

Electronic Health Records: Emerging and Future Legal Issues

Bruce Wilder, MD MPH JD, Wilder & Mahood PC
Annual Meeting, Health Law Section, The Rivers Club, May 14, 2010
bwild@wildlaw.com

This presentation will serve as an orientation to the legal environment of electronic health records (EHR), and discuss current developments. Experience from the perspective of users is presented and discussed. Present and future legal issues are emphasized, including the effects of HIPAA and HITECH. A discussion of existing and proposed policy is included.

Overview

The acquisition, storage and retrieval of health care data in digital form have the potential to vastly improve the quality, efficiency, and safety of health care delivery, and in doing so, better the health of individuals. The electronic health record can and should also be a ready source of information that benefits public health and research, and thus indirectly further benefit the health of individuals.

In order to achieve this potential, however, the information obtained in the process of the delivery of health care must be managed properly. That means the protection of the privacy of individuals, and the confidentiality of physician-patient communications; a way to acquire and retrieve information that is not disruptive to provider workflow; the integration of information from numerous sources into a form that is useful; and the ability to transfer information among health care providers in electronic form.

“ . . . [D]espite the tremendous value of computer technology, the law as it is presently structured unduly inhibits the application of computer capabilities to medical record information systems in hospitals and other health care institutions.”¹

That statement still holds true today, albeit for perhaps different reasons.

Although the idea of keeping medical records in electronic form has been around almost as long as computer technology, it is only within the past few years that a useful EHR has become a reality. Despite an overwhelming perception that integration of digital technology into health care systems is not only desirable, but necessary, adoption has been slow, as well-documented in a recent report in the *New England Journal of Medicine*.² Other countries, particularly Denmark, have achieved much better results and with arguably much less in the way of resources.³ Why is this? The reasons for low adoption in the United States are numerous and complex.

Recognition of the need for EHR

In a 1991 report, updated in 1997, the Institute of Medicine concluded that computer-based patient records are an “essential technology” for health care delivery.⁴ A subsequent report in 1999, *To Err is*

1 Eric W. Springer, *AUTOMATED MEDICAL RECORDS AND THE LAW*, Aspen Systems Corporation, Rockville, MD, 1971.

2 Jha, AK, et al, *Use of Electronic Health Records in U.S. Hospitals*, *NEJM* 2009;360:1628-1638 (April 16, 2009) <http://content.nejm.org/cgi/content/full/NEJMs0900592> (last access 5/12/10).

3 The Commonwealth Fund, *Widespread Adoption of Information Technology in Primary Care Physician Offices in Denmark: A Case Study*, www.commonwealthfund.org/Content/Publications/Issue-Briefs/2010/Mar/Widespread-Adoption-of-Information-Technology-in-Primary-Care-Physician-Offices.aspx (last access 5/12/10).

4 Institute of Medicine, *The Computer-Based Patient Record: An Essential Technology for Health Care*, 1991, 1997.

Human,⁵ may be regarded as bringing about the birth of the patient safety movement, or at least the beginning of its gestation. Another report, in 2001, *Crossing the Quality Chasm: A New Health System for the 21st Century*,⁶ reiterated and emphasized the need for EHR technology.

Approaches to achieving universal adoption of EHR

In 2004, President Bush issued an Executive Order, establishing the goal of universal EHR adoption by 2014.⁷ Another Executive Order was aimed at furthering this goal by fostering interoperability and a certification program.⁸

Also in 2004, exceptions to Anti-Kickback and Self-Referral Rules were promulgated to allow hospitals to provide assistance to physicians in acquiring and using HIT.⁹

With the passage of the Health Information Technology for Clinical and Economic Health (HITECH) Act, enacted in 2009 as part of the American Recovery and Reinvestment Act (ARRA), the Obama administration embarked on a renewed effort to accomplish the goal of universal adoption of HIT by 2014.¹⁰ HITECH was enacted primarily in response to a stated need for widespread adoption of HIT. HITECH is also an acknowledgement that the privacy and security of e-PHI remains a priority. The rule-making process is ongoing. It, at least implicitly, recognizes that a resolution of those concerns continues to be problematic. It is not clear that policy-makers have considered the overall economic effects of compliance with an increasingly complex regulatory scheme, and the penalties for non-compliance, on the overall cost of health care. That is not to say that privacy protection is unimportant: rather, that we can and should direct more effort toward technological solutions.

