

# Health Information Technology: A Few Years Of Magical Thinking?

Technology and standards alone will not lead to health IT adoption, let alone transform health care.

by **Carol C. Diamond and Clay Shirky**

**ABSTRACT:** One of the biggest obstacles to expanding the use of information technology (IT) in health care may be the current narrow focus on how to stimulate its adoption. The challenge of thinking of IT as a tool to improve quality requires serious attention to transforming the U.S. health care system as a whole, rather than simply computerizing the current setup. Proponents of health IT must resist “magical thinking,” such as the notion that technology will transform our broken system, absent integrated work on policy or incentives. The alternative route to transforming the system sets all of its sights on the destination. [*Health Affairs* 27, no. 5 (2008): w383–w390 (published online 19 August 2008; 10.1377/hlthaff.27.5.w383)]

ONE OF THE BIGGEST OBSTACLES TO EXPANDING the use of information technology (IT) in health care may be, ironically, the current narrow focus on how to stimulate its adoption. IT is a tool, not a goal. Success should not be measured by the number of hospitals with computerized order entry systems or patients with electronic personal health records. Success is when clinical outcomes improve. Success is when everyone can learn which methods and treatments work, and which don't, in days instead of decades.

The challenge of thinking of health IT as a tool to improve quality requires serious attention to transforming the U.S. health care system as a whole, rather than simply computerizing the current setup. Indeed, the literature on computerization, stretching back to the 1980s, is unambiguously clear on this point: computers are amplifiers. If you computerize an inefficient system, you will simply make it inefficient, faster. IT can contribute to improving care only when underlying system processes are transformed at the same time.

Proponents of health IT must resist “magical thinking,” such as the notion that

---

*Carol Diamond (cdiamond@markle.org) is managing director of the Health Program at the Markle Foundation in New York City. Clay Shirky is an adjunct professor in the Graduate Interactive Telecommunications Program, New York University, also in New York City.*

isolated work on technology will transform our broken system. Another tempting and related notion suggests that a lack of technical standards is the main barrier to health IT adoption. This may explain the stimulus for some national efforts that focus primarily on technical designs and standards for a set of narrow use cases and “early wins.”<sup>1</sup> Without adequate investment in the much harder challenges—such as how to motivate IT adoption toward achieving better health and health care, which financial policies will support this goal, or what information policies are necessary to protect information and engender patient trust—we will surely miss the mark.<sup>2</sup>

Connecting for Health, a public-private collaborative operated by the Markle Foundation with participation from more than 100 health care and IT organizations, has been surveying and trying to improve the state of health IT since 2002.<sup>3</sup> It has long been clear to us that technology and standards alone will not lead to health IT adoption, let alone transform health care. There are serious structural barriers to the use of IT that have nothing to do with technology. Current legal and financial incentives provide little motivation to share information across institutions, which is critical to improving patient outcomes as well as efficiency. There is also deep concern on the part of doctors and hospitals about how the technology will be financed, and on the part of consumers about how their data will be used and kept safe from misuse. These are thorny issues, requiring answers that delve deeply into information policy.

Much of the conversation in recent years has focused on a single issue—standards—as the principal driver of health IT adoption. One of the immediate results of this approach has been widespread impatience. If it’s just a question of standards, what is taking so long?

The Office of the National Coordinator for Health Information Technology established the Health Information Technology Standards Panel (HITSP) to harmonize and designate health information standards and the Certification Commission for Health Information Technology (CCHIT) to certify vendor products three years ago. These efforts deserve praise for increasing public and industry interest in health IT and for encouraging adoption of technical standards. Yet after three years of standards documentation and the resolution of several standards “disputes,” we remain a long way from seeing these standards used and implemented to enable health information sharing.<sup>4</sup> As Sam Karp of the California HealthCare Foundation stated in his testimony to the Institute of Medicine Board on Health Care Services and National Research Council Computer Science and Telecommunications Board, “Not a single data element has been exchanged in real world health care systems using standards this process has developed or deployed.” He went on to state that “greater emphasis is placed on ‘ideal’ standards and less on what can be feasibly implemented in the short-term—hence three years of work, millions of dollars spent and little real progress toward interoperability.”<sup>5</sup>

