

## REPORT

While existing ABA policy calls for protection of personal health information and of the confidentiality of physician-patient communications, it does not explicitly refer to technological methods, and implicitly restricts methods to rules and regulations regarding permissible disclosures, and it does not recognize the need for open source code EHR systems to achieve that goal, i.e., the need to enable meaningful input from end user providers and patients, who are the key interested parties in the preservation of privacy and confidentiality.

More than five years after Executive Order 13335,<sup>1</sup> health care providers in the United States continue to lag behind those of other developed countries in the adoption of the electronic health record (EHR), a cornerstone of health information technology (HIT). Universal adoption of EHR will significantly improve the safety, efficiency, and quality of health care in the United States, and benefit the public health.

There are several reasons why adoption of EHR in the United States has been slow. Concerns about the protection of personal health information, the confidentiality of physician-patient communications, and other personal data are foremost. A recent report commissioned by the Agency for Healthcare Research and Quality (AHRQ) has documented that members of the public “believe that if they do not participate in making [decisions about the design of health IT to safeguard the privacy and security of their medical data], then parties who did not have the best interests of patients in mind might make these decisions.”<sup>2</sup> That same report points out that “participants [in the study] consistently had strong feelings about the effect of computers upon the privacy of personal information,” and “wanted some assurance that their medical data would be secure and used only in ways that they authorized.”<sup>3</sup> At the 2009 Computers, Freedom and Privacy conference, a panel of experts took up the question of how do health IT providers ensure that patients remain in control of their most sensitive personal data in a digital healthcare regime, acknowledging that it doesn't really have an answer at this point.<sup>4</sup> More recently, concerns have been raised about the ability to “re-identify” anonymized personal health information.<sup>5</sup> We

---

<sup>1</sup> 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](http://www.archives.gov/federal-register/executive-orders/2004.html) (last access 12/16/09), 69 FR 24059, May 5, 2004.

<sup>2</sup> FINAL REPORT: CONSUMER ENGAGEMENT IN DEVELOPING ELECTRONIC HEALTH INFORMATION SYSTEMS, July, 2009 [http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS\\_0\\_888520\\_0\\_0\\_18/09-0081-EF.pdf](http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_888520_0_0_18/09-0081-EF.pdf) p.40 (last access 9/24/09).

<sup>3</sup> FINAL REPORT: CONSUMER ENGAGEMENT IN DEVELOPING ELECTRONIC HEALTH INFORMATION SYSTEMS, July, 2009 [http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS\\_0\\_888520\\_0\\_0\\_18/09-0081-EF.pdf](http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_888520_0_0_18/09-0081-EF.pdf) p. 38 (last access 9/24/09).

<sup>4</sup> Kenneth Corbin, *Privacy a Stumbling Block in Healthcare IT*, June 3, 2009 [www.internetnews.com/government/article.php/3823361](http://www.internetnews.com/government/article.php/3823361) (last access 12/16/09).

<sup>5</sup> Natasha Singer, *When 2+2 Equals a Privacy Question*, NEW YORK TIMES, October 18, 2009 (Sunday Business, p. 4) <http://www.nytimes.com/2009/10/18/business/18stream.html?th&emc=th> (last access 12/16/09), referencing Arvind Narayanan and Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, [http://www.cs.utexas.edu/~shmat/shmat\\_oak08netflix.pdf](http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf) or <http://www.cs.utexas.edu/~shmat/> (last access 12/16/09).

continue to see reports of inadequate data protection.<sup>6</sup>

While the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is believed by some to provide such protection, it is seen by others as a sieve. The Food and Drug Administration Amendments Act of 2007 (FDAAA) “authorizes the FDA to oversee development of a nationwide data network, the Sentinel System, aimed at including data for 25 million patients by July 2010, and 100 million by July 2012.”<sup>7</sup> The Institute of Medicine has recognized that there is a need to improve the privacy and data security of health information in the context of health research.<sup>8</sup> The widespread acquisition of personal health information by electronic means other than the EHR has led to a proliferation of databases.<sup>9</sup>

