athenahealth

July 7, 2014

Leslie Kux
Assistant Commissioner for Policy
Food and Drug Administration
Division of Docket Management (HFA–305)
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

Submitted electronically via www.regulations.gov

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

Dear Ms. Kux,

athenahealth, Inc. ("athenahealth") appreciates the opportunity to comment on the draft FDASIA Health IT Report (the "Report"), and the continued willingness of the Food and Drug Administration (FDA), the Federal Communications Commission (FCC) the Office of the National Coordinator for Health Information Technology (ONC) (collectively, "the agencies"), and engaged Members of both chambers of the US Congress to engage with industry stakeholders in the crucially important task of creating an appropriate, risk-based oversight framework for health information technology ("health IT") that protects patients while fostering innovation and avoiding regulatory duplication. As described more fulsomely below, we agree emphatically with much of the approach outlined in the Report, but assert just as emphatically the need for Congressional action to codify that approach.

athenahealth provides electronic health record ("EHR"), practice management, care coordination, patient communication, data analytics, and related services to physician practices, working with a network of over 50,000 healthcare professionals who serve approximately 50 million patients in all 50 states. All of our providers access our services on the same instance of continuously-updated, cloud-based software. Our cloud platform affords to us and our clients a significant advantage over traditional, static software-based health IT products as we work to realize our company vision of a national information backbone enabling healthcare to work as it should. Our clients' successes, exemplified by a Meaningful Use attestation rate more than double the national average, underscore the very real potential of health IT to improve care delivery and patient outcomes while increasing efficiency and reducing systemic costs.

Those successes and the benefits they confer on care providers and their patients, in other words, underscore the profound importance of structuring and implementing an oversight framework for health IT that protects and fosters continued innovation and

avoids the kind of regulatory uncertainty and jurisdictional creep that has limited entrepreneurialism and innovation in healthcare.

Since Congress called in July 2012 for a recommendation from the Administration for a risk-based oversight framework for health IT, few principles have garnered so much universal support from across the spectrum of interested stakeholders as the need for "regulatory certainty." Industry, entrepreneurs, care providers, government officials and regulators—all agree: "certainty" is a crucial objective if an oversight framework is to achieve Congress's tripartite goal of protecting patients while protecting innovation and avoiding regulatory duplication.

Unfortunately, a framework that depends on unfettered regulator discretion built upon a virtually limitless statutory grant of jurisdiction to that regulator simply cannot provide regulatory certainty. Quite the opposite; such a framework perpetuates precisely the regulatory uncertainty that Congress quite evidently hoped to avoid with its very specific FDASIA mandate.

To underscore why this is so one need only refer to the FDA document *Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff*, issued in September 2013 and cited repeatedly throughout the Report to illustrate the agencies' intended regulatory approach to health IT. Like all such guidance documents, each and every page of that document bears the prominent header, "*Contains Nonbinding Recommendations*." If the import of that header were unclear, the bold-box disclaimer at the very beginning of the text is explicit: "This guidance represents the [FDA's] current thinking on this topic. It does not create or confer any rights for or on [sic] any person and does not operate to bind FDA or the public." It is, in regulatory parlance, a statement of present regulatory intent. To an attorney advising either an established health IT industry player or a prospective health IT innovator the meaning of these headers and disclaimers is abundantly clear: "No, as a legal matter you cannot rely upon this document." Indeed, less than a year following issuance of the "final" Mobile Medical Applications guidance, the FDA substantially revised that guidance in important (and in our view productive) respects via its draft medical device data systems (MDDS) guidance. Ergo: the *opposite* of regulatory certainty.

If these observations seem at odds with the more detailed, largely supportive comments below, this apparent incongruity is explained by our recognition that the human beings currently in charge of regulatory policy at the agencies, whose present regulatory intent is reflected in the Report, are like all of us only temporary occupants of their current positions of authority. We are in fact highly supportive of the present regulatory intent of those human beings, and we are anxious to work with them and with Congress to ensure that a lasting framework codifying that intent results from the FDASIA process.