## Misplaced Focus On Standards

The risk now is that growing impatience will put even more pressure on the standards process, further delaying the policies needed to guide a transformation in the way health care information is handled, shared, and acted upon. It is clearly important to have broadly adopted standards, but a primary focus on standards is misplaced for three reasons: First, protocols are created, but standards are adopted. Second, information won't be shared until there is a compelling reason to share it and until the parties who need to share it trust each other. Third, and most critically, in networked systems, it is impossible to separate the creation of technology standards from the development of information policy.

■ **Protocols are created, but standards are adopted.** It seems obvious that a lack of standards for sharing data is a big obstacle and that creating a set of standards will remove that obstacle quickly and permanently. Unfortunately, it never really happens that way.

The process of standardization is incremental, never solving every problem at once and often leaving prospective data-sharing protocols to be worked out in the field, and only then submitted for ratification after the fact. For example, the basic standards for the Internet, constituting the world's most intensively used data standards, were created and revised over decades, often enabling primitive tools first and then learning from what the users did with them.<sup>6</sup> This approach requires a willingness to accept a high degree of underlying variability at first, as well as the discipline to address only critical requirements for any given increment of improvement.<sup>7</sup>

By contrast, the history of failed standards efforts is filled with vendor-approved standards that never passed the crucial test, which is clear utility for the user. It seems tautological, but standards aren't really standard unless they are widely adopted, and this step can't be easily mandated. To return to the example of the Internet, an enormous variety of very well-designed data-networking standards, whether designed by individual vendors or international consortia, were largely unable to compete on a global scale with the Internet's simple but evolving standards. Openness, the discipline to solve only core problems, and incrementalism trumped standards that were well engineered on paper but hadn't been subjected to the baptism by fire that is user adoption.

Gordon Bell led the National Science Foundation's Computing Directorate team that made the Internet. In "A Time and Place for Standards," Bell's review of IT standardization efforts, he explains why design-by-committee standards are generally a bad idea. He notes that vendors can "throw their support behind faux standards, containing cloaked, yet potent, proprietary advantages designed to serve their own interests. ...Owing either to arrogance or innocence (or possibly both) the vendors that played the faux standards game all made the fatal assumption that most of the buyers could be fooled most of the time. Of course these ven-

dors succeeded only in deluding themselves. That's because it's been shown time and again that genuine standards created to serve the true interests of consumers will also generally end up serving the best interest of vendors."<sup>8</sup>

You can't "make" a standard any more than you can "make" friends; people become friends over long association, and so it is with standards. The way something becomes a standard is for it to become standard—which is to say, for it to become the normal case in the field, not merely in the lab or a conference demonstration.

The risk here isn't just overemphasis on standards—that would be a simple misallocation of effort. The risk is that by not accompanying standards with work on information policies and incentives, the current efforts may, paradoxically, slow the very transformation that health IT can deliver. This risks creating a vicious circle, where impatience leads to still more pressure to push unadopted standards proposals, leading to still more impatience. As Bell put it, "To push those efforts prematurely is to hope vainly that standards and consortia can somehow drive the technology to maturity."<sup>9</sup>

■ **Motivation and trust.** The second reason we should reconsider the current focus on standards is that information won't be shared until there is a reason to share it. There are two separate problems: First, the current way we pay for health care undermines the case for investing in the sharing of data—even though people agree that such sharing is both in the patient's best interests and a critical tenet of high-quality care. Indeed, one of the obvious lessons from the field is that people adopt standards after they have a reason to share, and that standards in the absence of such reasons (or the trust necessary to sustain such sharing) is like pushing string. Recent news on failed efforts to achieve communitywide interoperability in many U.S. communities continue to document both the need for privacy policies and the lack of compelling financial drivers as the reason for demise. In one article chronicling the demise of the Oregon Regional Health Information Organization (RHIO), a hospital chief information officer (CIO), Dick Gibson, noted that the project estimated a \$10 million drop in combined revenues for hospitals through the elimination of duplicative testing, yet hospitals were being asked to pay for the project.<sup>10</sup> This kind of disincentive cannot be overcome primarily by standards and technical work. Until we place financial value on the kind of high-quality patient care that can only be achieved with information sharing, there is little reason to believe that the adoption of standards will progress at anything other than the current slow pace.

