June 16, 2014

Chairman Joe Pitts
Committee on Energy and Commerce
US House of Representatives
420 Cannon House Office Building
Washington, DC 20515

Ranking Member Frank Pallone
Committee on Energy and Commerce
US House of Representatives
237 Cannon House Office Building
Washington, DC 20515
Via telemedicineideas2014@mail.house.gov

Re: **Telehealth to Digital Medicine: How 21st Century Technology Can Benefit Patients**

Dear Chairman Pitts and Ranking Member Pallone,

athenahealth, Inc. ("athenahealth") appreciates the opportunity to comment on the potential of 21st century technologies to improve healthcare. The 21st Century Cures Initiative is a critical step to ensure that the federal government encourages, and does not impede, innovation while still promoting patient safety.

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.

We are not far from the day where nearly every patient encounter in this country will be facilitated by the use of health IT. When health IT works efficiently, providers are "able to coordinate and provide care more efficiently with comprehensive records stored at their fingertips. The fast and easy sharing of patient data across providers should improve patient outcomes…identifying harmful drug interactions, reducing unnecessary duplicate testing, and helping physicians manage patients with

multiple conditions."[1] With the promise to reduce costs and benefit patient care, it is important that health IT maximizes its potential through continuous learning, improvement, and innovation.

Following last month's hearing on telemedicine and digital medicine, there are two areas where the federal government can and should do more to encourage innovation and optimize the potential of health IT. First, Congress should remove the cloud of uncertainty currently hanging over the health IT industry and act on legislation to ensure that low and moderate risk health IT will be subject to a new framework designed specifically for health IT, not the FDA's device framework. Second, the removal of policy barriers to interoperability of health information is needed ensure that the federal government does not continue to reward and subsidize laggard technologies that cannot achieve the broad goals of the 21st Century Cures initiative.

I. Legislation is needed to remove regulatory uncertainty and create a new regulatory framework for health IT.

The 21st Century Cures initiative should include an evaluation of how to best promote continued innovation in the health IT industry, particularly with respect to avoiding unnecessary, uncertain, or overly-burdensome regulation. To that end, the SOFTWARE Act, introduced last year by Rep. Marsha Blackburn, lays the groundwork for a new oversight framework to ensure the safe development, implementation and use of health IT. This bill provides much-needed clarity regarding the oversight of various types of health IT.

a. The FDA's jurisdiction over health IT will stifle innovation in that sector.

The current regulatory structure applicable to health IT is broad and outdated. The definition of "device" (21 USC 321(h)), last revised in the 1970s, grants to the FDA broad authority to regulate any "instrumentality" used in the diagnosis or treatment of patients. Functionally, then, the FDA can if it wishes assert virtually limitless jurisdiction over health IT under a statute last revised before any of the technologies in question existed. This is inappropriate and counter-productive in a number of ways:

- The vast majority of health IT is fundamentally different from the medical device technologies that the FDA traditionally and appropriately regulates. Potential patient safety issues associated with the use of health IT, to the extent that they exist, arise in its implementation, customization, and use, not in the manufacturing processes that the FDA appropriately regulates in the devices context. There is no "software factory" for FDA to inspect, and no end "product" for FDA to evaluate, and the FDA does not have authority over the contexts in which most health IT is implemented, customized and used: hospitals, physician offices, and other care settings. The FDA's efforts to ensure the safety of health IT would be hampered by the inapplicability of their regulatory framework.

