HIMSS Electronic Health Record Association

33 W. Monroe, Suite 1700
Chicago, IL 60603
Phone: 312-915-9582
Fax: 312-915-9511
E-mail:
himssEHRA@himss.org



July 7, 2014

Margaret A. Hamburg, M.D.
Commissioner
Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993

[Submitted Electronically]

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

Dear Dr. Hamburg:

On behalf of the EHR Association (EHRA), we are pleased to respond to the Food and Drug Administration Safety Innovation Act (FDASIA) Report for Health IT on a **Proposed Strategy and Recommendations for a Risk-Based Framework.** Speaking for our nearly 40 member companies, we support many of the concepts proposed in the health IT framework, and look forward to working with key stakeholders to move these important concepts forward.

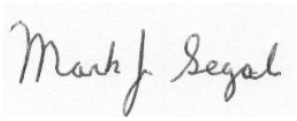
EHRA members believe that patient safety is of paramount importance, the responsibility for which is shared among all participants in the healthcare community – physicians, nurses, hospitals, clinics and other clinicians providing care to the patients; software developers and those who implement health information technology (health IT); and health information exchange (HIE) organizations.

We appreciate the agencies' good work in developing this proposed framework and recognize the significant effort that is being made to engage the broadest group of stakeholders to ensure that final recommendations are balanced and, ultimately, support our shared objectives to deploy health IT to improve patient safety.

EHRA supports the approach proposed in the draft report that categorizes health IT based on the level and nature of risk, then applying appropriate oversight mechanisms. We have promoted such an approach for some time. Our general comments on the proposed framework, along with our detailed responses to the agencies' questions, are attached and reflect alignment with many proposals as well as recommendations in some areas.

Representing a key stakeholder group, we look forward to the final report and participating in future activities that drive operational details from learnings and identifies innovative approaches to address the challenges inherent in implementing such systems. It is imperative to all health IT stakeholders that the ensuing framework is comprehensive, and avoids redundancies and conflicts in oversight and regulatory mechanisms.

Sincerely,

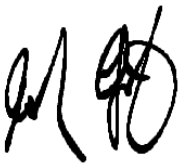


Mark Segal, PhD
Chair, EHR Association
GE Healthcare IT

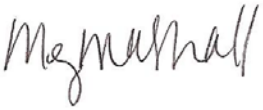
Sarah Corley, MD
Vice Chair, EHR Association
NextGen Healthcare

**HIMSS EHR Association Executive Committee**

Leigh Burchell
Allscripts



Joseph Geretz
SRSsoft



Meg Marshall, JD
Cerner Corporation

Ginny Meadows, RN
McKesson Corporation

Hatem (Tim) Abou-Sayed, MD
Modernizing Medicine

Sasha TerMaat
Epic

CC:
Karen DeSalvo, M.D., National Coordinator for Health Information Technology
Tom Wheeler, Chairman of the Federal Communications Commission

### About the EHR Association

Established in 2004, the Electronic Health Record Association (EHRA) is comprised of more than 40 companies that supply the vast majority of operational EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families.

The EHR Association is a partner of HIMSS. For more information, visit www.ehrassociation.org.

# EHR Association Detailed Comments on a Proposed Risk-Based Regulatory Framework and Strategy for Health Information Technology Report (Docket No. FDA–2014–N–0339), July 7, 2014

Categorizing health IT based on level and nature of risk – and then applying appropriate oversight mechanisms – is an approach that we have long supported. We agree that the intended functionality of health IT is the primary focus in defining categories, and we appreciate the agencies' understanding that the framework must be cognizant of practices and context that may introduce additional factors critical to understanding the true nature of risk of any given health IT or health information system. At the same time, the limited number of examples of applications in each category provided in the report is not sufficient to determine the risk categories for the many existing and new applications being developed and we urge their expansion as this proposal is finalized. We support the proposal that health management and administrative software as generally defined in the report would not be subject to FDA regulation. Reference to clinical workflow and clinical recordkeeping would also be helpful in characterizing the health management health IT functionality.