The sharing-then-standards case describes every successful data-sharing effort we have surveyed in our Connecting for Health work. Standards play a critical role in all of those cases but were adopted in response to the business case, rather than as a replacement for it. The pattern of a high degree of technical design but a low degree of trust or incentive to share describes a number of prominent failures, such as the Santa Barbara RHIO.<sup>11</sup> In general, standards and technologies were available, but the efforts collapsed because the participants saw no financially rational reason to share their data, and many reasons not to.

The second, narrower point is that at this early stage of evolution in health IT, standards for moving data across the network are more important than standards expressing the content of that data. Put another way, it is better to share important but uncodified information between Doctor A and Doctor B so that an informed clinical decision can be made, than to have perfectly formatted data that never leaves Doctor A's office.

Many health care records are simply free-form notes. Simple access to essential parts of those records would be a huge improvement over today's system, in which sharing is far from routine. Meanwhile, most of the standards efforts today are focused on domain-specific content standards—what metadata should accompany x-rays, and what should accompany electrocardiograms (EKGs)? These standards will be more broadly adopted someday, but that day is when routine sharing has already been worked out and when sites of care have sophisticated computerized decision-support mechanisms that require such interoperability.

Neither of these conditions is the norm today, and they will not be made real by having standards for content (what we name things in a medical record) but not for transport (how we share it over the network). Standards generally do not drive upgrades; rather, upgrades generally drive standards. We shouldn't be delaying the sharing of some unformatted data that would nevertheless be useful to an actual human caregiver, simply in order to make the data comprehensible to a computerized decision-support system that will likely be a long way in coming to most practices. Any work done on the motivations and methods of simple sharing—"Get this patient's information, as it exists today, from here to there"—will pay off in an increased desire for the creation and adoption of content standards. The corollary is not true.

■ **Technology is policy.** Finally, it is impossible to separate technology and policy in networked systems. Inevitably, a standard places a "stake in the ground" on key policy issues, even if these issues were not given explicit focus in the standards development process. For example, choices among technical standards and architectures will also determine how personal health information is discovered on a network, how it will be accessed, and where data will be stored or aggregated. Thus, decisions about standards and architectures affect the nature and degree of risk to which data will be exposed. Some proposals for searching a network for patient data commingle demographic and clinical information in directories that locate information. Such a standard, if adopted, would dramatically increase the exposure of some level of clinical information in these searches and, therefore, the risk of accidental disclosure. Post hoc overlay of policy can modify these kinds of risks but is unlikely to remove them.

Standards in health IT have been likened to construction specifications for building the interstate highway system. Yet it turns out that an explicit policy framework is as important as any effort to create technical standards. In health IT, technology standards by themselves are like an interstate highway system with no

rules of the road. To serve the communities through which it passes, a highway must have a coherent set of rules, made obvious through signage and visibly enforced. Computer systems that use the same technical standards will not move information by themselves for the care of a patient. Pushing the “send” button requires that the people who need to share information trust each other, understand and implement the necessary protections for the information they hold, and know that the information policies in place across a network will be upheld and enforced in the event of a breach.<sup>12</sup>

Another way in which technology and policy are intertwined is through the architecture of the data-sharing system. If you design a technical system that requires regional aggregation of patient data, the system will require ongoing resources for security and response to break-ins. If you design a more distributed system, which allows information to be shared from local sources over a network but does not require it all to be aggregated in one place, your risk for catastrophic breaches will be reduced, because the breach of any one site will not compromise the whole data set.<sup>13</sup> The recent catastrophic loss of twenty-five million child health benefit records in the United Kingdom demonstrates this principle in a chillingly real-world fashion: an employee at HM Revenue and Customs filled a request for a subset of data by simply resending the entire, enormous data set.<sup>14</sup>