The Obama Administration has clearly enunciated a re-commitment to the stated objectives of Executive Order 13335. On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009 (ARRA).<sup>10</sup> That legislation includes provisions that codify the establishment of the Office of National Coordinator of Health Information Technology (ONCHIT), originally a creation of Executive Order 13335. It also provides for a HIT Policy Committee, and a HIT Standards Committee. The composition of membership of the HIT Standards Committee

“shall at least reflect providers, ancillary health care workers, consumers, purchasers, health plans, technology vendors, researchers, relevant Federal agencies, and individuals with technical expertise in health care quality, privacy and security, and in the electronic exchange and use of health information.”

The membership of the HIT Policy Committee consists of at least 20 individuals, but with only at least one physician, and one expert in health information privacy and security, and “[s]uch other members as shall be appointed by the President as representatives of other relevant Federal Agencies.”<sup>11</sup>

<sup>6</sup> Molly Merrill, *New survey shows healthcare IT executives worried about data security*, HEALTHCARE IT NEWS, 3/3/08, <http://www.healthcareitnews.com/news/new-survey-shows-healthcare-it-executives-worried-about-data-security> (last access 12/16/09); Molly Merrill, *Survey: Healthcare organizations’ security not up to HITECH standards*, HEALTHCARE IT NEWS, 11/4/09, <http://www.healthcareitnews.com/news/survey-healthcare-organizations-security-not-hitech-standards> (last access 12/15/09).

<sup>7</sup> Barbara J. Evans, *Congress’ New Infrastructural Model of Medical Privacy*, 84 NOTRE DAME LAW REVIEW, 585-654 (2009).

<sup>8</sup> Institute of Medicine, *BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH*, National Academies Press, 2009, [www.iom.edu/CMS/3740/43729/61796.aspx](http://www.iom.edu/CMS/3740/43729/61796.aspx) (last access 12/16/09).

<sup>9</sup> Edward F. Shay, *Health Care Databases and the Law*, PENNSYLVANIA HEALTH LAW INSTITUTE, Philadelphia, 3/13/09, [www.pbi.org](http://www.pbi.org) (last access 12/16/09, subscription required).

<sup>10</sup> American Recovery and Reinvestment Act of 2009 (ARRA). Title XIII of Sec. 2, Division A (p. 112), Sec 13001 contains the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Sec. 3000-3009 [http://thomas.loc.gov/cgi-bin/t2GPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111\\_cong\\_bills&docid=f:h1enr.txt.pdf](http://thomas.loc.gov/cgi-bin/t2GPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.txt.pdf) (last access 12/16/09).

<sup>11</sup> See Note 10, Sec. 3003(c)(2).

ARRA also incorporates the recommendations of the ONC-Coordinated Federal Health IT Strategic Plan: 2008-2012.<sup>12</sup> That report was completed in part in response to a report of the GAO, dated February 1, 2007, which called for a “comprehensive privacy approach” for the protection of personally identifiable health information.<sup>13</sup> In a subsequent report of September 17, 2008, the GAO noted that

“[HHS’s privacy approach has] fallen short of fully implementing GAO’s recommendation. In particular, HHS’s privacy approach does not include a defined process for assessing and prioritizing the many privacy-related initiatives to ensure that key privacy principles and challenges will be fully and adequately addressed.”<sup>14</sup>

An indispensable link in the protection of patient privacy and of the confidentiality of physician-patient communications is the security of EHR systems. A white paper, *Evaluating Open Source Software for Health Information Exchange*,<sup>15</sup> published by the Health Information Management Systems Society (HIMSS) in June of 2008 contains the following statement:

“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. If anything, use of open source software enhances security.”<sup>16</sup>

ARRA contains a number of provisions designed to protect patients’ privacy by means of regulation—more stringent than those imposed by HIPAA—along with strict penalties for violations. Additionally, these new provisions of ARRA also seem to require the HIT Policy Committee to “make recommendations” for, among other things,

