Original Investigation

Software-Related Recalls of Health Information Technology and Other Medical Devices: Implications for FDA Regulation of Digital Health

JAY G. RONQUILLO^{*,†}
and DIANA M. ZUCKERMAN[†]

**Western Michigan University Homer Stryker M.D. School of Medicine;*

†National Center for Health Research

Policy Points:

- Medical software has become an increasingly critical component of health care, yet the regulation of these devices is inconsistent and controversial.
- No studies of medical devices and software assess the impact on patient safety of the FDA's current regulatory safeguards and new legislative changes to those standards.
- Our analysis quantifies the impact of software problems in regulated medical devices and indicates that current regulations are necessary but not sufficient for ensuring patient safety by identifying and eliminating dangerous defects in software currently on the market.
- New legislative changes will further deregulate health IT, reducing safeguards that facilitate the reporting and timely recall of flawed medical software that could harm patients.

Context: Medical software has become an increasingly critical component of health care, yet the regulatory landscape for digital health is inconsistent and controversial. To understand which policies might best protect patients, we examined the impact of the US Food and Drug Administration's (FDA's) regulatory safeguards on software-related technologies in recent years and the implications for newly passed legislative changes in regulatory policy.

Methods: Using FDA databases, we identified all medical devices that were recalled from 2011 through 2015 primarily because of software defects. We

counted all software-related recalls for each FDA risk category and evaluated each high-risk and moderate-risk recall of electronic medical records to determine the manufacturer, device classification, submission type, number of units, and product details.

Findings: A total of 627 software devices (1.4 million units) were subject to recalls, with 12 of these devices (190,596 units) subject to the highest-risk recalls. Eleven of the devices recalled as high risk had entered the market through the FDA review process that does not require evidence of safety or effectiveness, and one device was completely exempt from regulatory review. The largest high-risk recall categories were anesthesiology and general hospital, with one each in cardiovascular and neurology. Five electronic medical record systems (9,347 units) were recalled for software defects classified as posing a moderate risk to patient safety.

Conclusions: Software problems in medical devices are not rare and have the potential to negatively influence medical care. Premarket regulation has not captured all the software issues that could harm patients, evidenced by the potentially large number of patients exposed to software products later subject to high-risk and moderate-risk recalls. Provisions of the 21st Century Cures Act that became law in late 2016 will reduce safeguards further. Absent stronger regulations and implementation to create robust risk assessment and adverse event reporting, physicians and their patients are likely to be at risk from medical errors caused by software-related problems in medical devices.

Keywords: medical device recalls, FDA, patient safety, software, electronic medical records, health information technology, health IT.

SOFTWARE IN MEDICAL DEVICES HAS BECOME AN INCREASINGLY critical component of health care. In many clinical settings, medical equipment and devices controlled by software have numerous applications, such as tracking patients' vital signs, alerting physicians to the risk of adverse drug events, and controlling the amount of medication that patients receive. The use of medical software, both in stand-alone form or integrated into other technologies, is becoming increasingly central to the practice of medicine.^{1,2} Health information technology (IT), for example, includes electronic medical records (EMRs), clinical decision support (CDS), mobile medical applications, and any software-driven medical device used in the diagnosis or treatment of disease.³ Hospitals often depend on software-controlled devices for routine

medical care and are leveraging large amounts of medical data generated, collected, and analyzed by software to help reduce medical errors, lower hospital readmissions, and understand population health.^{1,4}

Prior to passage of the 21st Century Cures Act in December 2016, the US Food and Drug Administration (FDA) was responsible for ensuring that medical devices (including EMRs and other health IT) were safe and effective for patients. However, as Table 1 shows, the regulatory landscape for software in medical devices is complex, with the FDA using both objective and subjective methods to categorize, review, and recall software devices that pose a risk to patients.⁵ The regulation of medical devices starts with a review of a device before it is allowed to be sold and continues after it goes on the market. The type of FDA product review plays a key role in risk assessment, since it determines the amount of evidence required for a product to be approved or cleared by the FDA. Premarket approval (PMA), the FDA's most stringent review process for devices, applies to software posing the greatest risk to patient safety and requires the manufacturer to provide clear evidence of safety and effectiveness. In contrast, products expected to pose less risk to patients, and thus go through the 510(k) review process, are not required to be proven safe, effective, or accurate but instead must demonstrate that they are similar to a product already sold in the United States in order to be cleared for market by the FDA.^{6,7}

