athenahealth

In Defense of the PROTECT Act

Introduction

Earlier this month Senators Deb Fischer (R-Neb.) and Angus King (I-Maine) introduced the PROTECT Act. Like the SOFTWARE Act, introduced last year in the House by Representative Marsha Blackburn (R-TN), the PROTECT Act would lay the groundwork for a new oversight framework to ensure the safe development, implementation and use of health information technology (health IT). Despite the Act's reasoned approach to risk-based regulation of health IT, the mHealth Regulatory Coalition and the CDS Coalition (which are functionally the same organization, steered by the same individual) have responded in staunch opposition, with a document that purports to list "Examples of Software That Would Be Deregulated Under the Protect Act"—a list intended to frighten off potential supporters of the PROTECT act by claiming (falsely in the vast majority of cases) that certain high-risk technologies would be freed from all regulatory oversight were the PROTECT Act pass into law. A collection of advocacy groups comprised of the American Medical Women's Association, the Annie Appleseed Project, Jacobs Institute of Women's Health, the National Consumers League, the National Physicians Alliance, NRC for Women and Families, the National Women's Health Network, Public Citizen, the TMJ Association, the Union of Concerned Scientists, the National Coalition for Women with Heart Disease, and Woody Matters also sent a letter to Senator Tom Harkin (D-IA) raising a number of concerns about the PROTECT Act.

This document responds to those missives, acknowledges the legitimate concerns and criticisms raised by the coalitions and suggests constructive ways to address those concerns, and clarifies both the intent and the functional impact of the PROTECT Act with regard not only to the specific technologies (and categories) listed in that document, but also more broadly.

Background

As a prefatory matter it is important to establish the current regulatory structure applicable to health IT. The extremely broad definition of "device" (21 USC 321(h)), last revised in the 1970s, grants to the Food and Drug Administration ("FDA") unfettered 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 information technology under the broad authority of a statute last revised before any of the technologies in question existed. This is inappropriate and counter-productive in a number of ways:

1. The vast majority of health IT is fundamentally different from the medical device technologies that the FDA traditionally regulates. Potential patient safety issues with health IT, to the extent that they exist, arise in its implementation, customization, and use, not from 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. In fact, the FDA does not even have jurisdiction to police the contexts in which most health IT is implemented and used: hospitals, physician offices, and other care settings. This lack of authority makes the FDA a wholly inappropriate regulator for health IT. The PROTECT Act aims to provide appropriate, risk-based oversight for health IT that does not require a vast and disruptive extension of FDA jurisdiction.

2. 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. Even if taken wholly at face value, such an assertion is of inherently limited value, since "present regulatory intent" is non-binding and susceptible to revision at the agency's discretion.

3. 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 that FDA proposes to do via "enforcement discretion"—define (and periodically redefine) the boundaries of its own regulatory reach.

The PROTECT Act

To vindicate Congress's proper Constitutional role by setting appropriate boundaries around FDA jurisdiction, the PROTECT Act defines two new statutory categories of health IT: clinical software and health software. Because the technologies within those categories present little to no 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 Act removes those technologies from FDA regulation and instead subjects them to a new oversight framework better tailored to the unique nature of health IT.

Contrary to the claims made by opponents of the PROTECT Act, the Act would not leave clinical and health software unregulated. 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 PROTECT Act is a freshly introduced bill, the specific language of which can and likely will be refined through the legislative process. Opponents of the Act make some valuable points, and those points suggest potentially appropriate revisions to the Act's definitions (explained below).

Specific responses to each critique by the mRC and CDSC of the PROTECT Act:

These coalitions incorrectly assert that certain high risk clinical decision support (CDS) technologies, as well as mobile medical apps and software with medical device functionality, would be "deregulated" by PROTECT . Specifically:

1. **Apps and other software that guide untrained users to make very complex medical decisions**

   Response:
   Many of the examples that fall into this category of software would remain under FDA regulation under section (ss)(3)(A) on page 5 of the PROTECT Act, which exempts from the definitions of clinical and health software any software that interprets patient-specific device data to directly diagnose a patient without the intervention of a health care provider. Consumer use melanoma and sports concussion injury apps would both fall under this exemption.
   Ironically, some of the examples set forth in this category are arguably subject to FDA "enforcement discretion" (meaning they are effectively unregulated for the time being) today. By defining these

examples as clinical or health software, the PROTECT Act would subject them to sensible oversight—effectively increasing rather than decreasing the amount of scrutiny given to these technologies. For example:

- Disease managers for patients are specifically identified in the FDA's October 2013 Mobile Medical Applications Final Guidance (MMA Guidance) as software for which the FDA intends to exercise discretion, as are apps that provide or facilitate supplemental clinical care by prompting or coaching patients (*see* sections (V)(B)(1) and (2) of the MMA Guidance). Neither technology is, according to the FDA, currently under active regulation.

