by Rachel Hall
May 13, 2009

Your Liberty and Your Health: Protecting Electronic Health Records on the Nationwide Health Information Network

I. Introduction: Coordinating Care

Healthcare providers across the nation are implementing Electronic Health Record (EHR) systems. According to the market research firm Healthcare Information and Management Systems Society (HIMSS), almost 40 percent of hospitals now have the basics of an EHR system in place (Pelino, 2008). Functions of EHR systems vary widely, but in general they are automated clinical systems that include data related to medical history, patient demographics, clinicians' notes, drug information, electronic prescription, and diagnostic test orders (Venkatraman et al, 2008).

Healthcare providers are turning to EHRs because they are looking for better ways coordinate patient care. Care coordination remains one of the most formidable obstacles to providing lower-cost, effective health care in the United States. In a 2004 study, Eric Coleman followed patients for 30 days after discharge as they were transferred from one facility to another, and found that a full quarter of these patients experienced avoidable complications in their recovery due to poor coordination of care (Coleman, 2004). Some examples of failed care coordination include incomplete or inaccurate diagnoses, incorrect drug dosages and failure to employ indicated tests (IOM, 1999).

When patients see multiple healthcare providers to treat chronic conditions, they, too, face complications due to poorly coordinated care. For instance, they run the risk of paying two or three times—or even more—when different physicians order them to undergo repeat tests and procedures. In fact, providers have few incentives to avoid redundant procedures because our current healthcare system is based on a pay-per-service model of compensation. Several researchers have documented this problem within the last ten years (Hampton, 2008; Hostetter, 2007; Jacobson, 2002; McCarthy and Beck, 2007; Mertz and Folkemer, 2008). In its seminal 2001 report, *Crossing the Quality Chasm: A New Health System for the Twenty-first Century*, the Institute of Medicine (IOM) insists that health care delivery must be integrated in order to minimize redundancies, improve the quality of care transitions, and reduce the threat of medical errors (IOM, 2001).

EHR systems have vast potential for integrating the healthcare industry. By using electronic instead of paper systems, doctors will be able to quickly access critical information from patients' medical histories in emergency situations. Redundant tests and procedures will be reduced, ultimately lowering the cost of treatment. Information will be more easily standardized, permitting faster retrieval and review. Real-time public health surveillance will be possible, data collection speed will improve, research errors will be reduced, and better health education and training programs can be developed (Hampton, 2008).

However, most of the extraordinary advantages of EHRs have yet to be realized. This is because healthcare providers generally purchase EHR systems from private vendors, and most early versions of EHR systems are not interoperable with other versions. This means that providers from one organization cannot share EHRs with providers from other organizations (Kush et al, 2008). In fact, some larger organizations planned the implementation of their EHR systems so poorly that they have ended up using one system for their clinical services and another system altogether for their surgical services—this

was the case at the regional teaching hospital in New England where I worked from 2006-2008. This lack of interoperability directly negates the anticipated benefits of EHR systems.

In order for EHRs to be effective, they must be interoperable. Some healthcare providers have started sharing medical information within regionally or community-based organizations called Health Information Exchanges (HIEs) that aggregate encrypted data on a central server. However, even HIEs are quite limited in scope and most are not interoperable with one another.

In 2004, President Bush issued an executive order "to provide leadership for the development and nationwide implementation of an interoperable health information technology infrastructure" (EO 13,335). Thus, the Office of the National Coordinator (ONC) set out to develop a Nationwide Health Information Network (NHIN) that will make EHR systems across the nation interoperable with one another. From 2007 to 2008, the ONC awarded grants to 15 HIEs, including providers and Federal agencies, for a trial phase of this "network of networks" that is currently underway (HHS, n.d.). And in a January 2009 speech, President Obama pledged that his administration will continue to support this initiative, stating, "We will make the immediate investments necessary to ensure that within five years all of American's medical records are computerized" (Pear, 2009). With Kathleen Sebelius' recent confirmation as the Secretary of Health and Human Services on April 28, 2009, further developments regarding EHRs and the NHIN are on the very near horizon.