Through their existing regulatory infrastructure, the FDA classifies all products according to their general risk to patients (see Table 1): Class I devices have the lowest risk; Class II devices have a moderate risk; and Class III have the highest risk.⁶ In addition, the FDA has the authority to recall a device after it goes on the market; it defines such recalls as the removal or correction of a marketed device in violation of FDA law.⁵ Recalls can be initiated by either the manufacturer or the FDA if a medical device is determined to be a risk to patient health or safety; any voluntary recalls by the manufacturer must be reported to the FDA.⁵ The FDA recalls devices using a classification system based on the severity of their potential to cause harm. In this system, Class I recalls are those that pose the highest risk to patients; Class II recalls are those that pose a moderate risk; and Class III recalls are those that pose a relatively low risk to patients.^{5,6}

In 2015 and 2016, the FDA published several guidance documents for industry, describing its approach to regulating the growing

Table 1. FDA Medical Device Regulatory Categories

Medical Device/ Software	Low Risk Class I	Moderate Risk Class II	High Risk Class III
FDA Review Type	Exempt from any application materials	510(k): Does not require clinical trial or evidence of safety or effectiveness but must be “substantially equivalent” to a device already on the market that was also subject to 510(k) review. Premarket inspections not allowed.	PMA: Requires proof of being “reasonably safe and effective” based on one premarket clinical trial and premarket inspection of manufacturing facility.

number of software devices. The guidance also discusses the FDA's plans to exercise its enforcement discretion by not actively regulating software that does not perform clinical analysis, such as medical device data systems that exchange or display medical data, medical image storage and communications devices, and low-risk general wellness software focused on maintaining a healthy lifestyle.^{8,9} Instead, the FDA planned to regulate software that involves the direct diagnosis or treatment of disease, or software that could lead to serious harm if it malfunctioned.

Once a medical product is on the market, there are voluntary and mandatory reporting and monitoring policies in place. The US Congress first gave the FDA the authority to regulate medical devices by amending the Food, Drug, and Cosmetics Act in 1976, leading to the creation of the PMA and 510(k) review processes for medical devices described earlier.⁶ Over time, the scope and complexity of medical devices and innovations have continued to expand rapidly. The Health Information Technology for Economic and Clinical Health (HITECH) Act passed in 2009 focused on converting paper medical records into electronic form, which has led to the rapid adoption, by most hospitals and clinics throughout the country, of EMRs, clinical decision support, and other health information technologies.¹⁰

The FDA Safety and Innovation Act's (FDASIA's) working group is a collaboration of the FDA, the Office of the National Coordinator for Health IT, and the Federal Communications Commission. The working group has recommended a risk-based regulatory framework to address safety-related concerns for health IT.³ Its proposed framework places eligible health IT products into 3 risk categories (low, medium, high) based on a group of factors, including product purpose, intended audience, severity of potential injury, complexity of software and upgrades, required amount of training, and degree of connectivity and security.³ The FDASIA's recommendations would apply to diverse types of health IT software and underscore the need to find a balance between fostering innovation and ensuring that patient populations are protected from the potential risks associated with software devices.

Important concerns about the regulation and safety of software in health care have frequently been raised and continue to be a critical topic of discussion.¹¹ The 21st Century Cures Act, which was signed into law in December 2016, removes electronic medical records, decision-support

software, and related stand-alone software from the FDA's regulatory jurisdiction.¹² Understanding the possible risks and benefits of the FDA regulation of software in its diverse forms, along with the impact of these legislative changes in the FDA's regulatory scope, is important to the future of health care.