- Drug dose calculators often merely automate what was previously done by clinicians with pen and paper. The FDA specifically disclaimed in the MMA Guidance any intention to actively regulate this variety of software (*see* section (V)(B)(5) of the MMA Guidance). Drug dose calculators that perform radiological treatment calculations would remain FDA-regulated, as they are today, under (ss)(3)(B) on page 5 of the PROTECT Act (which exempts software that conducts analysis of radiological data to provide patient-specific treatment advice).

Legitimate concerns raised by the coalitions about the potential impact of the PROTECT Act on certain CDS could be adequately addressed via a minor amendment to the language in (ss)(3)(A) on page 5 of the Act. Revising that section to explicitly include apps that provide *"treatment"* advice, by interpreting patient-specific device data without the intervention of a health care provider (meaning that the patient follows advice from the software directly without needing to consult a clinician) would ensure appropriate oversight of apps such as disease managers that vary treatment advice based on device input (*e.g*., a blood glucose monitor). It would also close the potential loophole identified by the coalitions that makers of the melanoma and concussion apps, for example, could evade oversight by arguing that their apps only help a patient determine whether to see a clinician (which is a type of treatment advice).

2. Software used in a setting that does not allow the doctor sufficient time to second-guess the software

Response:
Much of the higher risk software in this category, such as the technology used by EMTs or by nurses for in-patient monitoring, would remain FDA-regulated under the PROTECT Act, because it is software that is conducting an analysis of imaging or radiological data, is integral to a currently-regulated medical device, or is a component of a currently-regulated medical device (see section (ss)(3)(B), (C), and (D) on page 5 of the PROTECT Act).

To address legitimate concerns raised by the coalitions, the language in section (ss)(3) on page 5 of the PROTECT Act could be strengthened by including an additional exemption to the definitions of clinical and health software for technologies upon which a clinician is intended to be substantially dependent for the diagnosis, treatment, cure, mitigation or prevention of a life-threatening disease or other condition. For such an exemption to be workable, however, the term "substantially dependent" must be tightly defined: a clinician should only be considered "substantially dependent" 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; 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.

3. **Software that takes a very complicated calculation and presents a result without transparently revealing the basis for the calculation.**

   Response:
   Software in this category would often remain FDA-regulated for all of the reasons stated immediately above—most would fall under section (ss)(3)(B)(C) or (D) on page 5 of the PROTECT Act. The inclusion of a "substantial dependence" exemption to clinical and health software in the PROTECT Act would also ensure that all software in this category is properly overseen.

4. **Mobile medical apps and other medical device functionality.**

   Response:
   Sections (ss)(3)(C) and (D) on page 5 of the PROTECT Act ensure that medical device functionality remains FDA-regulated, regardless of whether such functionality runs on a mobile or other platform. Where a mobile platform is effectively transformed into one of the medical devices identified by the coalitions, the mobile software running the device would clearly either be integral to the function of or a component of the device. For example, drug calculators that automate simple calculations are not currently FDA-regulated, as explained above. Calculators that are integrated with a device that is administering or otherwise controlling the dispersing of the drug, however, are integral to the device and therefore are and would remain FDA-regulated. Similarly, where a mobile platform is used as the primary display of a medical device, the mobile software is integral to the function of the device because the data cannot be accessed without the primary display. That software would remain FDA-regulated under the clear language of the PROTECT Act.

