THE e-HEALTH INITIATIVE “BLUEPRINT”: WILL POTENTIAL PROFITS TRUMP PATIENT PRIVACY?

By Bruce Patsner, M.D., J.D.

The eHealth Initiative (eHI)1 was created in 2001 to “serve as a forum where diverse stakeholders in healthcare could find common ground on ways to drive improvements in the quality, safety, and efficiency of healthcare through information and information technology (IT).”2 eHI is a non-profit industry coalition comprised of a diverse group of over 200 organizations - members of the health insurance industry, pharmaceutical industry, pharmacies, hospitals, health care IT organizations, consumer organizations, health policy gurus, health care academics, telemedicine business entrepreneurs, state and federal officials, and other “stakeholders” – all of whom are committed to generating a framework for incorporating information technology into the fabric of healthcare delivery by providers, providing expanded healthcare information and portability to patients, and allowing healthcare data access to insurers and government underwriters.3 IT will be laying the tracks on which the train carrying personalized medicine, telemedicine, and health law policy together will be traveling, and eHI and other organizations like it are working to ensure that interoperability issues among competing IT systems are minimized so that the gauge of the track will be the same for all users. Advances in proteonomics, metabolomics, genomics, and internet technology will help push the train along.

A stated goal4 of eHI is to improve health care efficiency, quality, and patient safety through use of IT; in effect, switching the U.S. healthcare system over to a fully integrated, electronic information-based platform. eHI publications will ultimately help provide a roadmap for policy makers seeking to integrate telemedicine technology, information technology, and “personalized medicine.”5 Although eHI states in its publication that IT has a “demonstrated role in improving health and healthcare”6 no data is provided to support this contention. Available data on the issue of whether use of electronic medical records actually improves the quality of care from sources7 outside of eHI suggest that the benefits of electronic health records may be elusive depending on the parameter (e.g. inappropriate prescribing of medications) being examined.

eHI sponsored a meeting this October in Washington, D.C. to review the past six months of collaboration among its members. The outcome of this meeting was “The eHealth

1 eHEALTH INITIATIVE BLUEPRINT, BUILDING CONSENSUS FOR COMMON ACTION, PHASE I, October 10, 2007, available at www.ehealthinitiative.org (last accessed on October 20, 2007).
2 Id. at 4.
3 Id. at 2.
4 Id. at 4.
5 Wylie Burke and Bruce M. Psaty, Personalized Medicine in the Era of Genomics, 298 JAMA 1682 (2007).
7 Jeffrey A. Linder, Electronic Health Record Use and the Quality of Ambulatory Care in the United States, 13 ARCH. INT. MED. 1400 (2007).
Initiative Blueprint: Building Consensus for Common Action, a Phase I document which laid out five general categories of focus for health care organizations and providers looking to advanced the interface of information technology, medical care, health care coverage, and patient access to information. The five focus areas were: (1) engaging consumers; (2) transforming care delivery; (3) improving population health; (4) aligning financial and other incentives; and (5) managing privacy, security, and confidentiality.

The authors of the eHI Blueprint acknowledged the lack of consensus on details and very preliminary nature of their proposals while at the same time calling for immediate action and adoption of IT technology to healthcare. The goal for the year 2008 will be to obtain “stakeholder” input, as member organizations attempt to operationalize the recommendations of the Blueprint, in order to generate the Phase 2 report of “best practices” for IT technology implementation. The generation of this Phase 2 data will be an ongoing process that can be monitored via the internet. At its core level, the purpose of eHI’s industry coalition is to influence members of Congress and presidential candidates in an election year where health policy decisions are of paramount importance to voters. Some candidates have already commented specifically on the role IT will play in cutting healthcare costs and improving the quality of care. Not surprisingly, eHI is not the only player in the electronic health information technology arena which has put forth proposals to federal agencies.

eHI’s Blueprint offers both guiding principles and practical strategies for addressing the broad issues in the 5 key areas noted. Of the five areas, the areas of least agreement concerned paying for the crossover to this electronic medical world and preventing patient information from being shared inappropriately. Close reading of the Blueprint on the issue of “Managing Privacy, Security, and Confidentiality” of electronic medical records and information illustrates both the potential and the dangers of eHI’s Blueprint. Consensus was reached only on “broad principles” such as transparency (“Individuals have the right to know how their personal health information has been used and who has access to it,”); collection of information (“Consumers have a right to privacy of their personal health information, taking into account existing exceptions under the law,”); individual control (“Individuals should be able to limit when and with whom their identifiable personal health information is shared,”); security (“Measures should be implemented to protect the integrity, security, and confidentiality of each individual’s personal health information, ensuring that it cannot be lost, stolen, or

---

8 eHEALTH INITIATIVE BLUEPRINT, supra note 6.
9 Id. at 6.
13 eHEALTH INITIATIVE BLUEPRINT, supra note 6, p. 6.
14 Id. at 75.
15 Id.
16 Id.
17 Id.
18 Id.
accessed or modified in an inappropriate way,”19); accountability and oversight (“Individuals should be apprised as to who monitors policy compliance with privacy, security and confidentiality policies, how complaints will be handled, how individuals will be informed of a violation and existing remedies available to them,”20); and technology and privacy (“Privacy protections must be addressed at the forefront of all technological standards. Privacy issues cannot be addressed post-system design and implementation.”21). It is noteworthy that managing privacy and security of patient health information is the last item on the list even if eHI states that these issues should be resolved first.22

All of this is well and good, but the rub comes when we delve a little deeper into the section on “Common Core Questions About Privacy and Security.”23 eHI’s Blueprint’s authors simply note that there are not only conflicting state and federal laws regarding medical records, but that the laws may differ, or be absent entirely, for electronic records as well as written ones.24 Further, “not all entities are covered by the same laws, even in the situation where they perform the same services.”25 Conspicuously absent is any mention of the issues of whether the electronic medical file should contain all of the individual’s medical data; if there should be more than one electronic medical file (e.g. a separate one for psychiatric records); if there should be a firewall so that some health care providers or carriers can be prevented from accessing private medical information they do not need; or anything remotely resembling a concrete proposal for ensuring that privileged medical information won’t be accessed by potential employers, banks, mortgage companies, or the U.S. government if one becomes a homeland security concern.

