Cars were dangerous in the 1960s, but thanks largely to Ralph Nader’s powerful book *Unsafe at Any Speed*, car safety has since improved dramatically. Nader’s 1966 bestseller motivated changes in automotive safety legislation and a cultural shift in the industry from “drivers have accidents so safety isn’t our problem” to “drivers have accidents so cars must be engineered to be safer.” For instance, seat belts alone reduce the risk of front-seat deaths by 45 percent, and automakers now invest in and promote many new technologies that make cars and driving safer.

A similar cultural transformation is required for health IT. We need at least passive safety technologies—the equivalent of seat belts and air bags—to detect errors and limit their harm. Furthermore, we must promote designed-in safety, now integral to the automotive and aviation industries. We also need a lever to help effect this cultural shift—evidence-based labeling—to develop and evaluate IT in healthcare safety as rigorously as in other safety-critical areas.

Cars were dangerous in the 1960s, but thanks largely to Ralph Nader’s powerful book *Unsafe at Any Speed*, car safety has since improved dramatically. Nader’s 1966 bestseller motivated changes in automotive safety legislation and a cultural shift in the industry from “drivers have accidents so safety isn’t our problem” to “drivers have accidents so cars must be engineered to be safer.” For instance, seat belts alone reduce the risk of front-seat deaths by 45 percent, and automakers now invest in and promote many new technologies that make cars and driving safer.

A similar cultural transformation is required for health IT. We need at least passive safety technologies—the equivalent of seat belts and air bags—to detect errors and limit their harm. Furthermore, we must promote designed-in safety, now integral to the automotive and aviation industries. We also need a lever to help effect this cultural shift—evidence-based labeling—to develop and evaluate IT in healthcare safety as rigorously as in other safety-critical areas.

While not a magical solution to healthcare problems, improving IT will improve quality and reduce preventable errors that cause patient harm.

**HEALTH IT AS MAGIC**

Healthcare is in trouble. Costs are rising, transparency is lacking, and care is often badly managed, resulting in unnecessary and harmful procedures. Many people enthusiastically promote health IT modernization as a means to magically eliminate these problems. Going paperless, using mobile medical devices and apps, leveraging big data and AI to gain new health insights—such changes, it’s argued, will improve both efficiency and patient satisfaction.3–5

Unfortunately, just investing in “better” IT to improve healthcare oversimplifies some critical issues.

First, most highly successful companies built on cutting-edge IT like big data, cloud computing, and machine learning have very different business models than healthcare organizations. Everyone with an Amazon account, for example, follows a similar and fairly simple process—search for an item, make a payment, and track the order—that’s ideally suited for automation. In contrast, healthcare is a complex, often messy process that requires all sorts of workarounds.6 Patients also are much more diverse than consumers: nobody’s medical history or treatment is the same. In these circumstances, IT might amplify, rather than simplify, a problem.

Second, the stakes are much higher in healthcare than in most other industries. If I make a mistake...
ordering something online or post a message I regret, it might cause some inconvenience but does no physical harm and is usually easily corrected. If a hospital makes a mistake, however, I could suffer irreparable harm or even die.

Third, when healthcare errors occur, we’re often too quick to blame caregivers and not the IT system upon which they rely. This unfortunate scapegoating is encouraged by typical health IT contracts that hold vendors harmless. Consequently, many IT-related problems aren’t addressed through, for example, needed software upgrades or policy changes, let alone avoiding them in the first place through proper design and careful procurement.

HEALTH IT AS A SOURCE OF ERROR

Human error is a major killer in healthcare. In hospitals, fatalities from preventable error are on a scale comparable to that of cancer and heart disease. Reducing error will improve healthcare outcomes better than any medical intervention, including breakthrough treatments for diabetes and other deadly diseases. Unfortunately, stakeholders underestimate the frequency of errors and often don’t recognize them until it’s too late. Indeed, if we ever noticed errors before it was too late, we’d do our best to fix them!

But many errors result from system design flaws. In particular, errors in calculations—which are ubiquitous in healthcare—are a common source of preventable error. This might be somewhat surprising given that one of IT’s main benefits is the ability to carry out a high volume of calculations quickly and more reliably than humans can, but when the stakes are as high as they are in healthcare, there’s no room for error. The system must be extremely dependable—a wrong result could be the difference between life and death.