EHRA agrees that only health IT that represents the greatest risk to patient safety should be regulated as "medical devices" by the FDA, and looks to authoritative clarification that confirms the agency's current approach to such a policy.

We also agree with the depiction of the "health IT ecosystem" in both the FDASIA draft report and ONC's recent white paper "Connected Health and Care for the Nation: A 10-Year Vision to Achieve an Interoperable Health IT Infrastructure," recognizing the challenges in providing adequate oversight mechanisms that represent the appropriate balance of assuring patient safety while enabling innovative health IT development, modularity, and flexibility in implementation. Included in this balance is the concept that some health IT policy and practices will be implemented across categories – such as those that facilitate and improve interoperability, patient matching, and certain other issues.

Overall, since health IT products and the needed infrastructure are still evolving, we should first focus on establishing the needed learning environment for health IT that crosses all stakeholders within the healthcare system. Once the learning environment for health IT is established and sound evidence is analyzed, these experiences will drive the refinement of the proposed health IT framework (e.g., further define the three risk-based categories, agree on and drive adoption of process standards, and further identify clinical decision support (CDS) characteristics that do/do not require regulation or oversight. We suggest that a methodical approach to refining the proposed health IT framework from learnings will enable an oversight framework that is beneficial and sustainable for the entire health IT ecosystem.

We support the three risk-based categories in the FDASIA Report for health IT as it lays the critical ground work for developing a sustainable framework for health IT going forward. We also support that the proposed categories of health management and administrative health IT and most CDS functionality would not be subject to FDA regulation. These categories establish the foundation for the needed framework to continue to mature and improve the national health IT system. To summarize our recommendations for improving the structure of the proposed framework:

- Clear and more detailed definitions for the risk categories: Although the examples in the report communicate the intent of the categories, in order for the categories to be sustainable and to remove ambiguity for stakeholders, clear and detailed definitions need to be developed.
- Comprehensive, coordinated framework: We suggest that there should be a comprehensive framework for all categories of health IT regardless of which federal agency or agencies have

oversight. This framework would use controls based on the risk category and include a continuum of controls that are defined as a holistic path forward for overseeing all health IT versus a focus on a single category. If these categories are given different oversight controls for the same function, the result could require software developers to conform to potentially conflicting or duplicative requirements to get one product to market.

- Platform agnostic: As indicated in the report, we agree that it is vital for the framework to be platform agnostic (i.e., if the same functionality is applied to a mobile platform, cloud platform, or other technology platform, the functionality should be equally subject to the framework or equally excluded). Across the health IT space, there is an increasing trend of moving functions from hardware to software, including the use of mobile platforms, and the framework will need to recognize this shift for it to be fully effective. In addition, it will be important for the framework to also consider additional risks and controls needed that is introduced by platform-specific technologies.
    - EHRA cautions that the term "platform" may not have a consistent definition understood by all health IT stakeholders, and so we propose that the agencies consider the following: "A platform is a hardware architecture and software framework (including application frameworks) that allows software to run. Typical platforms include a computer's architecture, operating system, programming languages and related user interface (runtime libraries or graphical user interface), and operating environment (e.g., mobile or static, wearable device, phone, tablet, or workstation)."

For certain overlapping functionalities, the agencies should take a "primary purpose and context" approach that allows functions in the context of clinical workflow to remain in the health management health IT category, even if similar functions also occur in the context of medical device health IT functionality. For example, both traditional medical device health IT and EHRs may have lower level functions that are common to both (e.g., EHRs and certain medical devices may store medical information or have patient identification structures). EHRs may have reference image viewers or allow for library storage and recognition of such storage. As the agencies further develop their approach in this area, it would be useful to acknowledge that functions primarily in the context of advancing and maintaining clinical workflow and associated recordkeeping would not trigger medical device regulation.