The “meaningful use” requirement of EHR subsidies under HITECH continues to plague the rule-making process, and creates significant uncertainty among providers as to willingness to commit to EHR.

Worries over the security of EHR are increasing because of recurring, well-publicized breaches in electronically-stored information in general. HIPAA¹¹ came about primarily in response to consumer pressure on health insurance companies denying coverage for pre-existing conditions, when changing from one company to another. By the time it was enacted in 1996, it was to become a comprehensive, complex body of legislation and subsequent rules that dramatically changed our law on the privacy¹²

5 Institute of Medicine, *To Err is Human: Building a Safer Health System*, Committee on Quality of Health Care in America, Ed. Kohn LT, et al, Washington, DC, National Academies Press, 2000.

6 Institute of Medicine, *Crossing the Quality Chasm: A New Health System for the 21st Century*, Committee on Quality of Health Care in America, Washington, DC, National Academies Press, 2001.

7 Executive Order No. 13335, Incentives for the Use of Health information Technology and Establishing the Position of the National Health Information Technology Coordinator, April 27, 2004, www.archives.gov/federal-register/executive-orders/2004.html (last access 5/12/10), 69 FR 24059, May 5, 2004.

8 Executive Order No. 13410, August 22, 2006, Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs, www.archives.gov/federal-register/executive-orders/2006.html (last access 1/13/09), 71 FR 51089, 8/26/06.

9 71 FR 45110-45171 (August 8, 2006).

10 HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH (HITECH) ACT, Title XIII of Division A and Title IV of Division B of the AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009) http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.txt.pdf (last access 5/12/10).

11 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT, Pub. L. 104-191, 1996.

12 *Standards for Privacy of Individually Identifiable Health Information* (“Privacy Rule [2000, 2002]”), 45 CFR 160 and 164, Subparts A and E, www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html (last access 5/12/10).

and security¹³ of protections of individually identifiable health information. Although not exclusively related to electronically stored and transmitted health information, it recognized how electronic acquisition and transmission of health information created an increased need for data security, and created a framework for the handling of such health information. HIPAA and its accompanying rules are complex. “Many patients . . . are unaware that they already have the right to access their health information under the Health Insurance Portability and Accountability Act (HIPAA).”¹⁴

Attempts to solve problems related to privacy and security have largely been in the form of HIPAA regulations, with thousands upon thousands of complaints, but remarkably few penalties to date. HITECH has expanded the scope of privacy and security regulation, notably by extending the responsibilities placed on covered entities to business associates, ramping up enforcement by increasing penalties, and adding requirements for breach notification. Neither HIPAA nor HITECH creates a private right of action for a security breach, and patients must rely on the threat of penalties to users of EHR systems for protection. There is no reason to think that there might not be a private cause of action under state law, however. Unfortunately, though, once there has been a breach, there is no way to undo it, and damages may be difficult to assess and prove.¹⁵

The concerns of health care providers.