Responses to the American Medical Women's Association, *et. al*, February 14, 2014 Letter to the Honorable Tom Harkin, Chairman of the US Senate Health, Education, Labor and Pensions Committee

Responses to each objection raised in the February 14 letter to Chairman Harkin are as follows:

1. **The Act is premature because Congress is still awaiting the study that it commissioned in the Food and Drug Administration Safety and Innovation Act (FDASIA) of2012 requesting that agencies make recommendations on an appropriate, risk-based regulatory framework for health IT.**

   Response:
   There is no foundation for the proposition that Congress is obliged to wait on a recommendation that Congress itself ordered—a recommendation that is, as of this writing, nearly two months overdue. More to the point, in FDASIA Congress directed the FDA and its sister agencies to recommend a comprehensive, risk-based regulatory framework for health IT. It did not via that directive authorize the agency to define its own jurisdiction. In the nearly two years since FDASIA, FDA has moved steadily to consolidate its authority over health IT, first by issuing premature mobile "guidance" last summer, and then more recently by previewing its intended CDS guidance, due to be released shortly following publication of the FDASIA report. The PROTECT Act properly reasserts Congress's prerogative (indeed, its duty) to set the parameters of executive agency regulation. By

setting those parameters in advance of the FDASIA report, Congress is appropriately defining the context in which the FDASIA report's recommended framework should be crafted.

2. **The Act undermines FDA's proper role and patients' reliance on the FDA to ensure that devices are reasonably safe and effective.**

Response:
It is indisputable that patients rely on the FDA to ensure that medical devices are safe, and sometimes that they are effective. Software is not a medical device. Indeed, this point goes to the heart of the rationale for Congressional intervention to ensure that software is not inappropriately subjected to the FDA's onerous device framework. Further, as previously noted, potential safety risks raised by health IT, to the extent they exist, occur in its implementation, customization and use, not in its design and development. The FDA does not have authority to oversee the implementation, customization or use of health IT in the care settings where these activities happen.

3. **The Act does not ensure that any agency will validate the effectiveness of technology, which could harm patients through inaccurate results.**

Response:
The *current regulatory environment* does not ensure that any agency will validate the effectiveness of health IT. Currently, the FDA does not evaluate the effectiveness of every device that it regulates. It only evaluates devices that fall in the higher-risk Class II and III categories. Yet by the FDA's own stated classification structure and enforcement discretion strategy, the vast majority of health IT falls under the lower-risk Class I or is not classified at all. By creating a new oversight structure for clinical software, the PROTECT Act facilitates a more thoughtful approach for these lower risk technologies, while leaving the riskier Class II and III technologies—health IT or otherwise—to be evaluated by the FDA.

4. **The Act muddles the definition of device by creating categories that can potentially overlap with the current definition of device, yet not be regulated as devices.**

Response:
The PROTECT Act defines two new categories of health IT and removes them from the definition of device. No potential overlap is created: either a technology is clinical software, health software, or it remains a device regulated by the FDA. The current definition of device was written in the 1970s, long before the advent of today's information technologies. That definition is overly broad and inapplicable in many ways to modern reality. Clinical and health software should not be regulated as devices, because device regulation does not appropriately ensure the safe use of these technologies. A new oversight framework for clinical and health software will better achieve that important objective.

5. **MRIs and CT scanners and heart monitoring devices may all be no longer regulated under the Act.**

Response:
There is no basis whatsoever for this claim. The PROTECT Act only applies to software. MRI machines, CT scanners, heart monitoring devices, and the majority of what the FDA currently regulates are traditional devices comprised of hardware, not software. To the extent that these

devices have software components, that software clearly would remain under the FDA’s jurisdiction under sections (ss)(3)(C) and (C) on page 5 of the PROTECT Act, which exempt from the definitions of clinical and health software any software that is integral to the function of or a component of a device. Device manufacturers would not be able to use the definitions of clinical or health software to escape regulation based solely on the fact that a device includes some software.

6. **The Act’s finding that the National Institute of Standards and Technology (NIST) should oversee the standards used to ensure safety in clinical software will harm patients because NIST’s role is to promote US innovation and competitiveness, which would undermine the FDA’s mission to protect public health by assuring the safety and efficacy of drugs, biological products, and medical devices.**

Response
Health information technology is not a drug, a biological product, nor a medical device. It is unclear why standards developed by NIST for health information technology should be expected to undermine any facet of the FDA’s important mission. NIST is the appropriate agency to ensure that flexible standards are developed to promote safety and innovation in the development, implementation, customization, and use of health IT because it has the technical expertise to evaluate the entire software life-cycle. The FDA simply does not have this technical expertise or infrastructure. Once NIST establishes standards, other agencies with public-health-oriented missions will be able to leverage those standards to ensure patient safety. For example, the Centers for Medicare and Medicaid can include implementation and use standards in its conditions of participation for health care providers, and the Office of the National Coordinator for Health IT can include development standards in its certification rules for the Meaningful Use program.