The advent of a network that will make patients' individually identifiable health information available electronically on a nationwide network opens up a host of practical and ethical concerns, such as data security, patient privacy, and confidentiality, that will need to be addressed by policy makers as the ONC moves forward with its initiatives (Bath, 2008). In this paper I examine uses of electronic health information by healthcare providers, private vendors, and the United States government. Although a digitally networked environment also has major legal implications concerning the use of aggregated anonymous health information for public health, research, education and commerce, my focus is specifically on individually identifiable information.

II. Use By Healthcare Providers

Right to Access

With health records going digital, there is growing concern that patients will withhold important medical information from their healthcare providers—or worse, not seek treatment at all—because they don't trust that the information will be secure. Patients might believe that unauthorized personnel will view their records, or that unauthorized digital copies of their medical information will be made and distributed.

In fact, electronic records can actually be more secure than paper records in many respects. Digital rights management (DRM) technology such as encryption and expiration dates can be employed to improve security. For example, complex password "keys" known only by authorized personnel could be required to link a patient's name to his electronic information. Electronic records can also be organized into security levels, giving users access to different levels of information depending on their security clearance (Myers et al, 2008). In another scenario, consider a patient who has been to see her neurologist after a severe concussion, but wants a second opinion from another provider. She could allow the second neurologist to access her electronic MRI, but only for a set period of time before that

particular copy of the data is programmed to "self-destruct." This limits the opportunity for unauthorized uses of her personal health information in the future.

Indeed, the security of the system architecture used to store and transmit electronic health records is a critical issue that many capable minds are studying and will require exploration beyond this paper. In its "Nationwide Privacy and Security Framework," the ONC emphasizes the need to establish trust in the NHIN's system architecture before the project can move forward meaningfully (ONC, 2008). But even supposing the system were entirely secure, such that only authorized persons were actually able to access a patient's health information, there are still many access questions to consider. For instance: who should be authorized to access a patient's information in the first place: The Emergency Department doctor who treats a patient after a car accident? Nurses who work down the hall from the unit where a patient is admitted? A patient's health insurance company? His *auto* insurance company? His employer, bank, or credit card company? What about real estate agents and marketing firms?

Patients might be surprised when they discover the extent of who can already gain access to their health information. Twila Brase of the Citizens' Council on Health Care warns that "'As long as they call themselves public health, they can get medical data.' The Federal Aviation Administration 'announced a couple of years ago; they said that they would be considered a public health entity so they could ask for public health data and get it under HIPAA'" (Conn, 2008). Likewise, banks, investment companies, data processing firms and pharmaceutical companies are among the potential users of HIPAA-protected health information under the Leach Bliley Financial Services Act (Robertson, 2008). If health information is available electronically via a nationwide network, the scope of this access will increase significantly. But is it reasonable to allow an *investment* company to use the NHIN to access a patient's full medical history?

Marcia Stepanek has written about the dangers of "weblining," a practice in which companies aggressively gather information about their client-base to determine what services they will offer to each individual (Stepanek, 2000). Marketing companies such as Acxiom, Naviant Technologies Inc., and HotData are aggregating massive amounts of digital consumer data and selling this information to companies who want to attract high-value customers—and "weed out" the losers. The opportunities for discrimination are troubling enough as is, but imagine the risk if companies that engage in weblining are able to access electronic health information. In the wrong hands, this information could compromise a patient's job, credit history, insurance coverage, and more: for instance, a financial institution could deny services to consumers who have lung cancer; an employer could decide not to hire candidates with sickle cell anemia; a university could choose not to admit students with a history of psychiatric treatment; a real estate agency could show only certain properties to women who have had an abortion. We must do everything we can to prevent this from happening.

Under the direction of Secretary Mike Leavitt in December 2008, the ONC published a "Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information" to address pressing privacy concerns such as these. The document outlines eight principles "to guide the actions of all health care-related persons and entities that participate in a network for the purpose of electronic exchange of individually identifiable health information" (ONC, 2008). Four of these principles relate to access:

- *Individual access*, in that consumers should be provided with a simple and timely means to access and obtain their personal health information in a readable form and format.
- *Openness and transparency*, in that consumers should have information about the policies and practices related to the collection, use and disclosure of their personal information.
- *Individual choice*, in that consumers should be empowered to make decisions about with whom, when, and how their personal health information is shared (or not shared).
- *Collection, use, and disclosure limitation*, in that it is important to limit the collection, use and disclosure of personal health information to the extent necessary to accomplish a specified purpose.