The lack of consensus within the health IT industry as a whole on how to implement a national electronic medical record system using health information technology (HIT) is problematic. As Scott Wallace, President and CEO, the National Alliance for Health IT, has noted “The bigger struggle is to get policy makers to understand the complexity of the current system’s structure. There seems to be this notion that we’re going to talk about the benefits of HIT and somehow mandate the use of HIT, and then someone is going to sprinkle pixie dust all over the country, and voila’ we’re going to have all the benefits of HIT.”26

More bothersome is the paucity of concrete proposals devoted to developing firewalls to protect confidentiality of patient information before any of this technology is widely deployed. It seems clear from the wide-range of membership in the e-health movement that efforts to fully integrate the electronic age and healthcare in the United States will

---

19 Id.
20 Id. at 76.
21 Id.
22 EHEALTH INITIATIVE BLUEPRINT, supra note 6, p76.
23 Id.
24 Id.
25 Id.
26 Scott Wallace, 5 Questions with Scott Wallace, President and CEO, the National Alliance for Health IT, 8 ONCOLOGY NET GUIDE 20 (2007), available at www.onceng.com (last accessed October 20, 2007).
continue to grow and is going to be a major force in the business of healthcare. A quick perusal of the Federal Telemedicine News website quickly confirms this: much of the website information is directed towards the numerous legislative proposals before Congress on the healthcare-IT interface. For example one publication available through the Federal Telemedicine website is titled “How to Sell Healthcare Technologies to HHS.”

Business may be driving the train for the switchover to the electronic healthcare era, but the Bush administration is clearly on board the HIT train. In April 2004 President Bush issued a call for the widespread implementation of interoperable but secure electronic medical records for most Americans within a decade. This call followed the passage of The Medicare Prescription Drug, Improvement, and Modernization Act (MMA) which, as part of the new prescription drug benefit for Medicare recipients, directed the Department of Health and Human Services (DHHS) Secretary to establish a set of standards for electronic prescriptions. The goal of this directive was the same as that of the current eHI Blueprint “to improve patient safety, quality of care, and efficiency in the delivery of care.” And, in a move surely designed to move the development of a nationwide health information network along, HHS recently awarded the Regenstrief Institute at the Indiana University School of Medicine a $2.5 million grant to begin trial implementation of what will be called the National Health Information Network (NHIN).

Healthcare consumers are likely to be more interested in the privacy of their medical information than anything else to ensure that insurance coverage or employment decisions are not based on medical information that it not supposed to be used in the coverage or hiring calculus. Legitimate concerns over use of and access to private patient information – on HIV or infectious disease status, genetic risk for malignancy (e.g. BRCA analysis for breast or ovarian cancer), psychiatric history, prescription medication use, etc. have been around for more than a decade. Many of these concerns preceded the rise of internet technology, the Human Genome Project, and telemedicine.

28 Id.
30 Office of the President, A New Generation of American Innovation; President Bush’s Technology Agenda (2004), available at http://www.whitehouse.gov/infocus/technology/. The call was actually for most Americans to have a personal health record within a decade though this term is not precisely defined.
32 eHEALTH INITIATIVE BLUEPRINT, supra note 6.
These privacy issues have yet to be resolved. Whether these legitimate, theoretical concerns over patient privacy and security of medical information will prove to be real-world issues will only be known with time; the absence of significant case law in this area may simply reflect the fact that many existing HIT systems are “internal” (i.e. within only one hospital system), that disputes may have to go through a lengthy internal arbitration process before they reach the courts, or that the IT-healthcare interface is in its relative infancy. Given the dynamics of an expanding IT industry determined to quickly advance its business agenda and the clear support of politicians on both sides of the aisle for IT initiatives, patients and health law attorneys alike should be concerned about what’s coming down the track. With few of the critical confidentiality and privacy issues resolved, no uniform set of federal laws and regulations in place to supplement holes in HIPAA or remedies to address patient e-health-related injuries at a time when the development of the NHIN pilot programs are being funded, alarms should be going off. The protection of personal financial information by the securities industry might serve as a potential role model for NHIN design, but no one has proposed this as of yet.

Statements in the eHI Blueprint notwithstanding, it appears likely that critical items which could be ironed out prior to deployment of IT technology in healthcare are not so big a priority as financial incentives and rewards. It is possible that the increasing demand for use of electronic medical records (EMRs) as a de facto requirement for health care providers getting paid by both the private and government sides may effect the widespread use of this technology before all of the patient confidentiality and provider liability issues are resolved. There will likely be only one chance to get protection of patient information right before NHIN is a reality; unless government makes it a priority it seems unlikely eHI will either. The inevitable result will be ex-post resolution of system mistakes affecting large numbers of people in federal and state court.

36 eHEALTH INITIATIVE BLUEPRINT, supra note 6.