Out of the Filing Cabinet and into the Fire

How the Shift from Paper to Electronic Health Records Has Endangered Patient Privacy and Security and How to Calm the Flame

No. 110
January
2014

A Pioneer Institute White Paper

by Christina England and Josh Archambault

PIONEER INSTITUTE
PUBLIC POLICY RESEARCH

Pioneer's Mission

Pioneer Institute is an independent, non-partisan, privately funded research organization that seeks to improve the quality of life in Massachusetts through civic discourse and intellectually rigorous, data-driven public policy solutions based on free market principles, individual liberty and responsibility, and the ideal of effective, limited and accountable government.

Pioneer's Centers

This paper is a publication of the Center for Health Care Reform, which is focused on Medicaid and Health Care budget busters, specifically the cost of Medicaid programs, and long-term care and insurance reforms, cost containment by providing ideas to help businesses, large and small, compete by reducing their health care costs, and tracking the progress of the landmark Massachusetts health care reform.

The Center for School Reform seeks to increase the education options available to parents and students, drive system-wide reform, and ensure accountability in public education. The Center's work builds on Pioneer's legacy as a recognized leader in the charter public school movement, and as a champion of greater academic rigor in Massachusetts' elementary and secondary schools. Current initiatives promote *choice and competition, school-based management, and enhanced academic performance in public schools.*

The Center for Better Government seeks limited, accountable government by promoting competitive delivery of public services, elimination of unnecessary regulation, and a focus on core government functions. Current initiatives promote *reform of how the state builds, manages, repairs and finances its transportation assets as well as public employee benefit reform.*

The Center for Economic Opportunity seeks to keep Massachusetts competitive by promoting a healthy business climate, transparent regulation, small business creation in urban areas and sound environmental and development policy. Current initiatives promote market reforms to *increase the supply of affordable housing*, *reduce the cost of doing business*, and *revitalize urban areas*.

Pioneer Institute is a tax-exempt 501(c)3 organization funded through the donations of individuals, foundations and businesses committed to the principles Pioneer espouses. To ensure its independence, Pioneer does not accept government grants.

Out of the Filing Cabinet and into the Fire

How the Shift from Paper to Electronic Health Records Has Endangered Patient Privacy and Security and How to Calm the Flame

Christina England

Josh Archambault

Contents

Introduction

While there have been unprecedented technological developments in the past two decades, it is only very recently that similar rates of development have occurred in health information technology (HIT). Technology is providing new and exciting health management tools to manage one's health. Online medical websites like WebMD find conditions matching one's symptoms, smartphone apps like Lose It! keep track of your diet and exercise, and electronic health record (EHR) management systems allow patients to view lab test results online. In a 2012 survey, the Pew Research Center found that 72% of internet users looked online for health information.[1] One in three cell phone users have utilized their phone to find health information online. In 2009, 48% of physicians had adopted an EHR system.[2] By 2012, that number rose to 72% of office-based physicians using a health record system that was either partially or fully electronic.[3]

Despite the dramatic growth in the use of EHRs, few individuals have a clear understanding of what they are and why doctors are using them. EHRs refer to a technological system that enables providers to store and share private medical information. The stated goals of EHRs include reducing medical errors, promoting efficiency, and saving money. According to the Council of Economic Advisors, health care expenditures in the United States are about 18% of GDP—a number expected to rise sharply to 34% by 2040 if health care costs continue to grow at their current rates.[4]

Many private industries and the state and federal government have promoted EHR systems, with Massachusetts being particularly active in its use of EHRs. However, despite the growth in EHR use, privacy and security issues are rarely discussed. Massachusetts legislation, including Chapter 35 of the Acts of 2013 and Chapter 224 of the Acts of 2012, highlight the active nature of state government on EHRs. The Legislature has set up a statewide records exchange (Mass HIway) and gone as far as to mandate knowledge for the use of EHRs as a condition of licensure for all doctors in the state in two years.

This paper will discuss the importance of secure medical records in health information exchanges (HIEs), the general history of EHRs in the US and in Massachusetts particularly, the history of privacy rights in the medical field, and finally efforts being taken to ensure more protected and private EHRs. To be clear, this paper will not be evaluating the validity of claims of EHRs saving the state money or their impact on coordination of care, but instead will focus solely on the security and privacy concerns of the state's mandated EHR use.