This isn't simply a question of what policies “go with” what technologies—the technological choices themselves heighten or reduce certain kinds of costs and risks, and the policy choices require or forbid certain kinds of implementation. For example, if you design a policy system that assumes that the protections follow the data, you will require of your technology all of the same costs and inefficiencies that the music industry has suffered while chasing the same dream. Although many millions of dollars and person-years of effort have gone into securing music and movies with digital rights management (DRM), such schemes are usually cracked within days. The principal side effect of DRM, in fact, has been not to protect the data but to restrict user hardware choices, as with the MP3 player market by the linking of the iPod to iTunes online. DRM-style controls on health data would almost certainly be similarly ineffective as protection, while having the side effect of limiting users' choices of hardware and software. Such limitations would run counter to the policy goal of stimulating much-needed health IT innovation. As a result, it is impossible to design technology without reference to policy, because in the absence of clear direction, the choices of technology standards make policy de facto. The work taking place today in health care IT standards development is dangerously close to that point.

## **Key Lessons**

Because we have worked on both health IT policy and technology in Connecting for Health since 2002, one of the key lessons we have learned is that the highest value for the lowest cost in system design comes not just from co-evolving tech-

nology and policy, but from making each half do what it is best at.<sup>15</sup> For example, questions of trust are properly policy questions; technology generally cannot tell a hospital administrator whether he trusts an organization that wants the hospital's data. On the other hand, questions of verification—"Does this request actually come from an organization we have decided to trust?"—are technological.

As Dave Clark, another designer of several key networking standards, has put it, "One of the roles of architecture is to tell you what you can't do."<sup>16</sup> Because there is no clear set of information policies—there is, in fact, an ongoing absence of a set of specific, nationwide information policy goals relative to health IT—any resulting architecture may be unduly risky to patient data.<sup>17</sup> This has critical implications for patients' trust in the network. Here, among all of the problems with a standards-driven push for health IT, the failure is most glaring. Health information policies will inevitably be created; the current situation will make it harder to harmonize technology and standards with those eventual policies, at best. At worst, the technology could be incompatible with those policies. Since the current standards work is being driven by the body that could spearhead the development of a nationwide policy framework, fixing this mismatch is within our reach. Indeed, the hard work being done on standards today, in both HITSP and CCHIT, is occurring in a cloudy landscape for information policies; it would be much more powerful if guided by a clear policy framework.

## An Alternative Route

The alternative route to transforming the health care system sets all its sights on the crucial destination. This is not, "And then ten thousand hospitals bought new databases," but rather, "And then one million patients had better outcomes." This alternative approach would focus on a minimal set of standards at first and would make utility for the user to improve health outcomes, rather than agreement of the vendor on the key criteria. It would mean working simultaneously on removing other obstacles while concentrating on those standards necessary for actually sharing the information, however formatted in the short term, to flow between willing and authorized participants. Finally, it would require clear policy statements that will guide the design of technology. All of these issues are inextricably connected, and they should be pursued together.

Such a route faces sizable political and commercial obstacles. But those obstacles exist in the current system as well, and it is impossible to imagine that we can get improvements in quality, safety, and cost-effectiveness without facing them. It's equally implausible to think that a delay in policy work will make eventual policy solutions easier to integrate with today's technical choices. The appeal of magical thinking, as always, is not having to face hard problems. The appeal of this alternative route, hard as it might be, is that it could actually work.