While these principles are useful, they are not intended to serve as regulations. The report states that, "Where these principles set higher standards than legal requirements, adherence to these principles is encouraged." In other words, these principles are essentially just strongly worded suggestions. And perhaps they are not so strongly worded after all—the report does not indicate *how* patients ought to be empowered to make decisions, nor does it draw a much-needed distinction between appropriate and inappropriate "specified purposes."

In England, where the socialized healthcare system is rapidly adopting EHRs under the "Connecting for Health" project, the National Health Service (NHS) recently enacted a regulation that requires explicit patient consent before any person whatsoever can access the patient's EHR (Nursing Standard, 2008). This solution empowers the patient completely; however, it can also be viewed as a bureaucratic nightmare that complicates administrative duties and jeopardizes emergency care. Healthcare providers in England are now required to justify access of patient health records in emergency situations if consent was not obtained. If the United States were to adopt a similar model that requires patient consent for access, clear exceptions would need to be outlined for medical emergencies as well as routine clerical functions.

And of course, even in a highly secure environment, occasional security breaches are inevitable. For instance, Margaret Amatayakul documents the phenomenon of inquisitive health care workers peeking into Britney Spears' and other celebrities' medical records (Amatayakul, 2008). The ONC addresses this particular access issue with another privacy principle:

- *Accountability*, in that those who break rules and put consumers' personal health information at risk must not be tolerated. Consumers need to be confident that violators will be held accountable.

Several proposals suggest that patients must be notified when the privacy of their EHRs have been compromised without their consent (Pear, 2009). Perhaps an even more empowering solution would be to allow patients to view an audit trail of anyone who has accessed or modified their records via the NHIN. This is one distinct advantage that EHRs hold over traditional paper records—in digital environments, audit trails and security breaches can readily be recorded.

Right to Content:

Patients have a stake not only in *whom* is authorized to access their EHR, but also in the *extent and accuracy* of information that is actually stored in their EHR. If their record

contains any errors whatsoever, the quality of healthcare that the patient will receive could be severely jeopardized. The remaining two principles of the ONC's "Nationwide Privacy and Security Framework" pertain to the content of the records themselves:

- *Correction*, in that consumers should be provided with a timely means to dispute the accuracy or integrity of their personal identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied. Consumers should also be able to add to and amend personal health information in products controlled by them such as personal health records.
- *Data integrity*, in that those who hold records must take reasonable steps to ensure that information is accurate and up-to-date and has not been altered or destroyed in an unauthorized manner.

These principles address the accuracy of EHRs, but fail to adequately empower patients in the event of a dispute. Indeed, this model presumes that a physician's diagnosis is the final word and gives patients very little control over what goes into their medical histories once the diagnosis has been delivered. But why should health information belong to the healthcare system rather than to the patients? In a nationwide network of interoperable electronic health information, a bad diagnosis will follow a patient throughout her life. If she disputes the accuracy of the diagnosis, then this, too, will be recorded in her EHR so that all future healthcare providers will know her as someone who disturbs the status quo—she might then struggle to find a physician who is willing to treat her. And even if her diagnoses are all completely accurate, why shouldn't the patient be able to choose for herself what personal information she will disclose to the purveyors of her EHR? Perhaps some highly contagious conditions need to be documented for disease control purposes, but these conditions should be the rare exception.

In 2008, the NHS "Connecting Through Health" project established that every patient in England will actually have two separate EHRs—one called the "Summary Care" record and another called the "HealthSpace" record. According to Michael Kidd, the Summary Care record is "a centrally stored summary of health information created initially from general practitioner records. It contains information on current medications, adverse reactions, and allergies." HealthSpace, on the other hand, is "a separate initiative that allows patients to record selected data in their own internet based health record, with control over how they share this record with healthcare providers" (Kidd, 2008). Once again, this approach completely empowers the patient. Not only is she able to choose who accesses her records, but she also decides what the records contain, as well. It will most likely be in her best interest to provide full disclosure to her healthcare provider—but it is ultimately up to the patient to make this decision.

This model is viable in England because the healthcare system is socialized and patients cannot be denied treatment for previously existing conditions. In the United States, however, most patients rely on health insurance companies to pay the high costs for their care, and insurance companies require patients to provide full disclosure of their medical histories. Unless the healthcare system in the United States were to change to guarantee all patients a certain degree of affordable medical coverage, patients will be compelled to abide by a health record model in which the doctor is always right and insurance companies have the right to know.