Figure 1. Examples of flawed medical device designs. (a) CareFusion’s Alaris patient-controlled analgesia (PCA) modular syringe driver has a confusing display that makes it unclear how much drug the device is delivering. (b) Despite earning numerous awards and having CE marking, the Mersey Burns app recommends a dangerously high infusion rate of resuscitation fluids for burn victims; it miscalculates the burn time as well. (c) Many features of Abbott’s XceedPro handheld blood glucometer, including its “lockout technology,” do not work as advertised.

Consider, for example, the delete function, which is designed to correct an input error but is often implemented incorrectly. Suppose that, on a calculator, you try entering 0.5 but accidentally enter an extra decimal point. To correct the error while typing, you press the delete key after the
second decimal point. However, the calculator interprets what you typed, 0 \cdot \text{DEL} 5, as 5—you're "correction" has actually caused an error ten times higher than the intended number.

More generally, most medical devices fail to comply properly with the Institute for Safe Medication Practices' guidelines on number entry.10 Astonishingly, this problem is widely ignored despite the potentially serious consequences.11,12

Figure 1 shows some typical examples of other often-overlooked medical device design problems. These examples were chosen to be easy to visualize, but unfortunately many other problems are complex and hard to visualize.13

Figure 1a shows the display area of CareFusion’s Alaris patient-controlled analgesia (PCA) modular syringe driver. The device’s fixed label is contradicted by the programmed display: is it delivering the drug at a rate of 9 mL/h or 9 mg/h? This dangerous confusion is the result of inadequate testing combined with poor programming practices.

Figure 1b is a screenshot from the award-winning Mersey Burns app, which is designed to calculate the amount of resuscitation fluids to give a burn patient. In this case, the recommended infusion rate is an average 144 L/h, after giving 12 L in the first 5 minutes. However, the initial infusion is much more than an adult’s typical blood volume of 5 L.12 This faulty calculation is due to poor programming and reveals inadequate (or no) sanity checking on the part of the designers. Nevertheless, Mersey Burns is self-certified CE marked, which means it can be used in the EU. Unfortunately, self-certification won’t reveal developers’ own blind spots. Clearly, the numerous awards Mersey Burns received didn’t assess whether the app was well engineered.

Figure 1c is an Abbott XceedPro handheld blood glucometer, as used in hospitals. Abbott claims that it provides “lock-out technology” to help ensure compliance with mandated procedures for device use. However, as revealed in a much-publicized UK criminal trial of nurses accused of fabricating patient blood-glucose readings, this feature, among others, failed to work properly because the device was poorly programmed with no end-to-end checks. The court case highlighted IT management errors as well as problems with the device’s design, as Abbott itself deleted critical data uploaded to a centralized system.8

Another example of health IT as a source of error is “alarm fatigue,” which occurs when a system emits so many warnings or alarms that clinicians stop paying full attention to them. Not only can this lead to mistakes when critical alarms are ignored, it can also result in blame improperly being assigned to users rather than designers. Alarm fatigue can also waste staff resources: one UK study of 360,000 hours of infusion pump logs at a hospital found that 5 percent of infusion time was spent monitoring the system’s alarms—a cost of about £1,000 per year per pump.14 Alarm fatigue is often seen as a hospital, not a design, problem,15 yet the root cause lies in manufacturers’ lack of liability: it’s easier to design a device to beep than to think of a solution.

These and other basic problems are surprisingly widespread. Poor system design induces and exacerbates errors that can then be inadequately investigated, with doctors and nurses too often blamed for the consequences. When the causes of errors aren’t properly identified as design flaws, patients, staff, and overall healthcare quality suffer.