Finally, the agencies should assure that any proposal describes a workable and, on balance, useful approach that describes a specific use case or set of use cases, the nature of the risk, evidence concerning the risk, and other context concerning the problem. In reviewing use cases, the agencies and stakeholders must evaluate variations in the nature of patient safety risks and the relationship of such risks to various participants and technology in health information systems. Certainly, in the broader health information system context, a single piece of software can be the cause of a problem. However, assessing why there is inaccurate, incomplete, or misleading information and its significance in the healthcare delivery process requires understanding of specific operational contexts which will vary. Moreover, a given problem may not be as much inherent to a specific piece of software as it is the result of the interactions between non-interoperable software. Understanding what risks can be addressed by looking at the life cycle of specific software or health IT versus system risk will be important in informing the most appropriate approach to oversight.

## Responses to Specific Questions Posed in the Report

***Promote the Use of Quality Management Principles***

*Question: How do we assure stakeholder accountability for adoption of quality management principles? Is there a role for a non-governmental, independent program to assess stakeholder adherence to quality management principles? Is there a role for government?*

**EHRA Response:**

We note the apparent challenges throughout the industry to create a common understanding regarding the differences between a quality management system, standards, and best practices, as well as how conformity assessment tools relate to them. Before identifying which quality management principles should apply to health IT, we suggest these terms be defined and a general agreement reached about their definitions. Balancing both types of standards is critical to ensure that positive outcomes are achieved and that it is clear what the goal is for each standard so we focus the limited resources of the provider and software developer communities on those standards that will have proven outcomes. As such, we suggest the following terminology:

> **Process standards** provide requirements related to quality management systems (QMSs) for design, development, installation, and implementation.
> **Best practices** provide recommended practices to meet the requirements contained in process standards.
> **Technical standards** provide product-specific requirements associated with interoperability, usability, security and patient data matching.
> **All other functional capabilities -** We note that "all other functional capabilities" standards are beyond the scope of the proposed framework, considering privacy and security is addressed through programs such as HIPAA. All other functional capabilities should fully remain in the non-regulated space open to innovation and market drivers.

*Question: What essential quality management principles should apply to health IT?*

**EHRA Response**:

There are a number of effective quality management principles that can be drawn upon, with the recognition that developers should have some leeway to modify these for the variety of health IT development and use situations. Critical to the health IT risk framework will be a set of specific attributes of a QMS that can be consistently implemented and against which external verification can be conducted that a specific principle is being applied. <u>The focus should be on those aspects of these standards that are most likely to be associated with patient safety.</u> These principles should focus on such key elements as management controls, design controls, production and process controls, corrective and preventive actions, and post-market surveillance.

In addition, we must recognize that some health IT requirements transcend levels, such as interoperability requirements to enable consistent exchange of data regardless of the risk category, or privacy and security requirements to protect patient identity and manage authorized access. Although not solely patient safety issues, a regulatory and oversight framework should enable such consistency without using the burdensome certification approach currently deployed through the Office of the National Coordinator for Health IT (ONC) Certification Criteria and Standards program. Such a framework should address the dimensions of risk management, using the proposed categories, and provide a consistent, holistic approach with overlapping areas where national consistency in approach is essential – specifically interoperability, privacy, and security.

*Question: How should they apply to different stakeholders and at different stages of the health IT product lifecycle?*

**EHRA Response:**

We believe that it is important that all stakeholders adopt quality management principles, recognizing that the specific applicability and application of specific standards will vary among stakeholders. We note that ISO/TR 17791*, Health Informatics – Guidance on standards for enabling safety in health software*, provides an excellent overview of existing safety related standards for health IT and guidance on the applicability of these standards across stakeholders and stages of IT product lifecycles.

*Question: How do we assure stakeholder accountability for adoption of quality management principles?*

**EHRA Response:**

The focus on accountability should be on principles and not on each and every particular aspect of a standard, although adherence at the standard level should be able to be assessed if feasible and desirable for a stakeholder. This process of accountability should not be any more burdensome or intrusive than current FDA or ONC approaches and in general, even less so given the lower risks associated with the health management category.