Unintended software-induced medical errors, remote hacking of medical systems, and recent cybersecurity breaches of hospitals' EMRs are proof of the real and growing risks to patients if software defects are not monitored consistently. Unfortunately, there is currently very little published information available that describes the impact of health IT and other types of software on patient safety.¹¹ Earlier studies have investigated general safety issues in only a small number of medical devices or in only a few types of software.¹³⁻¹⁵ The ECRI Institute, for example, publishes a list each year of its 10 most important "generic hazards—problems that result from the risks inherent to the use of certain types or combinations of medical technologies."¹⁴ The institute's most recent list of health technology hazards includes at least 3 medical products (infusion pumps, ventilators, medical device software management) with safety risks tied, at least in part, to faulty software.¹⁴ However, to our knowledge the safety and regulatory implications of all software-related defects in medical devices have not been systematically analyzed.

In order to determine which policies might best protect patients, we have evaluated whether the regulation of medical software has provided essential safeguards for patient safety. The goal of our study was to determine the frequency of software-related recalls in medical devices, including more recent technologies like EMRs, and to examine key issues that the FDA determined could cause injury, serious harm, or even death.

Methods

In order to better understand the types of software malfunctions that could affect clinical care, we searched the FDA medical device databases over the most recent 5-year period for all medical devices recalled by the FDA primarily because of software defects.¹⁶

The FDA's database for medical device recalls is accessible online and can be searched by providing specific search criteria (eg, recall class, date

range). We performed a broad search for all medical devices that were recalled between January 1, 2011, and December 31, 2015, primarily because of their software, as coded in the database. We counted both the numbers of low, moderate, and high-risk recalls and the reported number of units of each recalled product on the market.

In addition, for the high-risk recalls and recalls of EMRs, we collected information about the recalling firm or manufacturer, device classification, submission type, medical specialty, product details, and categorization as either an implantable or a life-sustaining device. We then merged the search results, identified devices for which the manufacturer- or FDA-reported reason for recall directly involved software, and, finally, standardized the data (eg, removed duplicates and treated multiple products with the same manufacturer, recall date, and event identifier as single entries).

For all those high-risk recalls that satisfied those criteria and also for moderate-risk recalled EMRs, we used the FDA's databases to determine the type of testing used as the basis of the FDA's regulatory determinations that allowed the devices to go on the market. This included reviewing any relevant data or testing information described in device companies' 510(k) publicly available summaries, as described in an earlier study.⁷

We calculated our descriptive statistics using Microsoft's Excel Version 14.0 (Redmond, WA).

Results

Characteristics of Software-Related Recalls

Over the 5-year study period, 627 different devices (1,447,134 units) were recalled because of software-related issues, of which 23 devices (5,140 units) were low-risk recalls, 592 (1,251,398 units) were moderate-risk recalls, and 12 (190,596 units) were high-risk recalls.

The high-, moderate-, and low-risk categories of the recalls were not related to whether the devices were considered high, moderate, or low risk when they were initially submitted to the FDA for approval. Of the highest-risk software recalls (Table 2), the FDA initially classified only 1 of the 12 devices (Defibtech) as a high-risk (Class III) device when it was reviewed for approval, and it classified 11 of the 12 as

Table 2. FDA High-Risk Recalls due to Software, 2011-2015

Device	Manufacturer	FDA Review	Evidence Mentioned	No. Units
ABACUS TPN Calculation Software	Baxter Corporation	Exempt	Summary unavailable	2,034
Alaris PC unit model 8015	Carefusion Corporation	510(k)	Nonclinical	9,241
Alaris Pump module 8100	CareFusion 303, Inc.	510(k)	Nonclinical	55,756
Covidien Puritan Bennett 980 Ventilator	Covidien	510(k)	Nonclinical	324
Evita V500 and Babylog VN500 Ventilators with Optional PS500 Power Supply Unit	Drager Medical, Inc.	510(k)	Nonclinical	2,422
HAMILTON-T1 Ventilator	Hamilton Medical Inc.	510(k)	Nonclinical	97
Lifeline AED and ReviveR AED	Defibtech, LLC	510(k)	Nonclinical	91,472
McKesson Anesthesia Care System	McKesson Technologies Inc.	510(k)	Summary unavailable	10
Medfusion 4000 syringe infusion pump	Smiths Medical ASD, Inc.	510(k)	Nonclinical	257
NicoletOne Software with Cortical Stimulator License	CareFusion 209, Inc.	510(k)	Nonclinical	167
Puritan Bennett 840 Ventilator	Covidien	510(k)	Nonclinical	16,756
Respironics V60 Ventilator	Respironics California Inc.	510(k)	Nonclinical	12,060