.....  
*The authors thank Jill Cooper for her contributions to this paper.*

## NOTES

1. U.S. Department of Health and Human Services, "Health Information Technology: Federal Activities," <http://www.hhs.gov/healthit/privacy/federal.html> (accessed 15 February 2008).
2. GAO, *Report to Congressional Requesters. Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy*, January 2007, <http://www.gao.gov/new.items/d07238.pdf> (accessed 15 February 2008); J.C. Ebeler, M. Bruno, and T. Schmitt, eds., *Opportunities for Coordination and Clarity to Advance the National Health Information Agenda—A Letter Report* (Washington: National Academies Press, 2007); and J.M. Overhage, "Health Information Exchange: 'Lex Parsimoniae,'" *Health Affairs* 26, no. 5 (2007): w595–w597 (published online 1 August 2007; 10.1377/hlthaff.26.5.w595).
3. See the Connecting for Health home page at <http://www.connectingforhealth.org>.
4. F. Bazzoli, "Continuity of Care Document Is Approved by HL7, Endorsed by HITSP," *Healthcare IT News*, 14 February 2007, <http://www.healthcareitnews.com/story.cms?id=6408> (accessed 15 February 2008).
5. Sam Karp, California HealthCare Foundation, "Review of the Adoption and Implementation of Health IT Standards by the Office of National Coordinator for Health Information Technology," Testimony before the Institute of Medicine Board on Health Care Services and the National Research Council Computer Science and Telecommunications Board, 17 September 2007, <http://www.chcf.org/documents/healthit/KarpITAdoptionIOM.pdf> (accessed 23 July 2008).
6. J. Abbate, *Inventing the Internet* (Cambridge, Mass.: MIT Press, 1999); K. Hafner and M. Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (New York: Simon and Schuster, 1996); P. Baran and S.P. Boehm, *On Distributed Communications, II: Digital Simulation of Hot Potato Routing in a Broadband Distributed Communications Network*, Memorandum RM-3103-PR, August 1964, <http://www.rand.org/publications/RM/RM3103> (accessed 21 January 2008); and J. Reynolds and J. Postel, "IETF Network Working Group, Request for Comments: 1000," August 1987, <http://www.ietf.org/rfc/rfc1000.txt> (accessed 23 July 2008).
7. Overhage, "Health Information Exchange."
8. G. Bell, "A Time and Place for Standards," *ACM Queue* 2, no. 6, September 2004, <http://www.acmqueue.com/modules.php?name=Content&pa=showpage&pid=210> (accessed 1 August 2008).
9. *Ibid.*
10. P. Korn, "Record-Sharing Stalls; Cash, Privacy Issues Halt Effort to Electronically Link Patient Information," *Portland Tribune*, 10 August 2007.
11. R.H. Miller and B.S. Miller, "The Santa Barbara County Care Data Exchange: What Happened?" *Health Affairs* 26, no. 5 (2007): w568–w580 (published online 1 August 2007; 10.1377/hlthaff.26.5.w568); and J. Adler-Milstein et al., "The State of Regional Health Information Organizations: Current Activities and Financing," *Health Affairs* 27, no. 1 (2007): w60–w69 (published online 11 December 2007; 10.1377/hlthaff.27.1.w60).
12. Carol Diamond, "Private Health Records: Privacy Implications of the Federal Government's Health Information Technology Initiative," Prepared statement submitted to the Subcommittee on Oversight of Government Management, the Federal Workforce, and District of Columbia, Senate Committee on Homeland Security and Government Affairs, 1 February 2007, [http://www.connectingforhealth.org/resources/caroldiamond\\_february12007final.pdf](http://www.connectingforhealth.org/resources/caroldiamond_february12007final.pdf) (accessed 12 August 2008).
13. Markle Foundation, "The Connecting for Health Common Framework: Overview and Principles," <http://www.connectingforhealth.org/commonframework> (accessed 15 February 2008).
14. T. Espiner, "Government Loses 25m Confidential Records," *ZDNet UK*, 20 November 2007, <http://news.zdnet.co.uk/security/0,1000000189,39290951,00.htm> (accessed 15 February 2008).
15. Markle Foundation, "The Connecting for Health Common Framework."
16. Internet Society Network Working Group, "On the Design of Application Protocols," Memorandum, November 2001, <http://www.rfc-editor.org/rfc/rfc3117.txt> (accessed 15 February 2008).
17. GAO, *Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy*, January 2007, <http://www.gao.gov/new.items/d07238.pdf> (accessed 15 February 2008).