

Appendix E

Dissenting Statement: Health IT is a Class III Medical Device

Richard I. Cook, M.D.

This appendix is a dissenting statement from committee member Richard Cook, and contains his alternate recommendation for the regulation of health IT.

Recommendation 9: The Secretary of Health and Human Services should direct the FDA to exercise its authority to regulate health IT, including all EHRs and associated components, and health information exchanges, as Class III medical devices.

Medical and diagnostic devices have produced a therapeutic revolution, but in doing so they have also become more complex and less easily understood by those who use them. When well designed, well made, and properly used they support and lengthen life. If poorly designed, poorly made, and improperly used they can threaten and impair it. (President Gerald Ford, signing statement for Medical Device Amendments, May 28, 1976)

Rationale

Proponents and critics agree that health IT plays an important role in patient care and patient safety. Rather than being an adjunct or appendage of health care delivery, health IT is necessarily intimately woven into the fabric of patient care. Electronic medical records, digital imaging, provider order entry, and test results delivery do not “have an effect” on core medical functions; they *are* core medical functions. In contrast with, for example, electronic medical textbooks, health IT involves the generation, manipulation, storage, and display of patient- and provider-*specific* data. This need for specificity imposes special requirements on information technology. When a provider reads a laboratory result from the computer screen or enters an order for a medicine by mouse or keyboard, the patient context matters a great deal.

Until now, health IT’s quality, accuracy, precision, reliability, and safety have been left almost entirely to vendors. Although facilities and, to a lesser extent, users can configure and adapt health IT for their own uses, as a practical matter it is the vendors who control what health IT looks like and how it performs. While this may be reasonable for consumer or even some commercial software and hardware, it is unacceptable for health IT that must provide high-level performance in a hazardous environment. Medical practice is inherently hazardous and devices used to care for patients are regulated.

E-1

PREPUBLICATION COPY: UNCORRECTED PROOFS

Is health IT a medical device? If so, in the United States, the Food and Drug Administration (FDA) is charged with its regulation. According to law, a medical device is

...an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is—

- (1) recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them,
- (2) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or
- (3) intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes. [Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 321 SEC. 201]

Health IT components include items such as computerized provider order entry (CPOE), electronic medical records (EMRs), or electronic health records (EHRs). These components participate directly in diagnosis, cure, mitigation, treatment, and prevention of specified individual human beings. Health IT is a medical device and the FDA is or should be its regulatory body.

The 1976 Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act established three regulatory classes for medical devices. Class I devices are the simplest and are least likely to cause direct or indirect harm. The *tongue depressor* is a Class I device (its entry is in the Code of Federal Regulations at 21 CFR 880.6230). Class II devices include devices more likely to present some risk of harm. The *hearing aid* is a Class II device (21 CFR 801.420). The amendments define a Class III device as “one that supports or sustains human life or is of substantial importance in preventing impairment of human health or presents a potential, unreasonable risk of illness or injury.” Class III includes obvious high-risk devices such as external cardiac defibrillators (21 CFR 870.5310) but also includes HIV tests (21 CFR 864.4020).

What class of medical device is health IT? Because some health IT device characteristics may require a different approach to regulation than is practical under current classification rules, perhaps health IT should have its own classification. Under existing rules, however, I believe that health IT should be classified as a Class III medical device for at least three reasons.

First, health IT functionality is widely regarded as essential for safe care. The proponents and vendors of health IT regularly and consistently point to the safety afforded by the use of health IT. According to the IOM, human clinician errors are a major cause of morbidity and mortality (IOM, 1999). Preventing human clinician errors is one of the main functions of health IT and a primary rationale for the \$32 billion investment in health IT committed by the Recovery Act of 2009. This surely makes health IT of “substantial importance in preventing impairment of human health,” which is the central criterion of a Class III device.