Abbreviations: AED, automated external defibrillator; TPN, total parenteral nutrition.

moderate-risk (Class II) devices. The high-risk device and all but one moderate-risk device were reviewed and cleared for market by the FDA through the 510(k) review process, which is generally intended for moderate-risk devices (see Table 1). The one moderate-risk (Class II) device, “ABACUS Total Parenteral Nutrition Calculation Software,” was exempted from any FDA regulatory review because the FDA initially considered a regulatory review to be unnecessary. The FDA classified half of the high-risk recalled software devices as life sustaining, and none were implantable. The scope of the high-risk recalls varied widely in volume, ranging from only 10 units (McKesson Anesthesia Care System) to 91,472 (automated external defibrillators made by Defibtech), with a median of 2,228 units (interquartile range 234 to 13,234).

Medical Specialties of Devices Recalled as High Risk

The largest category of high-risk software-related recalls pertained to anesthesiology, with 6 devices, of which 5 were ventilators and 1 (McKesson) was a clinical decision support system (see Table 2). The manufacturers’ summaries in the FDA’s recall database explain that the software defect could lead to premature stoppage of mechanical ventilation and that the CDS software defect could lead to the storage of the wrong (ie, another patient’s) data for the current patient.

Four general hospital devices made up the second largest category, comprising one-third of the highest-risk recalls. Of these devices, 3 were infusion pumps designed to directly administer fluids or medications to patients. The FDA’s database described malfunctions in software (eg, device log corruption, communication error, broken timer functionality) that could lead to either the over- or the under-infusion of medications and fluids. The final device in this category calculated total parenteral nutrition (TPN), in which a malfunction caused the incorrect calculation and/or display of information, which could result in either highly diluted or toxic amounts of intravenous nutrition being given to patients. The recommended solutions for infusion pumps ranged from upgrading the software to contacting the manufacturer for repair, and the TPN software solution required health care providers

to perform additional time-consuming steps when interacting with the system.

The remaining products subject to the highest-risk recalls included one neurology device and one cardiovascular device. The neurology software problem affected the cortical stimulator control unit used to perform functional brain mapping, which helps surgeons decide which parts of the brain to remove in order to treat tumors or epilepsy.¹⁷ The cardiovascular product was an automated external defibrillator (AED) in which a software error could cause the AED to cancel electrical shock treatment to a patient in cardiac arrest.

Types of Premarket Studies of Software Devices from High-Risk Recalls

The only software device that was subject to a high-risk recall after being classified as high risk (Class III) before approval was also cleared through the 510(k) process, as noted earlier. Of the 11 software devices reviewed through the 510(k) process, none was tested in clinical trials to determine safety or effectiveness. In their publicly available 510(k) application summaries, the manufacturers stated that they performed nonclinical testing (eg, simulation, performance testing, software validation) to determine substantial equivalence to software devices already on the market. We did not include the type of nonclinical testing in Tables 2 and 3 because none of the summaries for the devices in this study provided testing data to prove substantial equivalence, even though the summaries are required by law to provide such data.⁷ For example, the 510(k) summary for the Covidien Puritan Bennett 980 Ventilator mentioned building more than 50 units “for different aspects of Verification and Validation testing” but did not provide further supporting details or data to describe their performance testing.¹⁸

Subanalysis of Software Recalls for EMRs

Of the 592 moderate-risk recalls due to software errors, 5 were EMR systems, with a total of 9,347 units (Table 3). The EMR defects were incorrect drug dosage calculations (MOSAIQ 2.6), treatment files (MOSAIQ 2.4), and medication order status (CareSuite), as well as failed allergy interaction warnings (ED PulseCheck) and the display

Table 3. FDA Recalls of EMRs (Moderate Risk), 2011-2015

Device	Manufacturer	FDA Review	Evidence Mentioned	No. Units
MOSAIQ Oncology Information System Release 2.6	Elekta Inc.	510(k)	Nonclinical	399
MOSAIQ Oncology Information System Release 2.4	Elekta Inc.	510(k)	Nonclinical	300
Picis Anesthesia Manager	Picis Inc.	Exempt	N/A	10
Picis ED PulseCheck	Picis Inc.	Exempt	N/A	62
CareSuite Critical Care Manager	Picis Inc.	Exempt	N/A	8,576

of medical information for the wrong patients (Picis Anesthesia Manager).