There are a range of approaches that can be used and, in general, the market should determine which add value. There are multiple options including:

- Self-attestation.
- Industry self-regulation – includes mechanisms such as the EHRA's Code of Conduct, which includes accountability to customers and to purchasers.
- Certification by appropriate third-parties.

We would like to stress that the ultimate health IT framework that emerges must be applied consistently for all federal programs and, at a minimum, be consistent at state and private sector levels as well. Each policy lever introducing its own program requirements will become too complex and overly burdensome.

Providers currently face a myriad of licensure, credentialing and accreditation requirements. In addition, policy levers include reimbursement and incentive programs. The approach implemented by the risk framework should be focused on achieving the desired outcome with the least possible additional barriers and burdens for clinicians and hospitals, and ideally fall within one of the programs with which they are already familiar (e.g., Joint Commission).

*Question: Is there a role for a non-governmental, independent program to assess stakeholder adherence to quality management principles?*

**EHRA Response:**

Yes, there is a role for such programs, but we do not believe that there should be a single designated non-governmental program or entity. There should be allowance for multiple qualified entities, possibly recognized by the federal government, but more appropriate, with industry credibility to assess adherence. Wherever feasible, self-attestation against quality management principles should also be considered.

Health IT stakeholders who voluntarily undergo external and independent verification of such mechanisms should maintain third-party certificates for the required quality management principles, if the stakeholder publically claims/advertises this certification.

Question: *Is there a role for government?*

**EHRA Response:**

We believe that the role of government should be to recognize the agreed-upon quality management principles and requirements as part of the framework, and to educate stakeholders on the same.

***Identify, Develop and Adopt Standards and Best Practices***

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

**EHRA Response:**

We agree with the identified priority areas for standards and best practices (health IT design and development, including usability; location/provider implementation, customization and maintenance of health IT; interoperability; quality management, including quality systems, and risk management).

We suggest that the private sector is best positioned to define best practices, but it may be appropriate for the federal government to recognize specific best practices for a given need. We also recognize that there need not be one set of best practices, but transparency in development and methodology is critical.

The best approach is to use existing standards bodies and organizations with the skills and expertise to develop standards and best practices. There should not be one single private sector program or organization designated for this role. The most appropriate federal government role is as a convener and source of suggested priorities for action. The federal government should not develop standards nor, in general, be a source of best practices (or contract for their development, as with the ONC-issued *Safer Guides*) but it could, using a structured, credible, and transparent process, identify and recognize mature standards and best practices. The EHRA Code of Conduct[1] is a good example of how private sector best practices can be developed with government and other stakeholder engagement.

Specific to usability, EHRA believes that addressing this issue is a shared responsibility:

- EHR developers have the responsibility to apply user-centered design principles and to incorporate new methods as research evolves and the industry moves forward. EHR developers also have a responsibility to their customers to continuously improve usability through research, innovation, testing, user feedback, and observation.
- Healthcare delivery organizations that implement EHRs have the responsibility to consider usability in their configuration of the system, to communicate problems to the EHR developer, and to implement fixes to usability problems to the extent reasonable. Along with the users of EHRs, they have the responsibility to take full advantage of training opportunities.
- Users of EHRs have the responsibility to escalate problems in usability to the organization or vendor that supports them, especially those problems that could lead to patient harm.
- Regulators and policymakers have the responsibility to advance the science of usability through stewardship of research and development of educational resources for system developers, procurers, implementers, and users. As in other industries, the government's role should help to ensure the safety aspects of usability. Other facets of usability are best served through competition in the marketplace.

[1] See www.ehrassociation.org/ASP/codeofconduct.asp

Although any discussion of health IT usability inevitably draws a connection between usability and patient safety, we believe that the two issues, although having some overlap, are different. Recognizing that these are two overlapping but distinct areas of concern, it is essential to make this distinction. Poor usability in an EHR's workflow can potentially affect patient safety, but not every "usability failure" will result in a potential or actual patient safety issue. In addition, the focus on safety aspects of usability most often is on the software. The issue of patient safety issues in relationship to usability must take the entire ecosystem into account.