- According to numerous recent statements by FDA officials, the agency's "present regulatory intent" is to exercise "enforcement discretion" with regard to the majority of health IT—effectively excluding many technologies from active FDA regulatory oversight. Under the Food and Drug Administration Safety and Innovation Act ("FDASIA"), the FDA, ONC, and FCC were

[1] Sen. Thune, Alexander, Roberts, Burr, Coburn, Enzi. REBOOT: Re-Examining the Strategies Needed to Successfully Adopt Health IT. Apr. 16, 2013. http://www.thune.senate.gov/public/index.cfm/files/serve?File_id=0cf0490e-76af-4934-b534-83f5613c7370

required to report to Congress on how to regulate health IT and recommend a risk-based framework. Released in April, a draft of the FDASIA report clarified FDA's regulatory intent, but failed to ease uncertainty about the future of regulation. The report is asking industry stakeholders to trust not only that human beings currently making policy will stick to their own recommendations over time, but that their successors will share their perspective as well. This is of inherently limited value, since "present regulatory intent" is non-binding and susceptible to revision at the agency's discretion, particularly as administrations change.

- In our system of government, it is axiomatic that Congress holds the authority and indeed the duty to define the parameters within which regulators regulate. Flipped: a regulatory agency does not have the authority to define for itself its regulatory jurisdiction. Yet under the extraordinarily broad terms of the current governing statute, that is in effect what FDA proposes to do via "enforcement discretion"—define (and periodically redefine) the boundaries of its own regulatory reach.

b. Only legislation can give the health IT industry the regulatory certainty needed to foster innovation while ensuring patient safety.

A common theme heard from Congress, agencies, and industry alike is the need to provide regulatory certainty to foster innovation. In the health IT industry, innovation comes in the form of technologies that iteratively release new versions every month, if not every week. Such technologies—from EHRs to clinical decision support to mobile medical apps--demand a regulatory framework conducive to rapid innovation. Software is simply not a medical device and should not be subjected to the FDA's onerous device framework. The possibility of future FDA regulation threatens innovation of the same technologies that can improve the delivery of care.

The SOFTWARE Act represents an excellent first step toward defining new statutory categories of lower-risk health IT—"clinical software" and "health software"—and removing those categories from the FDA's jurisdiction. Because the technologies within those categories present low or moderate risk to patients, especially compared to medical devices and software integrated with devices (which are now and would continue to be regulated by FDA under its device framework), the bill instead subjects such technologies to a new oversight framework better tailored to the unique nature of health IT.

The bill would not leave clinical and health software unregulated, nor would they impose burdensome new regulation over clinical and health software that would stifle innovation. These lower-risk categories would be subject to a new framework, appropriately calibrated to their risk profiles to both afford necessary patient protections and protect beneficial innovation in health IT (which itself fosters patient safety). The Committee should continue to work with the framework and definitions set forth in the SOFTWARE Act in the 21st Century Cures initiative.

Some groups[2] have raised concerns that the bill would improperly classify higher-risk medical devices into the lower-risk categories of clinical and health software, and, through the 21st Century Cures initiative, the legislative language can and should be adjusted where appropriate to address these

---

[2] mHealth Regulatory Coalition, *Examples of Software That Would Be Deregulated Under the PROTECT Act*, Feb. 12, 2014. http://assets.fiercemarkets.com/public/newsletter/fiercehealthit/protectactexamplesV1.pdf
Slabodkin, G, *Industry group voices "extreme" concern with PROTECT Act*, FierceMobile Healthcare, Feb. 19, 2014. http://www.fiercemobilehealthcare.com/story/industry-group-voices-extreme-concern-protect-act/2014-02-19

concerns. It is certainly no easy task to create statutory definitions that properly draw the lines between different categories of health IT risk, but the difficulty does not counter the need for a legislative solution. Only Congress can redraw the lines of jurisdiction and ensure the creation of an oversight framework that promotes safety and innovation in health IT.

II. Impediments to the open exchange of patient information threaten the quality of health care while driving up costs.

The 21st Century Cures initiative should also address issues with the particularly the lack of interoperability and information sharing among EHRs in its broader goal of addressing ways in which the federal government currently inhibits the use or adoption of such technologies. Interoperability is critical for health IT to improve care, but there are significant impediments to information flow in healthcare—many of them the unintended consequences of well-intentioned public policy decisions.

a. The Meaningful Use ("MU") program as currently structured impedes information sharing by subsidizing technologies that do not share information.