Physicians and their patients, and advocacy groups,¹⁶ continue to be concerned about the issues of privacy protection, and the protection of confidential physician-patient communications. Moreover, with the increasing use of the EHR, physicians have come to recognize and articulate a number of concerns relating to cost, patient safety, and alterations in workflow.^{17,18,19,20} “We have observed the electronic medical record become a powerful vehicle for perpetuating erroneous information, leading to diagnostic errors that gain momentum when passed on electronically.”²¹

While the cost of purchasing and maintaining EHR systems is a real consideration, it is not clear that federal policy-makers have gotten the message that providing financial incentives for adoption may not be the best way to achieve an optimal integration of HIT into the health care system, even if those incentives do increase adoption. In fact, the proposed economic incentives, while serving to defray the cost of EHR implementation and maintenance, may well turn out to be a pittance, when viewed in the

13 *Security Standards for the Protection of Electronic Protected Health Information* (“Security Rule [2003]”), www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html (access 5/12/10)

14 Mary Mosquera, *Patient access to e-record urgent, advocate tells federal panel*, Healthcare IT News, 4/22/10, www.healthcareitnews.com/news/patient-access-e-record-urgent-advocate-tells-federal-panel (access 5/12/10), quoting Joy Pitts, Chief Privacy Officer for the Office of National Coordinator for Health Information Technology.

15 Letter from Representative Henry Waxman (D-CA), attached as Appendix B

16 See, for example, Patient Privacy Rights, <http://patientprivacyrights.org/> (access 5/12/10).

17 Alexi Mostrous, *Electronic records not seen as a cure-all; As White House pushes expansion, critics cite errors, drop-off in care*, Washington Post, 10/25/09 www.washingtonpost.com/wp-dyn/content/article/2009/10/24/AR2009102400967.html (access 5/12/10), citing Letter from Senator Charles E. Grassley, 10/16/09, sample attached as Appendix A.

18 Hirschtick RE, *A Piece of My Mind. Copy and Paste*, JAMA 2006;295:2335-2336 <http://jama.ama-assn.org/cgi/content/extract/296/19/2315> (subscription required, access 5/12/10).

19 Siegler EL, and Adelman R, Editorial, *Copy and Paste: A Remediable Hazard of Electronic Health Records*, AM J MED 2010;495-496 www.ncbi.nlm.nih.gov/pubmed/19486708 (access 5/12/10).

20 Markel A, *Copy and Paste of Electronic Health Records: A Modern Medical Illness*, AM J MED 2010;123:e9 <http://articles.icmcc.org/2010/04/20/copy-and-paste-of-electronic-health-records-a-modern-medical-illness/> (access 5/12/10).

21 Hartzband P, and Groopman J, *Off the Record—Avoiding the Pitfalls of Going Electronic*, NEJM 2008;358:1656-1658 <http://content.nejm.org/cgi/content/full/358/16/1656> (subscription required, access 5/12/10).

long term.

eDiscovery

It has only been in the past two or three years that a substantial (though relatively small) number of health care institutions have gone paperless, and in the realm of litigation that relies primarily on medical records we have just begun to see the problems of cost, the access to accurate information, and authentication of evidence in the EHR and other sources containing relevant health information.

In Pennsylvania, “documents” includes electronically created data.²² Under Federal Rules, electronically stored information (ESI) is *not* a document: it is *sui generis* Electronically Stored Information (ESI).²³ Pennsylvania case law on e-discovery in general is sparse,²⁴ and non-existent as to limitations on discovery of the EHR.

Hash numbers are used for file identification and authentication, but also for encryption. As the use of encryption increases, we may see technical problems with file authentication and identification and authentication.²⁵

What should change?

Are the current approaches working?

With a few exceptions, the approach of the government to accomplishing the goal of universal adoption of EHR use has been to enable the existing paradigm of multiple proprietary vendors, with the belief that competition will be an effective means to arriving at the best EHR.

Interestingly, former House Speaker Newt Gingrich said HITECH's \$19 B in incentives, was “one of only two good things” in ARRA.²⁶ I suggest that the \$19B subsidy is not a very good idea. In effect, it provides incentives for institutional health care providers, group practices, and individual health care providers to adopt technology about which they still have significant concerns. Although cost is undoubtedly a factor in the poor rate of adoption, it is not the only one. Moreover, the dollar amounts will not be enough to maintain EHR systems, an important reason why we should get it right the first time. While it is likely that significant cost savings will be achieved with the adoption of HIT, it is not clear that those cost savings will accrue to the entities paying for this technology, without a fundamental change in the way EHR systems are designed and maintained.