Technologies that protect the privacy of health information and promote security in a qualified electronic health record, including for the segmentation and protection from disclosure of specific and sensitive individually identifiable health information with the goal of minimizing the reluctance of patients to seek care (or disclose information about a condition) because of privacy concerns, in accordance with applicable law, and for the use and disclosure of limited data sets of such information.<sup>17</sup>

Somewhat troubling, however, is the language,

Technologies that allow individually identifiable health information to be rendered unusable, unreadable, or indecipherable to unauthorized individuals when such information is transmitted in the nationwide health information network or physically transported outside of the secured, physical perimeter of a health care provider, *health plan, or health care clearinghouse* [italics added].<sup>18</sup>

<sup>12</sup> June 3, 2008. The report was supported under contract GS10F0223P by professional staff from Avalere Health LLC. Under ARRA, the National Coordinator is tasked with “updating” this report (§3001(c)(3)).

<sup>13</sup> See [www.gao.gov/new.items/d07400t.pdf](http://www.gao.gov/new.items/d07400t.pdf) (last access 3/2/09).

<sup>14</sup> See [www.gao.gov/new.items/d07400t.pdf](http://www.gao.gov/new.items/d07400t.pdf) (last access 3/2/09).

<sup>15</sup> See [www.himss.org/HIMSSWeeklyInsider/HIMSSWeeklyInsider\\_20080827.htm](http://www.himss.org/HIMSSWeeklyInsider/HIMSSWeeklyInsider_20080827.htm) (last access 12/16/09).

<sup>16</sup> See Note 15, at p. 9 (last access 3/2/09).

<sup>17</sup> See Note 10, Sec. 3002(b)(2)(B)(i), p. 120.

<sup>18</sup> See Note 10, Sec. 3002(b)(2)(B)(vi), p. 121.

It is likely that technology can be developed that permits the orderly administration of the provision of health care services (including the determination of quality measures) without the disclosure of individually identifiable health information to the patient's health plan or health care clearinghouse. There is no inherent need for such disclosure and it should be permissible for patients to forbid it. A health plan or health care clearinghouse would only need to know that (1) the patient is eligible under the plan to receive the service at the time it was or is to be rendered, (2) the service was actually received by that individual, (3) and the service was medically appropriate and necessary.

Not only is more meaningful (than by regulation alone) protection of patients' privacy achievable by incorporating state-of-the-art security measures into the design of EHR systems, but also such technological protections will simplify and facilitate the day-to-day operation of EHR technology by end-users, without fear and uncertainty as to what disclosures are permissible.

To accomplish these goals, there must exist the capability for meaningful input from, among others, consumers (patients), and the health care providers whom they encounter face-to-face in the clinic and at the bedside, in both the development and the maintenance and upgrading of EHR systems. Protection of the confidentiality of physician-patient communications is a time-honored principle and essential to the delivery of quality health care. Thus, patients and their physicians—combined, the heart of health care delivery—must have meaningful input. “[A] real barrier to the success of a technological approach to protecting the privacy of personal medical information is not the limits of technology itself, but the fact that the entities with the resources to accomplish this task are the same entities whose interests are adverse to the protection of individual privacy.”<sup>19</sup> Only with open source code—with its unique advantage of permitting “many eyes” to examine it—will this kind of input and its timely implementation be possible.

Source code can be thought of as a translator of the instructions given by a human being to a machine (the computer)—in other words, it translates instructions from a human being into language the machine can understand. Making the source code open is like publishing a transcript of what a translator between two parties heard one say in one language and then told the other party in another language what was said. Thus, anyone can examine the “transcript” to see if indeed the “translator” (or source code) accurately reflects what the human being intended the machine to do. Since the source code is open, anyone (not just the “translator,” i.e., programmer) can check the “transcript” for accuracy and point out errors and propose corrections. Once more, the concept of “many eyes” having an opportunity to see the source code achieves the desired goal of transparency, along with its unique ability to facilitate timely innovation from a virtually unlimited number of sources. Only with open source EHR systems will treating physicians and their patients have the power to ensure maximum possible protections against unnecessary disclosure of personal health information and physician-patient communications. Code has a way of exerting control in invisible ways that physician-EHR users don't always understand, or even know about.<sup>20</sup> If the code is open, physicians and their patients

---

<sup>19</sup> Wilder, BL, Letter: Privacy of Electronic [Health] Information, JAMA 2000;283:1564-5 <http://jama.ama-assn.org/cgi/content/full/283/12/1564> (last access 6/17/09, subscription required).