Because EHRs are highly configurable, EHRA members work to mitigate the risk of unintended outcomes by educating developers and user staff responsible for configuring and enhancing the product with recommendations to establish optimal usability and minimize the potential for patient safety risk. EHR developers are well positioned to anticipate the impact of customer implementation decisions, and share lessons learned among different healthcare delivery organizations to disseminate recommendations.

We have consistently expressed our concerns about the unintended consequences of attempting to regulate EHR usability or certifying EHR developer usability practices. An overly prescriptive approach to usability and design will stifle innovation and the user experience improvements that EHR developers compete on every day. As system developers, we have every incentive to continue to improve our products where it really matters – in the hallways of the hospitals and exam rooms of physicians' offices where they're put to use.

EHR software offers provider organizations extensive flexibility to craft the workflows that best match the way care is delivered locally, and to quickly evolve with new methods and techniques. Usability certification of an EHR could leave provider organizations with a mistaken sense of security in their certified product if their exact configuration is not the one that was certified.

***Leverage Conformity Assessment Tools***

**General EHRA Comment:**
We agree that conformity assessment is, in general, a good thing, but we point out that conformity assessments can reach a point of diminishing value and prevent work on other components of more value in a timely fashion. For example, conformity assessment is already embedded in the Quality Management System Process (QMS) (e.g., ISO 9001). Rather than layering on US-specific regulations, we suggest working with Standards Development Organizations (SDOs), such as ISO organizations, to update QMS requirements by evidence-based consensus, as each added requirement for performing conformity assessment increases cost and time-to-market, and diverts scarce resources from elsewhere in product development, such as usability.

We agree that Interoperability and other standards-conforming capabilities agreed upon as critical should be testable and tested, yet caution that testing tools or guidelines should be developed by the SDO for each of their standards, or by third-parties with oversight by the SDO. ONC and CMS should work with SDOs to encourage the availability and robustness of such tools. We also stress that interoperability testing as part of the ONC certification program should be limited to basic interoperability, since there are many enterprises, state and regional health information exchanges (HIEs) with many differing business models. Standard testing cannot guarantee that the product will work for every local variant of HIE. ONC should allow a choice of testing by the Accredited Certification Body (ACB)/Accredited Testing Lab (ATL), or by having the ACB review documentation of testing by a third party or public test tool.

We suggest that the value of communicating detailed conformity testing results to customers is marginal and should remain voluntary. Customers know that a QMS and safety-enhanced design were incorporated in certified electronic health record technology (CEHRT) products and, as applicable, certificates of conformance with standards are available. More detail on testing may, as appropriate, be available from vendors by request for those purchasers concerned about testing results. Any interventions beyond that should be evidenced-based to ensure real value to the purchaser and consumer. We suggest ONC and FDA team with AHRQ and NIST to develop the evidence that demonstrates clear value to patient safety before adding further requirements to its certification program.

*Question: What conformity assessment tools, if any, should be incorporated into a risk-based health IT framework? How should they apply to different stakeholders and at different stages of the health IT product lifecycle? How can adoption of and adherence to conformity assessment programs be promoted?*

**EHRA Response:**

We recognize that conformity assessment is an important focus area. We suggest, however, that rather than the federal government determining where these are needed, it should play a convener role to ultimately have the market determine where there is value in developing and using such tools.

*Question: Should interoperability be tested?*

**EHRA Response:**

We believe that the testing process, along with test plans and test tools, is an important element for products to assess their conformity to drive consistent interpretation, thus predictable implementation.

*Question: How should tests to validate interoperability be conducted?*

**EHRA Response:**

Testing can be conducted, with reference test plans and tools, either by the implementer of the product (self-assessment) or by a third-party test laboratory. Both should be allowed, and the market should be the driver.

It is important that a common test is agreed upon for a given standard, particularly with the SDO responsible for the implementation guide/standard, enabling both implementers and third-party laboratories to assert conformance to that test. This approach enables other parties to assess claims made, as conformance is claimed against an established test, and have a basis to adjudicate variances of interpretation with the SDO.