III. Use By Private Vendors

As medical information becomes increasingly digitized, private vendors are clamoring to grab a share of the market. In a 2007 article for the Wall Street Journal, Bill Gates of Microsoft writes that "increased digitization of health-care information alone will not solve the problems we face… patients never see this data, and doctors are unable to share it. Instead, individuals do their best to piece together the information that they think their caregivers might need about their medical history, the medications they take and the tests they've undergone" (Gates, 2007). He argues that patients, not doctors, should be in control of their own health information and who they share this information with—by using a *Microsoft product*. Microsoft and other private companies, such as Google, Wal-Mart, Intel, America's Health Insurance Plans, and the Blue Cross and Blue Shield Association, are developing internet-based applications that individuals can use to manage their Personal Health Records (PHRs) (Hampton, 2008).

Microsoft Health Vault and Google Health allow anyone to set up their very own PHR. By setting up a unique username and password, patients can build online health profiles where they will enter their health conditions, medications, allergies and lab results. They can import medical records and prescriptions from any of Microsoft or Google's partner hospitals and pharmacies. And they can also choose to share their health records with family members, friends and doctors, with the important caveat that they will always be able to see who has access to their information, and they can stop sharing this information at any time.

Ultimately, PHRs aim to be interoperable with other healthcare organizations' EHR systems via the NHIN—but there is currently no guarantee that private vendors operating on a nationwide network will be subject to the same privacy regulations that healthcare providers must follow, such as the Health Insurance Portability and Accountability Act (HIPAA) (Hampton, 2008). If a patient gives information to her doctor or another covered entity such as a health insurance company, then her information is protected under federal law—HIPAA requires healthcare providers to inform patients about how their information is being used and to whom it is disclosed; it limits the release of private health information without consent; it restricts the amount of information used and disclosed to the "minimum necessary;" and it calls for criminal and civil penalties for improper use or disclosure of information. However, if the same patient registers with a medical website that requests some of her personal health information, that website is probably not a HIPAA-covered entity and may therefore do whatever it likes with her information (Robertson, 2008).

Microsoft and Google recognize that many consumers are concerned about the privacy of their medical information, and both companies have taken steps to reassure consumers that their information is safe with them. Microsoft has joined the Coalition for Patient Privacy, vowing to meet the coalition's 17 principles for privacy, including patient control of all access, no secret databases, and no data mining (Hampton, 2008). And Google's website announces, "We believe that your health information belongs to you, and you should decide how much you share and whom you share it with… We store your information securely and privately."

But what exactly does Google mean by "securely and privately"? The fine print of Google Health's privacy policy assures consumers that "no personal or medical information in your Google Health profile is used to customize your google.com search results or used for advertising;" however, patient data stored on Google Health may be shared "between Google products to enable joint features" (Google Health, n.d.). And when patients choose to share medical records with third parties such as doctors and pharmacies, that information is then subject to the third party's privacy policy and Google no longer assumes any liability

for the information. If the patient decides to revoke access to a third party, she may do so at any time. However, Google acknowledges that the individual or company whose access she has revoked may have already seen the personal medical information or may have kept a copy of it, and this third party may—or may not—be governed by HIPAA regulations.

There is general consensus that private vendors like Microsoft and Google should be expected to adhere to a common set of basic standards to guard the privacy of personal health information. The National Committee on Vital and Health Statistics, which is the statutory public advisory body on health information policy to the Secretary of the Department of Health and Human Services, recommends the following: "Vendors should clarify the respective rights, obligations, and potential liabilities of patients, clinicians, and other stakeholders; consumers should have the right to make an informed choice concerning the uses of their personal information; and security should be ensured" (HHS, 2006). Some critics have even insisted that Microsoft Health Vault and Google Health should be subject to HIPAA regulations, but this is tricky territory indeed. Would this mean that any company collecting health data would have to follow HIPAA? How would "health data" be defined? Perhaps a company offers generic data storage to its customers, and then some of those customers choose to use the service to store their health information; would a HIPAA mandate restrict citizens to storing their health information with only government-approved data storage providers? Vendors could also argue that HIPAA regulations are unnecessarily restrictive, limiting innovative uses of health information that consumers have freely chosen to contract to them.