<sup>20</sup> See Lawrence Lessig, *Code, Version 2.0*, Basic Books, New York, 2006, p. 138.

have the opportunity to identify and point out flaws that might allow for unwanted and unnecessary disclosures.

On September 15, 2008, H. 6898 was introduced before the 110<sup>th</sup> Congress, and called for the establishment of a federal open source Health IT system. Sec 3001(c)(4) of that Act reads as follows:

(4) FEDERAL OPEN SOURCE HEALTH IT SYSTEM-

“(A) IN GENERAL- The National Coordinator shall provide for coordinating the development, routine updating, and provision of an open source health information technology system that is either new or based on an open source health information technology system, such as Vista, that is in existence as of the date of the enactment of this title and that is in compliance with all applicable standards (for each category described in paragraph (2)(A)) that are adopted under this subtitle. The National Coordinator shall make such system publicly available for use, after appropriate pilot testing, as soon as practicable but not later than 9 months after the date of the adoption by the Secretary of the initial set of standards and guidance under section 3003(c).

“(B) CONSORTIUM- In order to carry out subparagraph (A), the National Coordinator shall establish, not later than 6 months after the date of the enactment of this section, a consortium comprised of individuals with technical, clinical, and legal expertise open source health information technology. The Secretary, through agencies with the Department, shall provide assistance to the consortium in conducting its activities under this paragraph.

“(C) AUTHORIZATION TO CHARGE NOMINAL FEE- The National Coordinator may impose a nominal fee for the adoption by a health care provider of the health information technology system developed or approved under subparagraph (A). Such fee shall take into account the circumstances of smaller providers and providers located in rural or other medically underserved areas.

“(D) OPEN SOURCE DEFINED- In this paragraph, the term ‘open source’ has the meaning given such term by the Open Source Initiative.[\[www.opensource.org\]](http://www.opensource.org)<sup>21</sup>

That bill was vigorously opposed by the proprietary software lobby and died with the end of the legislative session.<sup>22</sup>

The use of open source code in the setting of a national HIT infrastructure also has immense potential to enable features in addition to privacy protection, such as reasonable cost, “future-proofing” EHR systems, and the development of open standards for interoperability.

Respectfully submitted,

Bruce Wilder, ABA Member  
February 2010

<sup>21</sup> See <http://thomas.loc.gov> (last access 12/16/09).

<sup>22</sup> IT Bill criticized, JAMA 2008;300(18):2110.

## GENERAL INFORMATION FORM

Submitting Entity: Individual

Submitted By: Bruce Wilder

1. Summary of Recommendation(s).

The Recommendation urges the United States government to protect the privacy and security of personal health information and doctor-patient communications to the maximum extent possible by providing the optimal environment for achieving this goal through technological means, i.e., availability of open source code HIT that permits meaningful input by health care providers and their patients.

2. Approval by Submitting Entity.

At this time no entity has approved this Recommendation, but approval is anticipated. No entity has to date expressed disapproval or opposition.

3. Has this or a similar recommendation been submitted to the House or Board previously?

No

4. What existing Association policies are relevant to this recommendation and how would they be affected by its adoption?

While existing ABA policy calls for protection of personal health information and of the confidentiality of physician-patient communications, it does not explicitly refer to technological methods, or to policy that would facilitate the implementation of such methods.

5. What urgency exists which requires action at this meeting of the House?

Since passage of the American Recovery and Reinvestment Act of 2009, there has been a new push on the part of the Administration for the adoption of HIT by physicians and health care institutions. Even though proposals to facilitate open source HIT have been proposed in the past, the current effort has largely ignored open source systems, and will likely result in perpetuating the current patchwork of various HIT systems, that, among other things, fail to provide adequate protection of the privacy of individuals. Citations to support this are contained in the Report.