Indeed, as a practical, legal matter we believe that the approach set forth in the Report *requires* express Congressional authorization and appropriation in order to be truly effective, and that such codification is very much in the interests of the regulators who will be responsible and accountable for implementation of a framework. Take, for example, the proposed Health IT Safety Center. To be an effective and secure repository for patient safety event information and a source of trusted, data-based best practices, such a center requires statutory authority and protections of a similar nature to those currently afforded patient safety organizations. Indeed, this reality was implicitly acknowledged by the agencies with the recent announcement that the intended scope of the Center would be scaled back, apparently to avoid the need for Congressional action. In our view that is precisely the wrong approach. The agencies should work collaboratively with the broad, bipartisan group of Members in both the House and Senate who have already engaged actively on the question of health IT oversight, to ensure that any eventual framework adequately takes into account their deep and varied bases of expertise.

To be clear, we are not proposing, as some have suggested, that Congress should undertake to establish the regulatory minutiae of a risk-based oversight framework. Congress should, however, define with much greater specificity the jurisdictional boundaries within which the agencies will be appropriately charged with implementing effective and flexible regulations. This is the crux of our high-level disagreement with the agencies' apparent present posture vis-à-vis the Congress: they propose both to establish the applicable oversight framework, and to define the jurisdictional parameters within which they will regulate. In this case, relying upon the jurisdictional authority conferred by a statutory definition of the term "medical device" that pre-dates any of the technology that will be subject to an eventual framework, the agencies propose in essence to operate within no jurisdictional boundaries at all save those that they themselves create and change based on occasional statements of present regulatory intent. Such an approach is, in our view, untenable.

athenahealth has been actively engaged in the multi-stakeholder effort led by the respected Bipartisan Policy Center (BPC) to craft recommendations for an appropriate, risk-based oversight framework for health IT. We were pleased to see the BPC's work product vividly reflected in the Report. We join in comments submitted by the BPC under separate cover. In addition to those comments and subject to the prefatory remarks above, we offer the following specific comments on the Report:

1. ***Health IT should be categorized and overseen according to risk profile, but those definitions must be clear, lasting, and not dependent on lists of examples.***

We agree with the Report's classification of health IT according to risk. We also agree that the risk profiles of health IT should be appropriately divided into three major categories: administrative, health management, and medical device. However, these

categories must be defined in a way that provides clarity, so that stakeholders know which technologies belong in each category, and with certainty, so that definitions will not need to be changed as technology evolves. To do this, the definitions must describe the characteristics of functionalities in each category, not rely on lists examples that in a fast-evolving industry will soon be obsolete.

The riskiest health IT, belonging in the medical device category, is software that is intended to change the structure or any function of the body (either because it is a component of a medical device or integral to its function), that acts directly on a patient with no opportunity for clinician intervention, or that provides diagnostic or clinical information to a clinician that he or she must substantially rely[1] upon with no opportunity to independently verify that information. These characteristics are consistent with the examples of medical device health IT functionality listed in the Report, including computer aided detection/diagnostic, radiation treatment planning, and robotic surgical planning software.

Health IT software that presents a moderate risk and belongs in the health management category is that which informs clinical decision making and supports the delivery of care but provides an opportunity for clinician intervention. The Report correctly states that most clinical decision support (CDS) software belongs in this category, but more clarity is needed around the term "most." CDS software that provides an opportunity for clinician intervention (as most does) should be classified in the lower risk categories, and that which does not provide such an opportunity should be classified in the higher-risk medical device health IT functionality.

Administrative health IT software supports the administrative and operational aspects of care delivery but is not used in the direct delivery of care. The final Report should recognize that administrative software should not be regulated as higher-risk health management software simply because it is tangential to the delivery of care, such as appointment scheduling software that leads to the delivery of care but is not used in the direct delivery of care.

We do not agree with the Report's approach in addressing CDS separately from other health IT, as we do not think CDS is inherently more risky than other health IT. The Report notes in Section 4 that, "electronic health records (EHRs) may have functionality that spans one or more of [the categories of health IT]." CDS is analogous to EHRs in that both terms describe a wide range of functionalities with varied risk profiles. The

[1] The concept of a "substantial reliance" has been suggested by other groups, such as the Clinical Decision Support Coalition, and must be tightly defined. A clinician should only be considered "substantially reliant" where: (a) he or she could not be trained to make a decision without the aid of software; and (b) the clinician has no visibility into the analysis performed by the software, precluding independent, learned evaluation of the information presented; or (c) the software is intended to be used in an emergency situation where the clinician generally does not have the time to independently evaluate the analysis performed by the software.

definitions of the three risk categories should be worded so that CDS functionalities can be classified as easily as other health IT, without reliance on a list of examples that are frozen in time.