But as I have argued in the previous section, the potential abuses of personal health information are too grave to leave entirely unchecked. This paper recommends that Microsoft, Google and other PHR vendors be subject to the same federal privacy regulations as healthcare providers, including HIPAA Privacy and Security Rules, the Privacy Act of 1974, the Confidentiality of Alcohol and Drug Abuse Patient Records Regulation, and the Federal Information Security Management Act of 2002, *if they wish to participate in the National Health Information Network* (ONC, 2008). This draws a clear line between the organizations that are accountable and those that are exempt. It will also give private vendors an incentive to adopt standard privacy practices, because they will find it in their best interests to make their services interoperable with the nationwide network.

IV. Use By the United States Government

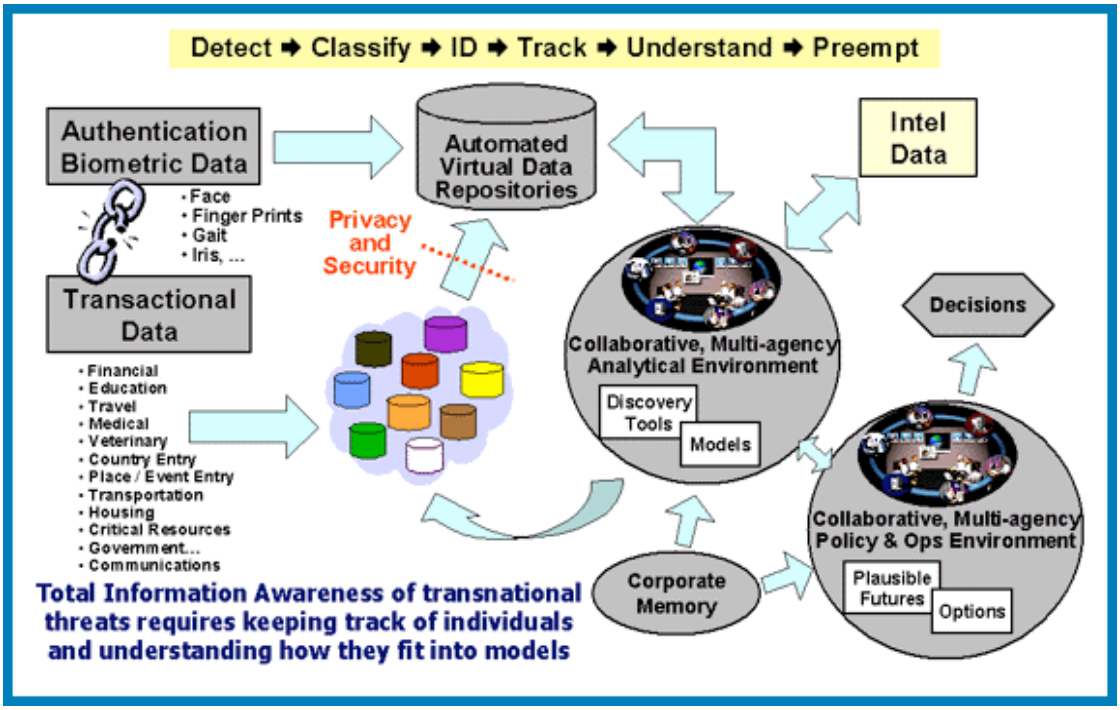
So far I have suggested that explicit consent should be obtained before any entity can access a patient's individually identifiable health information, and that all participants in a Nationwide Health Information Network—including health providers and private PHR vendors—should be regulated by existing healthcare privacy legislation. But where does this leave the U.S. government? Policy makers must consider whether government agencies should be exempt from these privacy regulations in special cases, such as law enforcement and anti-terrorism. As an example, I offer the following:

In 2002, Admiral John Poindexter approached the Department of Defense with an idea for a program called the Information Awareness Office (IAO) (EPIC, n.d.; Markoff, 2002; TAPAC, 2003). The purpose of the IAO, in Poindexter's words, would be to use information technology to "become much more efficient and more clever in the ways we find new sources of data, mine information from the new and old, generate information, make it available for analysis, convert it to knowledge, and create actionable options" (Poindexter,

2002). The Defense Advanced Research Projects Agency (DARPA) agreed to fund the IAO, and Admiral Poindexter officially launched the program later that year.