Anyone familiar with modern software engineering and formal methods in particular knows that many IT problems are avoidable16–18—in fact, we’ve known this for decades.19,20 The bottom line is that medical device manufacturers discount the importance of safe, dependable programming, and the best cure for this self-delusion is a liberal dose of formal methods.21

TRANSPARENCY BENEFITS
Health IT links together all stakeholders in the healthcare system including patients, caregivers, hospitals and clinics, insurers, device and drug manufacturers, and medical researchers. Improving IT is therefore the most efficient way to improve healthcare systems and processes and to reduce errors that cause harm. However, this requires transparency: we must be able to recognize an improvement before we can implement it. Without knowing all the facts, we might be easily seduced by IT solutions that promise magical results but that aren’t truly effective.4

Healthcare critics like Eric Topol point out that lack of financial transparency leads to inefficiencies and high costs.3 But also missing is transparency with regard to health IT quality and safety. Without safety transparency, there’s little incentive for manufacturers to improve their devices or for hospitals and clinics to switch vendors. In fact, there are numerous contractual impediments to sharing information about device quality and safety.6

Nevertheless, many IT quality measures exist, and others can be specified for healthcare safety. For example, in my own research I’ve evaluated the safety of number-entry user interfaces—such as those that use a knob or pair of chevron keys to advance numbers as well as traditional numeric keypads—so that hospital and clinics could preferentially buy the safer products.22,23

EVIDENCE-BASED LABELING
Figure 2 shows a selection of consumer rating schemes from different industries about product quality and safety. None of these schemes impose any particular regulations or mandate how manufacturers should make their products. In the relatively transparent consumer market, the idea is to provide basic information about goods to consumers so that they can make more informed choices. This in
turn creates market pressure to make better products and can even result in new ratings to reflect market improvement. For example, EU energy efficiency ratings for most appliances, light bulbs, and even cars originally spanned from A (most efficient) to G (least efficient), but as Figure 2c indicates, improved energy efficiency has led to new official A+, A++, and A+++ ratings for many products.

Likewise, every health IT product should have a simple, visible quality/safety rating. Such ratings would empower patients to be more proactive in their own care: “I don’t want to be hooked up to an infusion pump with such a low rating!” Clear labels would also motivate hospitals and clinics to purchase higher-quality goods to earn patient confidence and to attract new customers: “We use only AAA+++ certified medical devices.” When errors do occur, visible device ratings would help ensure that potential system failure is properly considered. Over time, then, incidence reporting will increasingly highlight the role of system design in errors and the fact that caregivers aren’t necessarily at fault.

Of course, health IT labeling assumes we know how to rate such products. It’s
widely recognized in healthcare that all clinical interventions should be based on evidence, as they might have many different side effects for different patients. Health IT is no exception: ratings of medical device safety and quality must also be evidence-based, reflecting documented estimates of the risk of using such devices and the severity of potential side effects.

Although IT is often naively proposed as “the” solution to healthcare’s problems, the reality is that improving health IT quality and safety is a long-term cultural and regulatory challenge that requires overcoming centuries of medical tradition and a lack of technological maturity. Today’s medical device market isn’t transparent, and hospitals and clinics can’t choose safer systems even if they want to. At the same time, health IT vendors clearly aren’t using modern software engineering techniques, let alone formal methods. These techniques are routine, indeed required, in the aviation industry and have produced very reliable software. Applying formal methods to health IT would likewise produce dramatic improvements in medical device and system software.

As a first step, unbiased system designers, medical and behavioral researchers, and computer scientists must work together to integrate modern software engineering techniques and computational thinking with health IT practice. Ironically, despite calls for big data in healthcare, that’s exactly what’s lacking. We need better data on how health IT systems work, the protocols clinicians follow, and their impact on patient care. How many and which preventable errors are induced by poor IT? Why aren’t accurate error logs routinely collected? What design innovations would minimize errors?

Just like prescription drugs, medical devices should be properly evaluated before they can enter the market. Once we have sufficient information to rate health IT systems for quality and safety, regulations are needed to mandate that all devices have easy-to-understand rating labels so that healthcare stakeholders can make more informed decisions.

Healthcare’s problems aren’t unsolvable; all that’s needed is the right approach and a commitment to fix health IT and improve patient safety.

REFERENCES
Looking for the BEST Tech Job for You?

Come to the Computer Society Jobs Board to meet the best employers in the industry—Apple, Google, Intel, NSA, Cisco, US Army Research, Oracle, Juniper...

Take advantage of the special resources for job seekers—job alerts, career advice, webinars, templates, and resumes viewed by top employers.

www.computer.org/jobs

---

This article originally appeared in Computer, vol. 50, no. 6, 2017.


HAROLD THIMBLEBY is a professor of computer science at Swansea University. Contact him at harold@thimbleby.net or visit www.harold.thimbleby.net.