2. *The proposed framework focuses on the correct key areas—quality management principles, standards and best practices, conformity assessment tools, and an environment of learning and continual improvement—but proper implementation of these areas will require greater detail.*

We concur with the four key priority areas and guiding principles identified in the Report for developing a risk-based framework for health IT, as well as the creation of a Health IT Safety Center to serve as a convener of stakeholders for the development and dissemination of best practices. However, the Report only sets forth broad concepts that could eventually form the basis of the framework. An actual framework needs to be proposed with greater detail, clarity, and certainty over implementation.

For example, the Report discusses many different types of conformity assessment tools without indicating which might be best suited for the different categories of health IT, how stakeholders will determine which tool to use, or how the agencies plan to leverage nongovernmental entities to conduct such testing. This does not provide stakeholders with the certainty and clarity needed to spur innovation, and it fails to offer any assurance of safety to providers and patients.

a. *Quality management principles, standards, and best practices must be sufficiently flexible to meet the needs of different health IT models and future innovation.*

We agree that quality management principles, standards and best practices are as essential component of assuring the safe development and use of health IT, but these measures must be implemented with sufficient flexibility. There are many health IT software models in use today and many more that are certain to emerge in the future. The agencies must take care to avoid overly prescriptive measures that inadvertently favor one software model over others, or that inadvertently favor present technology over future innovations. For example, mandatory best practices for on-site software installation would preclude a more efficient model that relies on remote, cloud-based software implementations. We recommend that the framework include a menu of options for quality management principles, standards, and best practices so that health IT developers of all sizes and models have the guidance necessary to implement safe design and development processes without stifling innovation.

In developing these flexible measures, the agencies should leverage non-governmental subject matter experts and standards development organizations in establishing these measures. Groups like the National Patient Safety Foundation, International

Organization for Standardization, Health Level Seven International, and the Alliance for Quality Improvement and Patient Safety all have expertise in different aspects of assuring patient safety. These organizations should play a central role in the development, curation, and maintenance of quality management principles, standards, and best practices.

b. *Conformity assessment tools must be uniform, flexible, and clearly defined to assure stakeholder accountability and promote consumer confidence.*

The Report outlines many different options for conformity assessment tools without indicating how the agencies will decide which tools are best suited for the different categories of health IT. Our recommendation is that the final report should outline a more streamlined, flexible, uniform, and definite approach for conformity assessment that could work across many different types of health IT.

Based on our experience implementing a variety of quality management systems and conducting numerous internal and external audits, we suggest that assessment of patient safety compliance among health IT developers be structured similarly to Sarbanes-Oxley assessments used by public companies or the Health Information Trust Alliance common security framework certification program. These programs rely on the implementation of corporate control activities to accomplish best practices and an independent audit of those control activities, the result of which can be reported to stakeholders. Such a program could ensure that health IT developers of all sizes and specialties are implementing appropriate quality management systems without an overly prescriptive government-led certification program. Additionally, a single conformity assessment tool that is flexible enough to apply to all health management health IT functionality will best enable providers and patients to understand the relative safety of various products.

We also caution against conformity assessment tools that focus on certification of functionality, as opposed to process-based measures. As we have seen with the ONC Health IT Certification Program, certification programs that prescribe specific functionality result in software that is built only to specification with a “check the box” mentality. Even if expanded to include health IT beyond EHRs, the ONC Health IT Certification Program is not a good conformity assessment tool for patient safety because it prescribes functionality, as opposed to assuring that health IT is designed, developed, implemented and used in conformance with certain processes.

c. *The agencies should take care to avoid regulatory duplication with respect to interoperability and should instead look to public-private initiatives*.

As the Report notes, interoperability plays a large role in promoting patient safety. However, because interoperability is a key aspect in many health policy discussions, the

risk of regulatory duplication is particularly high. The Report states, "The Agencies recommend that entities be identified to develop tests to validate interoperability, test product conformance with standards, and transparently share results of product performance to promote broader adoption of interoperable solutions." Much of this work is already being done in the context of the ONC Health IT Certification Program, so the creation of a new bureaucracy around validating and testing interoperability will likely be duplicative.