Discussion

Software plays an increasingly central role in the practice of medicine, and the regulation of these technologies has important implications for patient safety. Our study is timely, given the rapid adoption of software and health IT, increased concern for medical device cybersecurity vulnerabilities, Trump administration plans to revamp health IT regulations, and the recently passed 21st Century Cures Act that will deregulate many health technologies.^{10,19-22}

More than 190,000 software units were subject to high-risk recalls and were products that treated a broad range of patients in diverse clinical settings. More important, although many recalled devices, such as implants, pose a risk to only one patient, each EMR can be used for hundreds or thousands of patients served in a medical practice or hospital. Furthermore, other software devices are also often reused repeatedly on different patients, amplifying the potential impact of each unit recalled. The recalled ABACUS TPN software, for example, is a “Windows-based software application used by pharmacists to calculate or order TPN formulas,” and its flawed calculations could have affected every patient being treated during the 8 years it was on the market.²³ Other recalled software-controlled devices, such as ventilators and infusion pumps, are cleaned, sterilized, and reused many times on multiple patients. The types of software flaws leading to the high-risk recalls described in this study (eg, computer screens freezing, storage of wrong patient data, formula calculation errors) are not limited to products considered as high risk but could apply to almost any software device being used by health care providers.

The design of current health IT software can result in unintended consequences and medical errors that are hard to detect, challenging to monitor, and harmful to patients.^{13,24-26} For example, the McKesson clinical decision support system notifies physicians of possible adverse drug events for all patients during surgery. But since software flaws led to loading the wrong patient data, this warning system was not uniformly safe and effective for all surgery patients. These types of software issues would be magnified for hospitals with heavy patient

loads and would apply to those EMRs commonly used for all patients in a particular hospital. Although recent cybersecurity issues, such as the remote access/control (“hacking”) of drug infusion devices and the breach (and subsequent ransom) of electronic patient records by unauthorized users have not yet led to recalls, they underscore the serious vulnerabilities of software that is increasingly scalable and interconnected.^{14,21,27,28}

The results of our study provide insights into the FDA’s regulatory review process and postmarket surveillance of software devices before the regulatory changes that will be implemented in accordance with the 21st Century Cures Act or by the new FDA commissioner nominated by President Trump and confirmed in 2017. Although premarket testing is not infallible, greater FDA scrutiny during the premarket approval process could have reduced the introduction of defective software devices into the market and reduced the number of high-risk recalls. For example, only 14 recalled devices in the 5-year study were approved through the FDA’s PMA process, which is the only device review that requires proof of safety and effectiveness through a clinical trial or other scientific analysis; the defects later found in these devices resulted in low- or moderate-risk, not high-risk, recalls. In contrast, none of the high-risk recalls involved devices that had been reviewed through the more rigorous (PMA) process. The one device that had been exempted from any FDA review shows that even health IT that seems to pose little risk—in this case, nutrition calculation—can still result in life-threatening dangers.

The fact that none of the devices that the FDA recalled as having a high risk had been classified as high risk during the review process suggests that it underestimated the risk of these software devices before granting approval and therefore did not require them to be proven safe or effective as part of its review process. Instead, these devices were required to show “substantial equivalence” to other devices on the market, which were similarly not required to be proven safe or effective.⁷ AEDs, for example, were classified as high-risk devices but were reviewed under the less stringent 510(k) process for years until a large volume of medical device reports and recalls associated with AED failure resulted in a change in FDA policy requiring PMA applications in 2015.²⁹ This evidence gap has been described as a fundamental flaw of the 510(k) review process, in reports by the National Academy of Medicine (formerly the Institute of Medicine) and others.^{6,30}