A number of initiatives suggests that we can do a better job of making EHR systems less costly, more interoperable, and more secure.

Recent vendor initiatives, the proposed “safe harbor” of encryption in the Final Interim Rule,²⁷ and

22 Pa. R.C.P. No. 4009.1 (2010).

23 F.R.C.P. 34 (12/1/06).

24 In *Brooks v. Frattaroli*, PICS 09-1709 (C.P. Lebanon, October 25, 2009) the Court relied on the new Federal Rules and adopted a balancing test, noting, “Somehow the legal system must develop a balanced approach that uses the truth-gathering potential of ESI without abusing a litigant's legitimate expectation of privacy.”

25 Don L. Lewis, *The Hash Algorithm Dilemma – Hash Value Collisions*, FORENSIC MAGAZINE, December 2009/January 2009, www.forensicmag.com/Article_Print.asp?pid=238 (access 5/12/10).

26 Alexi Mostrous, *As White House pushes expansion, critics cite errors, drop-off in care*, WASHINGTON POST, 10/25/09, <http://www.washingtonpost.com/wp-dyn/content/article/2009/10/24/AR2009102400967.html> (access 5/12/10).

27 See also Letter from Henry Waxman, et al, 10/1/09, attached as Appendix B.

legislation (2010) in Massachusetts and Nevada, are encouraging signs, but one has to wonder why it has taken so long to integrate encryption technology, which has been around for decades, into the EHR for the protection of ePHI.

H 6898,²⁸ introduced in September 2008, called for the establishment of an open source EHR that would be available to any health care provider at “nominal cost.” The bill further provided that the EHR system would be governed by a consortium. The Health Information Management Systems Society (HIMSS) vigorously opposed that provision and H 6898 never got out of committee. The rest of the bill was essentially an early draft of HITECH. Subsequently, Senator Jay Rockefeller (D-WV) has introduced the Health Information Public Utility Act,²⁹ currently in committee, which re-introduced the open source EHR provisions of H 6898, except that it was to apply only to rural and underserved populations. Given the well-known crisis in how we are going to pay for health care, why should such a restriction apply? The answer, I suggest, will be obvious to some.

Yet, the most important aspect of the open source provisions in H 6898 was, in fact, not cost, but lay in how an EHR system permits updating. H 6898 had the potential to provide for far more flexibility, innovation and entrepreneurial stimulation than does our present system of multiple proprietary vendors, who exercise the ultimate control over what modifications are made to EHR software.

The Veterans Administration Information Systems and Technology Architecture (Vista)³⁰ was developed by and for the VA health care system, and the code is freely available through the Freedom of Information Act. It can be downloaded at no cost. Its use in the medical community at large was explicitly suggested in H 6898. Under the General Public License (GPL), WorldVista, a child of Vista, can be installed and used by any health care entity (actually anybody, for that matter). Moreover, it can be modified by end users (with certain restrictions under the GPL,³¹ principally that modifications in code must be shared with other users). That means that individuals who actually use the software can adapt it for their own use, and other users can avail themselves of those improvements.

Let us digress for a moment to describe another system in which scientific progress in health care delivery is achieved by the ability to modify accepted procedures in an environment where such modifications are made available to others: surgical pedagogy. For centuries, surgeons learned how to do particular operations from other surgeons, whether teachers or colleagues. As they gained experience in a particular procedure, modifications could be made, based upon experience, new medical knowledge, unique characteristics of the condition they were treating, and new technology.³² Typically, those modifications in technique were, and are, often shared with others in medical publications, i.e., journals, lectures and demonstrations, without a licensing cost to the recipients. This model has worked well, and continues to work well.³³

28 [Health-e Information Technology Act of 2008](#), “To promote the adoption and meaningful use of health information technology, and other purposes.” (access 5/12/10).