To-date, approximately 24 billion federal dollars have been spent under the auspices of the MU program administered by the Office of the National Coordinator for Health Information Technology ("ONC") to subsidize the adoption and "meaningful use" of health IT by care providers. The most common question we are asked by policymakers is why, in light of this very significant expenditure, are so few care providers able to share patient information?

There is a very simple answer to that question: too many of those federal dollars have subsidized the adoption of systems that either cannot or deliberately do not interoperate outside of proprietary vendor platforms, perpetuating the non-interoperable status quo that the program is intended to change. There are legitimate market demands for closed information networks in healthcare. If, however, an overriding objective of federal health IT policy is to foster data fluidity and information sharing in healthcare, then at a minimum federal dollars should not be spent to subsidize the acquisition and use of technologies that cannot or do not enable providers to share information outside of proprietary networks.

Indeed, the same arm of government that disburses those subsidies is now defining as a "hardship" the use of some of the very systems that have been subsidized, to allow providers a mechanism to avoid scheduled reimbursement penalties for failure to successfully attest to "meaningful use" due to vendor failings.[3] A pending rule proposed by the Center for Medicare and Medicaid Services ("CMS") will continue to actively subsidize old EHR systems that prior rulemakings stated would not be eligible for a subsidy beginning in 2014.[4] To say that fact is a glaring indictment of current MU policy is an obvious understatement.

Actual interoperation (as distinguished from the mere capability of "interoperability") should be a baseline prerequisite for MU certification. Until it is, the federal government will continue to pay for

---

[3] CMS EHR Incentive Program Payment Adjustment and Hardship Exceptions Guidance. http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/paymentadj_hardship.html.

[4] *CMS rule to help providers make use of Certified EHR Technology*. http://www.cms.gov/newsroom/mediareleasedatabase/press-releases/2014-press-releases-items/2014-05-20.html.

systems that impede one of the few bipartisan, bicameral objectives of health care reform. More to the point for present purposes, existing policy artificially distorts the EHR marketplace, providing a taxpayer-funded subsidy for technology platforms that do not meet the basic standards of 21st century information technology, and that absent that market distortion would more quickly be phased out by ordinary market competition.

b. Legal impediments to ordinary market dynamics in healthcare impede information sharing, which in turn stifles innovation.

In most every functioning marketplace across the economy, high-quality, curated data is treated as the valuable, innovation-fueling commodity that it is. Market participants in need of data are able to pay fair market value for that data. And those payments are used, in part, to build and maintain the necessary technological infrastructure to enable the efficient, secure exchange of both information and value. This is true everywhere from the banking and online trading systems to the national information network that enables the tracking and exchange of after-market auto parts.

In healthcare, however, because the transfer of patient data occurs most frequently in the context of a care referral any accompanying transfer of value is deemed illegal remuneration under the Stark Laws and/or the Anti-Kickback Statute. As a result, in healthcare the owner/curator of quality data is obligated to assume the cost of electronic transfer of information to a recipient. The beneficiary of the work and the infrastructure investment necessary to curate that data and enable its secure and efficient transfer—the recipient—is literally legally prohibited from paying fair market value for that work and investment. This paradigm, which forces the curator of data to pay for the privilege of sending it electronically to a recipient, operates as a very effective economic disincentive to innovation, investment in technology, and information sharing in healthcare.

Again, the solution to this problem is straightforward: policymakers must recognize that laws intended to prevent fraud and abuse in a fee-for-service world, written before the age of rapid innovation in information technology, are in current practice overbroad in their application and actively impeding desired information sharing in healthcare.

The 21st Century Cures initiative is much needed in health care today, and we applaud the Committee for taking on such an important issue. Health IT is increasingly the platform through which all care is delivered, and we will never be able to achieve the goal of improved quality of care at lower costs using 20th century technology. Thank you for the opportunity to provide feedback on this initiative. We look forward to working with the Committee on this topic and are of course willing to discuss these comments further at your convenience.

Sincerely,

Dan Haley
VP, Government and Regulatory Affairs