Although the 510(k) application summaries provided by manufacturers do not provide data, they do indicate that their software often underwent some type of performance and validation testing. Unfortunately, these software engineering approaches were not designed for assessing safety-related issues.^{31,32} More specifically, while performance and validation testing can find several important “bugs” and technical flaws, they are not able to ensure that the software will perform optimally in most safety-critical situations, such as those common in health care.^{31,32} Successfully addressing these issues in the future will require a multidisciplinary approach involving the application of new areas of informatics and computer science (eg, safety-critical computing) to health care.^{33,34}

Our findings also provide insight into the potential impact of the 21st Century Cures Act, which will reduce the types of health IT software under the FDA’s regulatory authority.¹² Had such legislation been in effect over the past 5 years, those deregulated software devices likely would not have been reviewed by the FDA and no adverse events would have been reported to any federal agency. Given the FDA’s central role in implementing device recalls, at least one high-risk recall in Table 2 and all the recalls listed in Table 3 would not have been possible had such proposed legislation been in place, nor are similar recalls likely to be implemented in the future.³⁵

The new legislation is expected to reduce the accountability and transparency of software problems, since companies would have sole authority to decide whether or not to recall defective devices and whether or not to make software problems public. Medical errors have been recognized in both studies and lawsuits as an important cause of patient morbidity and mortality, with physicians and medical facilities held responsible.³⁶ Indeed, unintended medical errors resulting from medical professionals using defective software devices have already begun to raise similar issues and concerns.^{14,15}

Improving the safety of medical device and health IT software on a national level will require a much more comprehensive approach. Indeed, any health IT safety strategy focused solely on product recalls would be fundamentally reactive and would identify risks only when someone has been potentially harmed, thereby shifting the burden of proof from the vendor (to demonstrate that the software is safe) to the health care organization (to determine when it is not).³⁷ Furthermore, many critical software flaws in diverse health IT systems probably cannot be detected or will not lead to FDA recalls, making recalls a

necessary but not sufficient component of any national health IT safety strategy.³⁸ Without a robust, mandatory, and enforceable approach to risk assessment and adverse-event reporting for software, whether through the FDA or another government agency with sufficient authority and resources, it is likely that the risks to patients from health IT and other medical devices will increase.

Limitations

This study has several limitations. First, our analysis focused primarily on data collected from a single database of medical devices recalled for patient safety concerns, and not from problems reported through the FDA's adverse-reporting system or reports made to the companies involved. Although this FDA database is not expected to include all defective devices, it is currently the most comprehensive source of safety-related issues for medical software. Second, the data provided in the recall summaries do not indicate whether the initial recall decision was triggered by the company, the FDA's recommendations, or direct complaints from patients, providers, or hospitals. Moreover, even if the companies initiated some of the recalls, we cannot know whether those recalls would have taken place or been implemented in the same way if the FDA did not have the authority to gather and publicize adverse reports and to take defective software products off the market. Finally, most adverse event reporting is voluntary, and software errors are difficult to detect and sometimes even impossible to separate fully from human error. As a result, the actual number of risky devices is likely to be underrepresented and the full impact of software problems underestimated. Despite these limitations, the data from this study help highlight some of the most important regulatory and patient safety issues in medical devices caused by software.

Conclusions

Software problems in medical devices are not rare and can hinder medical care. Premarket regulation has not captured all the software issues that could harm patients, evidenced by the potentially large number of patients exposed to software products that are later subject to high-risk and moderate-risk recalls. As a result of the 21st Century Cures Act's

weakening of the FDA's premarket and postmarket oversight of health IT devices, the number of physicians and their patients at risk from medical errors caused by software-related problems in medical devices is likely to increase.