Even if this new validation and testing work could be incorporated into the ONC Health IT Certification Program in a non-duplicative way, we instead support a regulatory approach that would incentivize actual interoperation as opposed to requiring the mere ability of systems to interoperate. While building interoperable infrastructure is certainly a necessary foundation, the biggest barrier to interoperation in our experience is the lack of properly aligned incentives for actual interoperation. The creation of a functioning market for the exchange of health information, where the business case for interoperability is clear, would promote patient safety much more than the validation and testing of interoperability capabilities. The agencies should seek to leverage existing private-sector initiatives to spur interoperability, such as the CommonWell Health Alliance and Direct Trust.

3. *An environment of learning and continual improvement depends on confidential and non-punitive reporting of safety issues and a trusted convener to aggregate and disseminate best practices.*

As the Report notes, the Patient Safety and Quality Improvement Act of 2005 recognized that improving patient safety in the health care system requires voluntary, confidential, and non-punitive reporting of safety issues with the goal of system-wide learning. That Act provides legal protections for health care providers to report issues to a Patient Safety Organization (PSO) without fear of the report being used against them. As health IT becomes increasingly adopted across all care settings, we believe that providers should incorporate reporting of health IT-related safety issues into their existing PSO reporting processes. Additionally, PSO reporting protections should be extended to health IT developers so that they can both report issues discovered internally and be a part of protected investigation, analysis, and mitigations discussions with reporting providers. We support mandatory reporting requirements where protections exist.

a. *Patient Safety Organizations are the ideal forum for confidential and non-punitive reporting of health IT safety issues.*

athenahealth was the first health IT developer to partner with a PSO when it announced its partnership with Quantros in the fall of 2013. As a result, over 18,000 providers using our EHR will have free access to PSO reporting for all patient safety issues, and

athenahealth will both report issues to Quantros and be involved in resolving health IT-related issues reported by our clients. Several other health IT vendors have begun structuring various partnerships with different PSOs, including ECRI PSO, which established the Partnership for Health IT Patient Safety.

The different approaches that health IT developers are taking with respect to PSO partnership underscore two things: 1) that the federated, public/private approach to PSOs is ideally suited to meet the various issue reporting and resolution needs of the many different health IT developers in the market today without requiring duplicative reporting; and 2) that a trusted convener, with the same protections as PSOs, is needed to aggregate learnings with respect to health IT from the eighty PSOs currently listed with the Agency for Healthcare Research and Quality and then disseminate best practices to all stakeholders.

b. *The Health IT Safety Center should be a trusted convener with the same protections as PSOs and should leverage existing third party expertise in health IT and patient safety.*

We applaud the proposal for a Health IT Safety Center, but we do not believe that such an entity requires heavy government involvement at this point. If implemented correctly, the Safety Center could serve as a trusted source for aggregation and analysis of patient safety reporting (whether to a PSO or other entity). The Safety Center should be led by an independent third party (or a collaboration of third parties) with expertise in the unique intersection of health IT and patient safety. For example, the National Patient Safety Foundation has demonstrated expertise in developing and disseminating safety materials and could play an important role in the Safety Center. In order to gain the trust of stakeholders and remain properly focused on learning and improvement, the Safety Center should have the same privilege and confidentiality protections as PSOs. These protections are important for preserving the incentive for providers to report issues (especially since many reports will include some aspect of user error) and do not need to detract from transparency in the governance and work of the Safety Center.

We do not believe that there is sufficient data on health IT-related safety issues to warrant the creation of an extensive surveillance component to the ONC Health IT Certification Program. Surveillance activities should be data-driven, leveraging the output of the Health IT Safety Center.

Again, athenahealth sincerely appreciates the opportunity to submit these comments and to participate in an ongoing basis in the important work of establishing an appropriate, risk-based oversight framework for health IT that protects patients, fosters innovation, and avoids regulatory duplication. We are heartened by and largely supportive of the approach reflected in the Draft Report, and eager to work with the agencies and with Congress to ensure that it results in a lasting, durable, and effective framework.

Sincerely yours,

Dan Haley
Vice President, Government and Regulatory Affairs