*Question: Should interoperability standard(s) be adopted and used for conformity assessments (i.e. develop a functional standard that specifies interoperability characteristics that could be used for conformity assessment)?*

**EHRA Response:**

Generally, standards are not sufficiently specific and more than a single standard needs to be combined into an implementation guide/profile specification to meet a specific use case. Conformity assessment should be conducted against such guides/profiles to be practical and effective.

If a "functional standard" is presumed to be an implementation guide/profile above, then yes, we believe these are critical and need to be developed by multi-stakeholders to be used for interoperability conformity assessment. If a functional standard means being at the functionality level (as perceived by the user), rather than at the interoperability level (what is exchanged on the wire), such functional standards should generally not be within the scope of the proposed framework. Such standards could only come within scope if a patient safety issue is directly attributable to health IT and where the

consensus of the stakeholders indicates that the only way to prevent these issues is through the adoption of a singular standard.

*Question: How should the intended user (e.g. health care provider, consumer, etc.) affect the type of conformity assessment performed?*

**EHRA Response:**

The type of conformity assessment performed should be related to the standards, either product or process, to which an entity is seeking to demonstrate conformity and whether it is a regulatory requirement or commercial requirement. Typically, products requirements, such as usability or meaningful use are subject to testing, while process standards are subject to periodic audits.

We suggest that there are existing consumer protection mechanisms, in addition to HIPAA, that we believe are more appropriate to address the consumer-facing issues.

*Question: How should conformance assessment results be communicated to stakeholders?*

**EHRA Response:**

We believe this communication should be accomplished, as it increasingly is, by the market, with transparency to processes used to conduct assessment. Rather than mandating disclosure (such as with certification results), we suggest focus on communication to purchasers, especially of certificates of conformance as applicable, with an understanding that the type of transaction should drive what is valuable to be transparent.

*Question: Is there a role for a non-governmental, independent health IT conformity assessment program? Is there a role for government?*

**EHRA Response:**

We do agree there is a role for non-government, independent health IT conformity assessment programs, but we strongly suggest that this should not be a single program. There may be a role for government to recognize conformity assessment groups that are domains of conformity assessment (e.g., quality, interoperability).

Question: *Should the ONC Health IT Certification Program be leveraged to protect patient safety through the use of conformity assessment tools?*

**EHRA Response:**

We strongly believe that the ONC Health IT Certification Program should not be expanded or leveraged in this manner.

***Create an Environment of Learning and Continual Improvement***

*Question: 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?*

**EHRA Response:**

We agree with the scope outlined in the draft report and suggest there be clarity that the Health IT Safety Center does not have an oversight or regulatory role. Initially the main goal of the center should be to determine the priority of issues to be addressed through collating and analyzing multiple data sources since there isn't one single source of truth

The center's mission/functions regarding data analysis should include an unbiased analysis of safety data to assess the relative contribution of health IT to patient risk, the contributing factors to this risk, and a

prioritization for standards and best practices across all aspects of development, implementation, and use of health IT. This logically ordered set of tasks should set priorities and inform the other work that needs to be done. Any resulting recommendations for standards, best practices, etc. should be developed by consensus of experts across the stakeholders and should be **evidenced-based**.

Governance of the Center should include all stakeholders, including representation from the vendor community. We suggest that there should be transparency, scheduled meetings, as few workgroups and meetings as needed to accomplish priority goals, clear roles for public and private sector participations, review of drafts by participants before they are finalized, and virtual (but transparent) communications.

*Question: 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?*

**EHRA Response:**

We encourage the federal government to rely upon and encourage market solutions in this area. In addition, we also see major value on aggregate reports from patient safety organizations (PSOs). Government effort should not focus on product/vendor-level experiences, which can be addressed as they are now by a range of private sector programs.

*Question: 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?*

**EHRA Response:**

We believe that additional discussion is required to understand the value and consequences of a non-governmental process for listing selected health IT products. Overall, we do not believe that the case for formalized listing has been made.