References

1. Kohane IS, Drazen JM, Campion EW. A glimpse of the next 100 years in medicine. *N Engl J Med*. 2012;367(26):2538-2539. <https://doi.org/10.1056/NEJMe1213371>.
2. Mega J, Sabatine M, Antman E. Population and personalized medicine in the modern era. *JAMA*. 2014;312(19):1969-1970.
3. Slight SP, Bates DW. A risk-based regulatory framework for health IT: recommendations of the FDASIA working group. *J Am Med Inf Assoc*. 2014;21(e2):e181-184. <https://doi.org/10.1136/amiajnl-2014-002638>.
4. Hernandez AF, Greiner MA, Fonarow GG, et al. Relationship between early physician follow-up and 30-day readmission among medicare beneficiaries hospitalized for heart failure. *JAMA*. 2010;303(17):1716-1722.
5. US Food and Drug Administration. Recalls, corrections and removals (devices). 2016. <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/RecallsCorrectionsAndRemovals>. Accessed January 16, 2016.
6. Zuckerman DM, Brown P, Nissen SE. Medical device recalls and the FDA approval process. *Arch Intern Med*. 2011;171(11):1006-1011. <https://doi.org/10.1001/archinternmed.2011.30>.
7. Zuckerman D, Brown P, Das A. Lack of publicly available scientific evidence on the safety and effectiveness of implanted medical devices. *JAMA Intern Med*. 2014;174(11):1781-1787. <https://doi.org/10.1001/jamainternmed.2014.4193>.
8. US Food and Drug Administration. *Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices—Guidance for Industry and Food and Drug Administration Staff*. Rockville, MD: US Food and Drug Administration; 2015.
9. US Food and Drug Administration. *General Wellness: Policy for Low Risk Devices—Draft Guidance for Industry Staff*. Rockville, MD: US Food and Drug Administration; 2015.
10. Blumenthal D, Tavenner M. The “meaningful use” regulation for electronic health records. *N Engl J Med*. 2010;363(6):501-504.

11. IOM (Institute of Medicine). *Health IT and Patient Safety: Building Safer Systems for Better Care*. Washington, DC: Institute of Medicine; 2012. doi:10.17226/13269.
12. US Congress. *Rules Committee Print 114–67 Text of House Amendment to the Senate Amendment to H.R. 34, Tsunami Warning, Education, and Research Act of 2015* [showing the text of the 21st Century Cures Act]. 2016. <http://docs.house.gov/billsthisweek/20161128/CPRT-114-HPRT-RU00-SAHR34.pdf>. Accessed January 4, 2017.
13. Myers RB, Jones SL, Sittig DF. Review of reported clinical information system adverse events in US Food and Drug Administration databases. *Appl Clin Inf*. 2011;2(1):63–74. <https://doi.org/10.4338/ACI-2010-11-RA-0064>.
14. ECRI Institute. *Executive Brief: Top 10 Health Technology Hazards for 2017*. Plymouth Meeting, PA: ECRI Institute; 2016.
15. Graber ML, Siegal D, Riah H, Johnston D, Kenyon K. Electronic health record–related events in medical malpractice claims. *J Patient Saf*. 2015;November 6:1–9.
16. US Food and Drug Administration. Medical device databases. Medical device recalls. Rockville, MD: US Food and Drug Administration; 2015. <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Databases/default.htm>. Accessed December 29, 2015.
17. Natus neurology. Natus Medical Incorporated website. 2015. <http://www.natus.com>. Accessed December 20, 2015.
18. US Food and Drug Administration. 510(k) premarket notification: Puritan Bennett 980 Series Ventilator System. 2016. http://www.accessdata.fda.gov/cdrh_docs/pdf13/K131252.pdf. Accessed January 7, 2016.
19. MEDTECH Act of 2015, S. 1101, 114th Cong. (2015). <https://www.congress.gov/bill/114th-congress/senate-bill/1101>. Accessed December 4, 2015.
20. 21st Century Cures Act of 2015, H.R. 6, 114th Cong. (2015). <https://www.congress.gov/114/bills/hr6/BILLS-114hr6rfs.pdf>. Accessed December 30, 2015.
21. US Food and Drug Administration. Cybersecurity vulnerabilities of Hospira Symbiq Infusion System: FDA safety communication. 2015. <http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm>. Accessed March 2, 2016.
22. Gottlieb S. Fostering medical innovation: a plan for digital health devices. *FDA Voice*. 2017. <https://blogs.fda.gov/fdavoices/index.php/2017/06/fostering-medical-innovation-a-plan-for-digital-health-devices/>. Accessed June 16, 2017.