One of the IAO's first and most important initiatives was the Total Information Awareness (TIA) program—a world-wide database that the intelligence community was building so it could mine for data in order to "detect, classify, identify, and track terrorists so that we may understand their plans and act to prevent them from being executed" (Poindexter, 2002). Poindexter argued that terrorists leave "information signatures," and that the TIA database would help the Department of Defense learn how to recognize these signatures. However, this database did not just aggregate data on suspected terrorists. The objective was to collect as much data as possible from as many people as possible—regardless of whether or not the Department of Defense had any reason to suspect them of wrongdoing—in order to *predict* illegal activities and take *preemptive* measures against them.

A diagram of the TIA program from the IAO website (which has since been decommissioned) indicates that the IAO sought many types of what it called "Transactional Data," such as "Financial, Education, Travel, Medical, Veterinary, Country Entry, Place / Event Entry, Transportation, Housing, Critical Resources, Government…, Communications." Admiral Poindexter stated that, in order to aggregate all of this information, the government needed to "break down the stovepipes" that separate commercial and government databases (Poindexter, 2002). In 2002, Lieutenant Colonel Doug Dyer of the IAO approached the commercial data warehouse company Acxiom ($1B/year, with customers like Citibank and Walmart) to form a partnership between Acxiom and the TIA program. In an email to Poindexter dated May 21, 2002, Dyer wrote, "Acxiom could build this mega-scale database" (Dyer, 2002).



(the above image is from a mirror of the decommissioned IAO site, www.darpa.mil/iao/TIASystems.htm)

As information about the TIA reached the public through the news media and civil liberties organizations such as the American Civil Liberties Union (ACLU), Electronic Privacy Information Center (EPIC), and Electronic Frontier Foundation (EFF), concerns about the program grew and Congress reacted. On January 16, 2003, Senator Russell Feingold introduced legislation to suspend the activity of the IAO and TIA pending a Congressional review of privacy issues (Consolidated Appropriations Resolution, 2003). In response, DARPA presented Congress with a report on the Total Information Awareness program in May 2003, but by this time it had changed the name of the program to "*Terrorism* Information Awareness" (DARPA, 2003). But the name change did not persuade Congress, and in October 2003 it voted to prohibit further spending for the TIA by adding provisions to the Department of Defense Appropriations Act of 2004 (Department of Defense Appropriations Act, 2004).

But civil liberties organizations such as the EFF argue that the program hasn't really ended. Several of the IAO initiatives were allowed to continue; they were just moved to the Intelligence Community's center for Advanced Research and Development Activity (ARDA) and the name was changed to the "Novel Intelligence from Massive Data" project. Importantly, Congress mandated that this incarnation of the project would be restricted to only military or foreign intelligence purposes against foreigners (EFF, 2003). Meanwhile, the federal government continues to undertake several other data mining projects. For instance, the Computer Assisted Passenger Prescreening System (CAPSII) operates much like a smaller-scale version of the TIA, culling data from airlines, hotel, car-rental and credit card reports (Tien, 2003), and the General Accounting Office has issued a report of nearly 200 data mining projects by federal government agencies that are either operational or in planning (GAO, 2004).

The Total Information Awareness program specifically targeted medical records. Although this program was shut down in 2003, there is currently no guarantee that individually identifiable health information will not be used for similar federal programs in the future. These programs would essentially amount to government "data profiling" that would look for patterns in citizens' data to predict whether they planned to participate in illegal activity. In other words, citizens' activities could be restricted *before they even occurred*, based solely on a *predictive model*. As the Nationwide Health Information Network becomes a reality, we need strong privacy laws that will prohibit government agencies from accessing our Electronic Health Records unless they have lawfully obtained a warrant.

V. Conclusion

The Government Accountability Office has often criticized HHS for not coming up with a comprehensive healthcare information privacy policy to supplement HIPAA. They say that lack of a privacy policy is crippling IT promotion efforts (Modern Healthcare, 2008). The Office of National Coordinator did finally release a Privacy Standards Framework in December 2008, but this framework is not enough.