It may be that the concept of transparency is more relevant for purchases made by consumers (non-provider users), yet even so, we suggest the focus should be on consumer protection principles, including consumer rights of action.

*Question: 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?*

**EHRA Response:**

We encourage the agencies to support the current pilots underway to test the voluntary reporting of health IT safety events. Broad adoption of these pilots nationwide will drive the recognition and definition of industry standards for event reporting thresholds. At the appropriate time, we recommend the agencies re-evaluate to determine if appropriate actions to incent reporting are necessary.

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

**EHRA Response:**

The interaction of patient safety events related to health IT broadly needs to be better understood. In general, hospitals and providers have established risk management system processes to analyze and investigate patient safety events. Focus should be on augmenting those processes for health IT in a supporting manner – not in a redundant or burdensome approach. Since there seems to be general support in the industry for the use of PSOs as a source of data, we recommend that action be taken to

provide vendors with the same confidentiality protections as the providers in order to ensure a culture of safety and facilitate a safe environment for discussion.

***Clinical Decision Support***

*Question: What types of CDS functionality should be subject to the health management health IT framework? Which types should be the focus of FDA oversight?*

**EHRA Response:**

In the FDASIA Health IT Report, the CDS tools below were suggested to be under the Health Management Functionality category:

- Clinician order sets;
- Drug-drug interactions and drug-allergy contraindication alerts;
- Drug dosing calculations;
- Drug formulary guidelines;
- Reminders for preventative care;
- Access to treatment guidelines;
- Calculation of prediction rules.

We agree with this listing and suggest that this approach to defining CDS should be maintained. We strongly believe there is no need to treat CDS separately than what is defined by the framework for all health IT. In addition, it is important to recognize that CDS is simply content or reference data, or provides the evidence to support a care protocol, reinforces the concept of the clinician as a learned intermediary, and stops short of the practice of medicine. Simply put, FDA regulation should focus on highest risk products and their intended uses, and we agree that the majority of CDS is unlikely to fall within this category.

*Question: How should the following priority areas identified in the health management health IT framework be applied to CDS categorized as health management health IT functionality?*

**EHRA Response:**

- Quality management principles: These are not unique to CDS, therefore the same QMS principles should be followed.
- Standards and best practices: There are many best practices and standards of care that are followed in medicine. This is not unique to CDS.
- Conformity assessments: This is not unique to CDS.
- Learning environment and continual improvement: This is not unique to CDS.

*Question: Are there additional safeguards for CDS, such as greater transparency with respect to CDS rules and information sources that are needed to appropriately balance patient safety and the promotion of innovation?*

**EHRA Response:**

The EHR Incentive Program has implemented source information so no additional safeguards are needed. Innovation in this area appears to be growing due to customer demand. We believe there are no additional safeguards necessary given the range of CDS as well as the other types of health management IT. Beyond the current certification approach, CDS safeguards should not be mandated. Certainly, it important to evaluate how the current 2014 certification approach to CDS transparency is working. However, it is also essential not to take any steps that limit the flow of knowledge into CDS rules and interventions.

*Question: Does the certification of CDS functionalities, such as those functionalities currently certified under the ONC Health IT Certification Program, sufficiently balance patient safety and the promotion of innovation?*

***EHRA Response:***

We believe it is too early to tell how well the approach to certification of CDS in the 2014 edition of CEHRT is working and whether it provides useful information to purchasers and is a practical and workable approach. Overall, we share a growing concern with many stakeholders that certification and associated measurement runs the risk of stifling innovation. One important issue is that there is a broad spectrum of CDS "interventions" as defined by ONC and these can involve both technology and content, as discussed previously in our general comments about CDS.

The private sector can develop high quality, safe CDS, as it has been, through the use of appropriate quality management principles and processes, application of appropriate usability and software develop lenient processes, and transparency as applicable about underlying clinical content. The government role should be as generally envisioned in this draft report.