23. US Food and Drug Administration. Baxter Corporation Englewood, ABACUS Total Parenteral Nutrition Calculation Software, versions 3.1, 3.0, 2.1, and 2.0: software errors may cause toxic or overdose symptoms. 2014. <https://wayback.archive-it.org/7993/20170112083845/http://www.fda.gov/MedicalDevices/Safety/ListofRecalls/ucm398428.htm>. Accessed March 2, 2016.
24. Ash JS, Berg M, Coiera E. Some unintended consequences of information technology in health care: the nature of patient care information system-related errors. *J Am Med Inf Assoc*. 2004;11(2):104-112. <https://doi.org/10.1197/jamia.M1471>.
25. Wears RL, Berg M. Computer technology and clinical work: still waiting for Godot. *JAMA*. 2005;293(10):1261-1263. <https://doi.org/10.1001/jama.293.10.1261>.
26. Wright A, Hickman T-TT, McEvoy D, et al. Analysis of clinical decision support system malfunctions: a case series and survey. *J Am Med Inf Assoc*. 2016;23(6):1068-1076. <https://doi.org/10.1093/jamia/ocw005>.
27. Terhune C. UCLA health system data breach affects 4.5 million patients. *Los Angeles Times*. July 17, 2015. <http://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html>. Accessed March 10, 2016.
28. US Food and Drug Administration. *Guidance for Industry Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software*. 2005. <https://www.fda.gov/MedicalDevices/ucm077812.htm>. Accessed January 2, 2016.
29. US Food and Drug Administration. FDA takes steps to improve reliability of automated external defibrillators (Press release). January 28, 2015. <http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm431907.htm>. Accessed January 1, 2016.
30. IOM (Institute of Medicine). *Medical Devices and the Public's Health: The FDA 510(k) Clearance Process at 35 Years*. Washington, DC: Institute of Medicine; 2011. <https://www.nap.edu/catalog/13150/medical-devices-and-the-publics-health-the-fda-510k-clearance>. Accessed December 7, 2015.
31. Parnas DL, van Schouwen AJ, Kwan SP. Evaluation of Safety-Critical Software. *Commun ACM*. 1990;33(6):636-648.
32. Medikonda BS, Panchumart SR. An approach to modeling software safety in safety-critical systems. *J Comput Sci*. 2009;5(4):311-322. <https://doi.org/10.3844/jcs.2009.311.322>.
33. Wears RL, Leveson NG, eds. *"Safeware": Safety-Critical Computing and Health Care Information Technology*. Rockville, MD: Agency for Healthcare Research and Quality (US); 2008. <https://www.ncbi.nlm.nih.gov/books/NBK43774/>. Accessed March 11, 2017.

34. Johnson C. *Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting*. Glasgow, Scotland: University of Glasgow Press; 2003. http://www.dcs.gla.ac.uk/~johnson/book/C_Johnson_Accident_Book.pdf. Accessed March 11, 2017.
35. Zuckerman DM, Jury NJ, Silcox CE. 21st Century Cures Act and similar policy efforts: at what cost? *BMJ*. 2015;6122:h6122. <https://doi.org/10.1136/bmj.h6122>.
36. Institute of Medicine. *To Err Is Human: Building a Safer Health System*. Kohn LT, Corrigan JM, Donaldson MS, eds. Washington, DC: National Academies Press; 2000.
37. National Research Council of the National Academies. *Software for Dependable Systems: Sufficient Evidence?* Jackson D, Thomas M, Millett LI, eds. Washington, DC: National Academies Press; 2007.
38. Institute for Safe Medication Practices (ISMP). Safety still compromised by computer weaknesses: comparing 1999 and 2005 pharmacy computer field test results. *ISMP Medicat Saf Alert*. 2005;10(17):1-3. <http://www.ismp.org/Newsletters/acutecare/articles/20050825.asp>. Accessed March 11, 2017.

Funding/Support: This project was funded by general support donations to the National Center for Health Research.

Conflict of Interest Disclosures: Both authors completed the ICMJE Form for Disclosure of Potential Conflicts of Interest. Diana Zuckerman reported owning stock in Johnson & Johnson; Jay Ronquillo had nothing to disclose.

Address correspondence to: Diana M. Zuckerman, National Center for Health Research, 1001 Connecticut Ave NW, Ste 1100, Washington, DC 20036 (email: dz@center4research.org).