6. Status of Legislation. (If applicable.)

S890 (introduced 4/23/09 (Rockefeller, WV, referred to Senate Committee on Health, Education, Labor, and Pensions, 4/23/09), and H3124 (introduced 7/8/09, Fudge, OH-11, referred to House Subcommittee on Health, 7/10/09, **HEALTH INFORMATION TECHNOLOGY (IT) PUBLIC UTILITY ACT OF 2009**, intend “to provide for the use of improved health information technology with respect to certain safety net health care providers.” Please note, however that this proposed legislation refers to the use of current (open source) Veterans Administration EHR (VistA), and appears to have been introduced primarily to ease the economic burden of HIT adoption on rural and underpaid providers. It does not relate to the privacy concerns contained in the Report and Recommendation.

7. Cost to the Association. (Both direct and indirect costs.)

None. It is anticipated that ABA adoption of this Recommendation will strengthen the case for this method of privacy protection if the formulation of Administration Policy.

8. Disclosure of Interest. (If applicable.)

None, other than what is contained in the substance of the Report.

9. Referrals.

Comment has been solicited from the Sections of Health Law, Real Property Estates and Trusts Law, Administrative Law, Science and Technology, and Business Law. None has been received. The proposal has been discussed informally with a representative of the Section of Intellectual Property and input from that Section is anticipated. The Section of Individual Rights and Responsibilities has approved the Report and Recommendation in principle, but has not, to date, decided to sponsor or support them in their present form.

10. Contact Person. (Prior to the meeting.)

Bruce Wilder, 412 261-4040, [bwild@wildlaw.com](mailto:bwild@wildlaw.com)

11. Contact Person. (Who will present the report to the House.)

Bruce Wilder

## EXECUTIVE SUMMARY

### **1. Summary of Recommendation**

Protection of the individual's personal health information and of the confidentiality of physician-patient communications is a necessary component of effective health care delivery.

### **2. Summary of the issue which the recommendation addresses**

Along with the transformation of medical record-keeping to electronic entry, storage, and communication, has come tremendous vulnerability to unauthorized disclosure, propagation of errors, and identity-theft. The need for interoperability of different EHR systems is well-recognized, as is the need for strong data protection. While the security of individual EHR systems has become highly developed within the perimeter of those systems, legislation designed to protect personal health information and the confidentiality of physician-patient communications has relied on complex regulations as to what and to whom personal health information may be disclosed, with the threat of strict enforcement. As a method, this approach leaves much to be desired: (1) It is not clear that all disclosures that are permitted are necessary; (2) Individuals and institutions faced with decisions about what may be disclosed are often uncertain as to how much disclosure is permissible, and may over-react out of fear of incurring penalties; (3) and enforcement where there have been breaches has been uneven, and largely ineffective, at least as far as HIPAA goes. New restrictions and more strict enforcement under the HITECH Act do not alter this fundamental approach and may be counterproductive. Moreover, disclosures that may not be necessary are still permitted, even though HITECH imposes more stringent requirements and exposes handlers of electronically stored health information to the threat of more severe penalties when there is a violation.

### **3. Explanation of how the proposed policy position will address the issue**

The individuals who have the most interest in the protection of personal health information and the confidentiality of physician-patient communications are patients and their doctors. The policy statement asks that the ABA support law and public policy that emphasize the need for technological means to protect privacy and confidentiality to the maximum extent permissible (not just what is required) under law. To achieve this goal, EHR systems that permit the needed flexibility and capacity for innovation by patients and end user health care providers are necessary. For such an environment, it is necessary that the source code of EHR systems be open and available to all parties with a legitimate interest. Of course, it goes without saying that versions of such EHR systems in use need to be governed and maintained by a responsible entity, but it must be an entity that is primarily responsive to the concerns of patients and their doctors. An underlying assumption of this proposal is that an open source EHR system is necessary to achieve that end.

### **4. Summary of any minority views or opposition which have been identified**

To date the only known opposition to open source HIT has been grounded in the proposition that government should not have a role in the design of HIT systems.