Dangers of Insecure Medical Information within HIEs

In April 2013, six U.S. senators released a report titled *REBOOT: Reexamining the Strategies Needed to Successfully Adopt Health IT* calling for the federal push for HIT adoption to be reexamined. The report received bipartisan praise.[5] One key implementation deficiency identified in the report is the risk to patient privacy. The report also highlighted how the non-partisan Inspector General of the U.S. Department of Health and Human Services (HHS) recently shared the concern that, "the security policies and procedures at the Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health

Information Technology—two federal entities which oversee the administration of the health IT program—are lax and may jeopardize sensitive patient data."[6]

EHRs contain much more than simply "medical" data—they are a potential treasure trove for identify thieves. Demographic and identity information such as social security numbers, dates of birth, addresses, and phone numbers are all contained in EHRs. Equally attractive is financial information, like the patient's medical account and credit card information.

Another kind of thievery involves medical identity theft for the purpose of using someone else's insurance and filing false medical claims.[7] Beneficiaries have been wrongly labeled as diabetic or HIV-positive when people with those conditions obtained services using the beneficiary's medical identity.[8] Suppliers have refused to furnish wheelchairs when records have incorrectly shown that an individual recently received the items.[9] Prescriptions have been denied when pharmacy records show that a prescription was recently filled when in reality it was not.[10] Since criminals can use prescription data to order medication, or reroute ordered prescriptions, and then sell the medicine online, pharmaceutical data has been growing in demand. Physician data can be used to write fake prescriptions as well.

For cybercriminals, the value of personal data is much higher than a credit card or bank account number. When a single credit card is sold on the black market with a full identify profile found in health care records, the value can be up to 20 times more.[11] Harvard fraud expert Malcolm Sparrow has noted in his well-researched book *License to Steal: How Fraud Bleeds America's Health Care System*, "nothing within the routine operations of the payment systems checks that the patient was sick; or that the patient received treatment; or that the patient has ever heard of the provider in question."[12] Unlike credit card fraud, most patients never know that their identities were stolen for health care fraud.

In 2009, nearly one of every six data breaches was targeted at the health care industry, according to the Open Security Foundation.[13] That number is expected to grow. According to a RAND report, the government may lose up to $98 billion annually to Medicare and Medicaid fraud and abuse, with a significant portion of that related to the theft of personal information from federal databases[14]—redacting their 2005 study claiming that the adoption of electronic medical records could save at least $80 billion.[15] With waste, fraud, and abuse within the health care industry already being a significant problem, EHRs may make such activity even more ubiquitous.

As of June 2013, the Office for Civil Rights under HHS had received more than 77,000 complaints regarding breaches of health information privacy and completed more than 27,000 investigations of those breaches.[16] For example, in October 2011, the Department of Defense announced that backup tapes had been stolen from TRICARE, compromising the medical records of 4.9 million patients treated in military hospitals for the past 20 years.[17] In April 2012, the Utah Department of Health disclosed a breach of its computer servers, resulting in the theft of personal information of 800,000 individuals.[18] In August 2012, hacks accessed medical records of a small practice in Illinois, encrypted them, and demanded a ransom payment to unlock the files.[19] Security breaches are also seen in

unauthorized access to patient information, as well as data loss or destruction. Laptop thefts, hard drive thefts, and loss of portable electronic devices are all ways of jeopardizing the security of EHRs.