Second, adoption of health IT has pervasive effects on basic health care delivery. Its use affects virtually every activity that takes place in a hospital, clinic, or doctor’s office. Health IT receives, stores, and displays clinical information. It accepts, validates, and transmits orders for care and treatment. It notifies physicians, nurses, pharmacists, and technicians of patient conditions. It tracks clinical actions and assessments. These are not trivial functions and their

PREPUBLICATION COPY: UNCORRECTED PROOFS

accuracy and reliability have direct impact on virtually every patient's well-being. Adopting health IT amounts to putting all the clinical eggs in a single basket. Unlike other medical devices, most of which have effects on a few hundred or thousand patients, health IT is on track to be *a medical device used for every person in the United States*.

The third reason it is a Class III device is that health IT *can and does* cause significant harm to patients. At least a few U.S. citizens—perhaps more than a few—have died or been maimed because of health IT. The extent of the injuries generated by health IT is unknown because no one has bothered to look for them in a systematic fashion. Indeed the failure to treat health IT as a medical device has played a significant role in keeping the problems with health IT from becoming known. Medical device manufacturers are obligated to report instances of patient harm connected to their devices. Health IT vendors are not. Problems and the resulting hazards from health IT cannot be addressed and fixed without first being identified through some form of reporting. The government's failure to treat health IT as a medical device has allowed manufacturers to keep the problems with health IT hidden and has made it possible for vendors to require contractual “gag clauses” that restrict open discussion of its problems.

Simply declaring health IT to be a medical device—even a Class III medical device—will not rectify the safety problem that health IT creates. It will, however, begin to bring this burgeoning area out of the shadows and into the light. This is a necessary part of improving its impact on patient safety.

Accidents involving health IT are complex events that require substantial forensic skill to detect and describe. The impact of health IT on system safety is most easily understood in cases of overt computer outages (sometimes described as system “crashes”), which deny clinicians access to the data and communications that these systems usually provide. Absurdly, when such an outage becomes public knowledge the system owners uniformly declare that “no patient was harmed.” If so, the case for health IT must be weak indeed. There are presently no standards for assessing or reporting such outages or for judging their effects on safety.

But most of the impact of health IT on safety must be more subtle than the overt computer crash. The “copy forward” case described in Box E-1 is more representative. Here, data appear out of context and are misinterpreted. The simple existence of a datum inside a database does not ensure that its significance will be appreciated. Similarly, the appreciation of a datum in one circumstance does not ensure that it will be appreciated in all circumstances. Problems with “pick lists”—e.g, menus of medications, procedures, or laboratory tests—are common in other areas and also appear in reports of difficulties with health IT. It is remarkably easy to select the wrong patient or the wrong drug from these lists.

BOX E-1

An abdominal ultrasound report in an electronic record appeared to indicate a blighted ovum and a dilation and curettage (D&C) was performed a few days later. The patient returned to the ER 4 weeks after the D&C with abdominal pain. Repeat ultrasound revealed a 21 week pregnancy. A damaged fetus was delivered at 26 weeks. The ultrasound result had actually been obtained several weeks prior to the date of the record in which it appeared. The report had been copied forward into that record and appeared out of context.

PREPUBLICATION COPY: UNCORRECTED PROOFS

We know this not so much from studies of health IT as from experience in other domains. Indeed this experience is the basis for modern methods for IT designs for use in hazardous settings. It is not surprising that such events are now being discovered in health IT. *What is surprising is that those creating and promoting these large systems have neither anticipated them nor looked for them.* The development of health IT is marked by an optimism about the effects of IT that are unwarranted and naive. And the willingness to embrace this optimism to the extent of making large-scale investments in these systems and only later asking what their impact might be on patient safety borders on recklessness.

Mounting an effort to bring device regulation to health IT will be challenging and demands both added resources and new methodologies for the FDA. It is clear from a recent IOM report (IOM, 2011) that medical device regulation itself will benefit from careful review and revision. But make no mistake: health IT is a medical device. It should be regulated as a medical device now and should have been regulated as a medical device in the past.

REFERENCES

- IOM (Institute of Medicine). 1999. *To err is human: Building a safer health system*. Washington, DC: National Academy Press.
- IOM. 2011. *Medical devices and the public's health: The FDA 510(k) clearance process at 35 years*. Washington, DC: The National Academies Press.

PREPUBLICATION COPY: UNCORRECTED PROOFS