients are given “access” to multiple portals that are owned by each of their doctors and hospitals from whom they receive care. The patient must manage multiple portals (one for each provider). But these portals do not share information with each other, which means the patient’s electronic health record continues to be fragmented and stored in different places just as it was in the world of paper records. In addition, patients are unable to transfer their records to another doctor. There is currently no standardized method by which such a transfer can occur from one EHR to another. This is actually worse than with paper records where the physician can at least send the stack of paper records to the new physician who then files it in his or her paper system. The fragmentation created by multiple portals and the lack of portability of electronic patient records from one EHR to another is a significant quality of care issue that includes patient safety risks that could be mitigated by actions of the Health IT Safety Center. For example, the Health IT Safety Center could promote the concept of personal health records that are portable from one EHR to another. Other solutions to these issues may arise as technological advances are made.

How can comparative user experiences with health IT be captured and made available to the health IT community and other members of the public to promote learning?

[1] Those who report issues should be able to do so without feeling threatened by potential liability, similar to how PSOs and hospital quality programs provide umbrellas of liability protection when safety issues or adverse events are identified, analyzed, and managed. A lack of umbrella protection creates an incentive for people to not report an issue.

Comparative user experience information is best left to the private sector to develop and manage. The primary purpose of data collected by a national Health IT Safety Center should be to improve patient safety. To promote the collection of data to achieve this purpose, the vendors, physicians, and providers must have reassurance that they can provide reports without fear of repercussions. The collected data should then be analyzed and used to resolve specific issues, identify the safety risks, develop methods to reduce those risks, and disseminate learned information to vendors, physicians, and providers for improving patient safety. This entire process must remain confidential and non-punitive. We believe that using data that is not aggregated and deidentified to create comparisons of vendor products would be counter-productive to the purpose Health IT Safety Center.

Public reporting by the Health IT Safety Center would be appropriate under several circumstances, such as findings pertaining to:

- patient safety deaths;
- public reports of patient safety events or risks;
- patient safety situations identified through confidential reporting where the responsible party fails to address the issue in a cooperative and reasonable manner; and
- findings based on deidentified, aggregated data for the purpose of disseminating information and monitoring progress of health IT safety at a national level.

How can the private sector help facilitate the development of a non-governmental process for listing selected health IT products? What types of products and information should be included? Should the results of conformity assessments, such as conformance with certain clinical or privacy and security standards, be included?

- All HIT vendors should be required to publically register their products, including each version of the products they support.
- Certification status and results of conformance assessments and adherence to privacy and security standards seem appropriate.
- As previously discussed, the government sector should not provide public reports comparing products or results of product testing; this should be left to the private sector

In terms of risk management, what type of safety-related surveillance is appropriate for health IT products categorized as health management functionality? What continued or expanded role(s), if any, should the ONC Health IT Certification Program play in the safety-related surveillance of health IT products?

HIT vendors should be required to report patient safety issues, and physicians and providers should be asked to make voluntary reports of suspected issues. Physicians and providers should be encouraged to make voluntary reports by simplifying the process of submitting a report. For example, developing a standard reporting mechanism and embedding it into the EHR products would make it easier for physicians and providers to submit reports at the point of care.

Patient safety risks could also be identified by automatic methods of reporting. More research is needed, but this type of surveillance is currently used, for example, by hospital Pharmacy

Committees to identify potential medication errors that are then investigated (such as an order for a narcotic reversal medication, which could indicate a narcotic dosing error).

An EHR certification program could be leveraged to incentivize EHR vendors to incorporate these tools into their products.

What role should government play in creating an environment of learning and continual improvement for health IT?

To encourage innovation, shared responsibility, and learning environments for patient safety, the environment used by PSOs and hospital quality committees should be emulated. The government can facilitate such environments by:

- Providing mechanisms for shared learning;
- Ensuring that the data, reports, and actions of the vendors, physicians, providers, and others within the context of the HIT patient safety infrastructure remain privileged and confidential;[2]
- Promoting shared responsibility for patient safety and identifying appropriate levels of accountability on an individual basis; and
- Minimizing the burden on the physicians, providers, and vendors as much as possible in order to make reporting easy and minimize regulations that impact the physician or provider.

TMA is very concerned about the speed with which physicians have been required to meet various requirements for programs such as meaningful use. We have and will continue to educate Texas physicians on the potential for poorly implemented or poorly used HIT to impede quality health care. It takes a lot of time and resources for physicians to ensure their EHRs are safe.

TMA remains strongly committed to improving patient safety in all aspects of HIT, not just electronic health records.

Should you have further questions regarding these comments, feel free to contact TMA Director of Health Information Technology Shannon Vogel via email at shannon.vogel @texmed.org or call (512) 370-1411.

Sincerely,

Matt Murray

Matthew M. Murray, MD
Chair, *ad hoc* Committee on Health Information Technology

[2] Transparent submission of reports and analysis of data depends heavily on reassurance that the reports and data will not be used in a medical liability case. The process must remain non-punitive.