29 [S. 890](#), introduced April 23, 2009, (access 5/12/10).

30 Colene M. Byrne, et al, *The Value From Investments In Health Information Technology at The U.S. Department of Veterans Affairs*, HEALTH AFFAIRS, 2010;29:629-638 <http://content.healthaffairs.org/cgi/reprint/29/4/629?ijkey=zm91rS/ZFWdqE&keytype=ref&siteid=healthaff> (access 5/12/10).

31 See, for example, http://worldvista.org/World_Vista_EHR/license-and-readme/WorldVista%20EHR%20GPL%20License.txt/view (access 5/12/10).

32 Modifications to established surgical procedures, and even novel surgical procedures are not subject to the regulatory restraints imposed upon the introduction of, say, a new drug or device.

33 See Samuel L. Pallin, M.D. v. Jack A. Singer, M.D. And Hitchcock Clinic, U.S. District Court, VT (1993), where an ophthalmic surgeon obtained a patent for “no-stitch” cataract surgery, and sued another surgeon for infringement. There

Thus, if health care providers, i.e., end-users, have the ability to directly modify EHR software to improve it, and share those modifications with other users, the capacity for developing user-friendly, future-proof, and effective EHR software is vastly increased. Such a method of EHR software development need not even be restricted to only free code. Kohane and Mandl³⁴ have proposed a scheme in which an EHR system is modular: plug-ins, either open source or proprietary, can be developed and integrated into an existing EHR system. If the users decide a particular module is not working well for them, they can “unplug” it and get another one. The authors liken this to the iPhone model.

Regarding the protection of patient privacy and of the confidentiality of physician-patient communications, the ability of patient advocacy groups and physicians to make direct improvements in EHR systems is critical. Both physicians and patients are, after all, the ones who have the most vested interest in these protections. It is most likely, then, that they can develop creative methods that provide technological protections, rather than relying mostly on the complex and imperfect regulatory scheme written into HIPAA and HITECH. A common misconception is that, because source code is “open,” it would be vulnerable to hacking and security breaches. Pretty Good Privacy (PGP) is as good as any encryption available, but it makes its code is publicly available. In a white paper published in 2008, HIMSS noted that,

There is an unfortunate tendency to conflate secrecy with security. When such confusion reigns, then it is easy to carelessly assume that open source code must not provide the same degree of security as proprietary code. In other arenas, such as elections, where privacy and security are very important, it has become apparent that using open source code is likely to ameliorate security concerns rather than increase them. . . .

A recent study demonstrated that a substantial number of projects in the U.S. Department of Defense and in the Intelligence communities have been implemented using open source software and that security considerations were critical in making the choice (<http://www.federalopensourcealliance.com/#Study>). If anything, use of open source software enhances security.³⁵

Obviously, for such a system to function properly and without utter chaos, a governing body (such as the “consortium” proposed in H 6898) is necessary, so that updated versions can be released at intervals (and provided free of charge to users).

Such an intellectual property regime does not mean that an EHR system will cost nothing to its users. There will still be costs associated with training users, technical support, reduced productivity associated with implementation, and perhaps some monetary contribution to maintain the governing “consortium.” Also necessary will be a critical mass of users who actively contribute to innovations and improvements. While users may not necessarily be remunerated financially for their contributions, they would benefit from the contributions of others so situated. Above all, it matters who has access to software code, and who can change it. If we do not have free access and ability to modify it, code has a

was widespread opposition from within the medical community, on the grounds that enforcement of patents on surgical procedures would stifle, rather than encourage, innovation, and Congress ultimately passed legislation that prohibited enforcement of patents on surgical procedures (P.L. 104-208, 110 Stat. 3009-67, Section 616, Limitation on Patent Infringements Relating to a Medical Practitioner's Performance of a Medical Activity, September, 1996), 35 USC 287(c) (1).