Certain privacy standards within the framework need to be made more explicit and written into legislation. For instance, the privacy standards should explain *how* patients will be empowered to decide who sees their information, and the standards should also draw a line between what constitutes appropriate and inappropriate uses of individually identifiable health information. To prevent discriminatory and exploitative uses of health information, patient consent should be required before health care providers or other entities can access

their records, although clear exceptions will need to be defined for emergency care as well as routine clerical functions. When it comes to the contents of the records themselves, patients—not doctors—should control what they choose to disclose in their EHR, unless they have been diagnosed with certain highly contagious diseases that are a matter of public health. However, if disclosure of health information is left up to patients instead of providers, questions remain about how insurance companies will handle coverage for previously existing conditions.

As private vendors start offering products for patients to manage their own information, they will find it in their best interests to make these Personal Health Records interoperable with the Nationwide Health Information Network. But if private vendors are allowed to participate in the NHIN, then these vendors should be accountable to the same privacy standards and regulations as healthcare providers themselves, including HIPAA, the Privacy Act of 1974, the Confidentiality of Alcohol and Drug Abuse Patient Records Regulation, and FISMA.

The U.S. government must not be exempt from any of these privacy standards. Government agencies should also be required to obtain explicit consent before accessing patient records, and they should be accountable to all applicable privacy legislation, unless they have lawfully obtained a warrant that authorizes other uses of individually identifiable health information.

The Nationwide Health Information Network is on its way, but before we can realize the enormous benefits that interoperable EHRs have to offer, including better care coordination, faster emergency responses, reduced redundancies and lower costs, we need to implement strong, unambiguous regulations that will protect patient privacy and prevent gross abuses of our civil liberties.

References

Amatayakul, M. (2008, May). Think a privacy breach couldn't happen at your facility? Think again. *Healthcare Financial Management*, 100-101.

Bath, P. (2008). Health informatics: current issues and challenges. *Journal of Information Science, 34*(4), 501-518. Retrieved from http://jis.sagepub.com/cgi/content/abstract/34/4/501

Coleman, E. (2004). Posthospital care transitions: patterns, complications, and risk identification. *HRS: Health Services Research, 39*(5), 1449-1465.

Conn, J. (2008). Who's peeking? *Modern Healthcare, 38*(41), 26-26.

Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, Division M, § 111(b).

Defense Advanced Research Projects Agency (DARPA). (2003). *Report to Congress regarding the Terrorism Information Awareness Program* (Report in response to Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, Division M, § 111(b). Retrieved from http://www.information-retrieval.info/docs/tia-exec-summ_20may2003.pdf

Defense Advanced Research Projects Agency (DARPA). (n.d.) Information Awareness Office. Retrieved on May 1, 2009, from http://web.archive.org/web/20030401082234/http://www.darpa.mil/iao/

Department of Defense Appropriations Act, 2004, Pub. L. No. 108–87, § 8131, 117 Stat. 1054, 1102 (2003).

Dyer, D. (2002). Ref: 02-F-0753. *Department of Defense Directorate For Freedom of Information and Security Review.* Retrieved from http://www.darpa.mil/iao/secpriv.pdf

Electronic Frontier Foundation (EFF). (2003). Total/Terrorism Information Awareness (TIA): is it truly dead? Retrieved from http://w2.eff.org/Privacy/TIA/20031003_comments.php

Electronic Privacy Information Center (EPIC). (n.d.) EPIC Terrorism (Total) Information Awareness page. Retrieved on May 1, 2009, from http://epic.org/privacy/profiling/tia/

Executive Order 13,335

United States General Accounting Office (GAO). (2004). *Data mining: federal efforts cover a wide range of uses* [Report]. Retrieved from http://www.gao.gov/new.items/d04548.pdf

Gates, W. (2007, October 8). Health care needs the Internet. *The Wall Street Journal*. Retrieved from http://www.wallstreetjournal.com

Google Health. (n.d.) Google Health privacy policy. Retrieved April 15, 2009, from http://www.google.com/intl/en-US/health/privacy.html

U.S. Department of Health and Human Services (HHS). (2006). *Personal health records and personal health record systems: a report and recommendations from the National Committee on Vital and Health Statistics* [Report]. Retrieved from http://www.ncvhs.hhs.gov/0602nhiirpt.pdf

U.S. Department of Health & Human Services (HHS). (n.d.) "Nationwide Health Information Network (NHIN): Trial Implementations"; Retrieved March 10, 2009, from http://www.hhs.gov/healthit/healthnetwork/trial/