34 Mandl, KD, and Kohane, IS, *No Small Change for the Health Information Economy*, NEJM 2009:360:1278-1281 <http://content.nejm.org/cgi/content/full/360/13/1278> (access 5/12/10).

35 HIMSS Healthcare Information Exchange Open Source Task Force, *Evaluating Open Source Software for Health Information Exchange*, June 2008 www.himss.org/ASP/topics_FocusDynamic.asp?faid=141 (access 5/12/10).

way of controlling our lives in invisible ways that EHR users and their patients don't always understand.³⁶

Where there are proprietary add-ons to open source systems, such an intellectual property environment may generate legal issues. There may be issues as to who would be liable for defects in software design that cause medical errors. It is well to remember, though, that typically, proprietary vendors disclaim liability for such defects through “hold harmless” clauses in EULAs, gag orders that prohibit disclosure of software defects by providers, and the learned intermediary doctrine.³⁷ Additionally, an open source system would enable more rapid and efficient bug detection and reporting, so that corrections could be distributed quickly.

Rather than creating what are, in the long run, probably marginally significant incentives for physicians and hospitals to adopt EHR technology they might not otherwise adopt, would it not be better to create a legal environment, i.e. intellectual property regime, and regulatory “consortium” that fosters innovation in a way that makes the EHR more user-friendly, safer, adaptable, less costly, and more protective of patient privacy and the confidentiality of physician-patient communications? The development of such an environment would likely obviate the need for certification bodies and the establishment of “meaningful use” criteria.

There has been, in fact, some recent activity toward the development of an open source EHR, in addition to Vista. The National Cancer Institute has announced the release of an open source patient record. “The standards-based software has core EHR features for sharing information about patient diagnosis, treatment and outcomes.”³⁸ Additionally, a number of smaller hospitals have adopted Vista-based open source EHR systems, perhaps largely for economic reasons.³⁹

“The government ought to mandate open source products based on open source reference implementations to improve security, get higher quality software, lower costs, higher reliability - all the benefits that come with open software.”⁴⁰ In developing national HIT, India seems to have recognized this some time ago.⁴¹

Conclusion

The *need* for integration of HIT into health care delivery, public health, and medical research is not questioned (and in any event, inevitable), in terms of efficiency, safety, and the betterment of personal and public health. Nonetheless, the potential for loss of individual privacy, economic burdens on an already strapped (and to some, unsustainable) healthcare system, inefficiency, and propagation of harmful errors is enormous. How we develop HIT in the coming years is crucial. Rather than focusing mainly on government subsidies and regulation of HIT vendors and users, we should develop policy that enables healthcare providers, public health agencies and research entities to have a more proactive

36 *This is a paraphrase.* See Lawrence Lessig, *CODE, VERSION 2.0*, Basic Books, New York, 2006, p. 138. “Code-based regulation— especially of people who are not themselves technically expert— risks making regulation invisible. Controls are imposed for particular policy reasons, but people experience those controls as nature.”

37 Letter from Senator Charles E. Grassley, 10/16/09, attached as Appendix A.

38 Mary Mosquera, *NCI to offer cancer e-care record*, Healthcare IT News, 4/20/10, www.healthcareitnews.com/news/nci-offer-cancer-e-care-record (access 5/12/10)

39 *For example*, Kern Medical Center, Bakersfield, CA; Oroville (CA) Hospital; Beauregard Memorial Hospital, DeRidder, LA; and Midland (TX) Memorial Hospital.

40 Scott McNealy, Sun Microsystems, news.bbc.co.uk/2/hi/technology/7841486.stm (access 5/12/10).

41 See Jim Dowling and Seif Haridi, *Developing a Distributed Electronic Health-Record Store for India* <http://ercim-news.ercim.org/content/view/444/656/> (access 5/12/10).

role in creating technological solutions to legal and other problems that are created by HIT adoption and utilization.