Hampton, T. (2008). Groups push physicians and patients to embrace electronic health records. *JAMA, 299*(5), 507-509. Retrieved from http://jama.ama-assn.org/cgi/content/full/299/5/507

Hostetter, M. (2007, May/June). In focus: toward a system of coordinated care. *Quality Matters: Newsletter of the Commonwealth Fund*. Retrieved from http://www.commonwealthfund.org/Content/Newsletters/Quality-Matters/2007/May-June/In-Focus-Toward-a-System-of-Coordinated-Care.aspx

Institute of Medicine (IOM). (1999). *To err is human: building a safer health system* [Report]. Retrieved from http://www.iom.edu/File.aspx?ID=4117

Institute of Medicine (IOM), (2001). *Crossing the quality chasm: a new health system for the 21st century.* Retrieved from http://books.nap.edu/html/quality_chasm/reportbrief.pdf

Jacobson, J. (2002, May). Removing bottlenecks: how the HIPAA privacy rule may impact care coordination and healthcare quality—and steps HHS can take to protect them. *Health Management Technology*. Retrieved from http://www.healthmgttech.com

Kidd, M. (2008, May 6). Personal electronic health records: MySpace or HealthSpace? *BMJ 336*, 1029-1030. Retrieved from http://bmj.com/cgi/content/full/336/7652/1029

Kush, R., Helton, E., Rockhold, F. & Hardison, C. (2008). Electronic health records, medical research, and the tower of babel. *The New England Journal of Medicine 358*(16), 1738-1740. Retrieved from http://www.nejm.org

Markoff, J. (2002, November 9). Pentagon plans a computer system that would peek at personal data of Americans. *New York Times*. Retrieved from http://nytimes.com

McCarthy, D. & Beck, C. (2007, May/June). Case study: Summa Health System's care coordination network. *Quality Matters: Newsletter of the Commonwealth Fund*. Retrieved from http://commonwealthfund.org/Content/Newsletters/Quality-Matters/2007/May-June/Case-Study-Summa-Health-Systems-Care-Coordination-Network.aspx

Mertz, K. & Folkemer, D. (2008, June). High-tech medical: can electronic records transform healthcare? *State Legislatures*.

Modern Healthcare. (2008). EHRs don't make much headway; HHS hit for lack of privacy rule (Special Report). *Modern Healthcare, 38*(51), 31. Retrieved from Health Reference Center Academic database.

Myers, J., Frieden, T., Bherwani, K. & Henning, K. (2008). Privacy and public health at risk: public health confidentiality in the digital age. *American Journal of Public Health, 98*(5), 793-801.

Nursing Standard. (2008). Rule change clarifies process for consent to access records. *Nursing Standard, 23*(3), 6-6.

Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (ONC). (2008). *Nationwide privacy and security framework for electronic exchange of individually identifiable health information* [White paper]. Retrieved from http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf

Pear, R. (2009, January 18). Privacy issue complicates push to link medical data. *The New York Times*. Retrieved from http://nytimes.com

Pelino, D. (2008, September). Hospitals have collected mountains of patient and clinical data—now what? *Healthcare Financial Management*.

Poindexter, J. (2002). [address] Overview of the Information Awareness Office: remarks as prepared for delivery at DARPATech 2002 Conference, Anaheim, Calif., August 2. [Transcript] Retrieved May 1, 2009, from http://www.fas.org/irp/agency/dod/poindexter.html

Robertson, L. (2008, May/June). Who's looking at your medical records? *The Saturday Evening Post,* 54-57, 92.

Stepanek, M. (2000, April 3). Weblining: companies are using your personal data to limit your choices—and force you to pay more for products. *BusinessWeek*. Retrieved from http://www.businessweek.com/2000/00_14/b3675027.htm

Technology and Privacy Advisory Committee (TAPAC). (2004). Safeguarding privacy in the fight against terrorism [Report for the Department of Defense]. Retrieved from http://epic.org/privacy/profiling/tia/tapac_report.pdf

Tien, L. (2003, January 26). Total Information Awareness: taking the fiction out of science fiction. *Freelance Star*. Retrieved from http://w2.eff.org/Privacy/TIA/tien-oped.php

Venkatraman, S., Bala, H., Venkatesh, V. & Bates, J. (2008). "Six strategies for electronic medical records systems." *Communications of the ACM, 51*(11), 140-144.