Security Failures Beyond Theft

There is even a growing view that de-identification mechanisms used to secure medical data have failed. In other words, medical data that is supposedly anonymous can be re-identified with relative ease, casting doubt on the ability to protect the information from privacy invasions. Researchers like Latanya Sweeney at the Harvard Data Privacy Lab have found methods of reporting the number of people who can be re-identified from person-specific, de-identified data.[20] Dr. Sweeney found that 87% of the US population can be uniquely identified by date of birth, gender, and ZIP code. Her contributions have expanded to include experiments on the identifiability of de-identified pharmacy data, DNA, public health registries, and more. In a 2009 experiment, Dr. Sweeney was able to take an anonymized medical record released to the public and link one of the identities to William Weld, former governor of Massachusetts throughout the 1990s.[21]

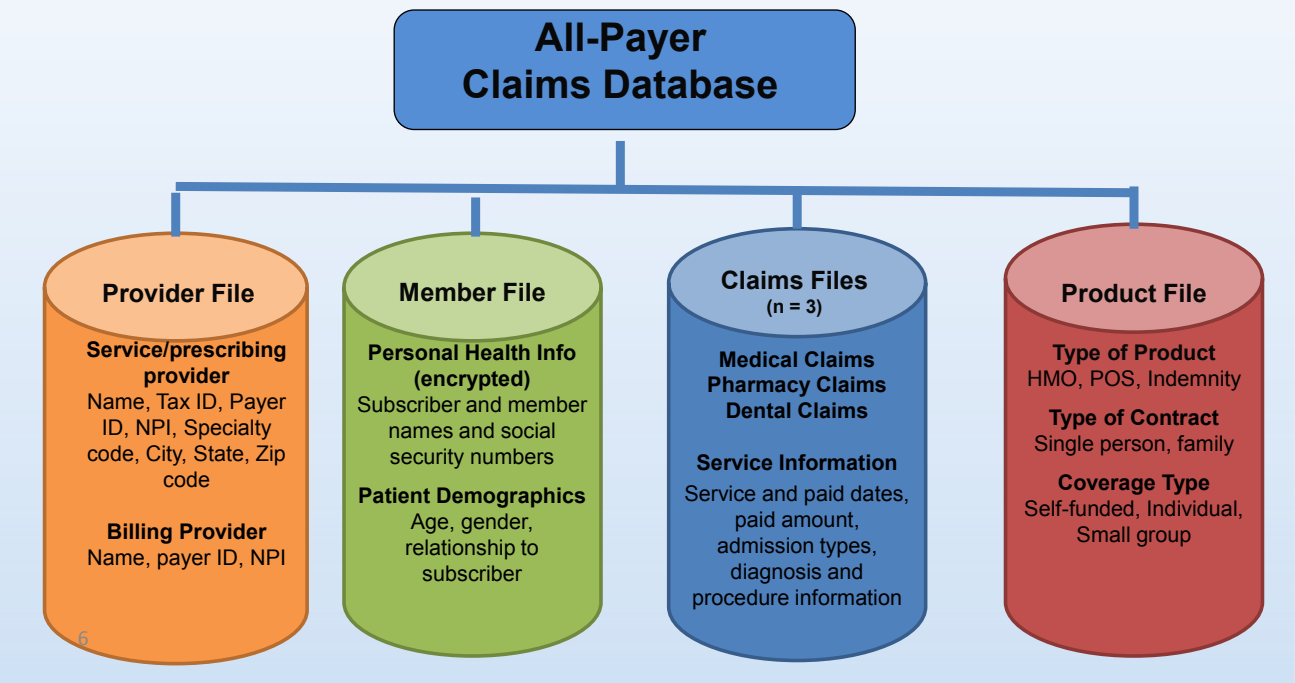
Data contained in EHRs has not only been stolen, but it has also been sold by individuals having lawful access to medical records. Despite the attempts that HIPAA, HITECH, and Massachusetts legislation make to protect the privacy of patients, public health agencies are exempt.[22] In 2011 alone, 12 of the nation's most populous states generated $1.9 million from 1,698 requests for medical data.[23] Washington sold its database 95 times that year and generated $15,950.[24] State public health agencies aggregate medical data using discharge details and claims processing post-adjudication, and since some state agencies are not "covered entities" regulated under HIPAA, their data can be sold like any other commodity to entities interested in the information.

The All-Payers Claims Database (APCD) in Massachusetts that contains medical claims, dental claims, pharmacy claims, and information from member eligibility files, provider files, and product files is one such state agency that has sold its data.[25] By this information being easily available, including one's history of psychological counseling, gynecological counseling, drug treatments, and more, people can be denied certain jobs, pay more for insurance, and suffer personal embarrassment if the data is misused. The following Figure 1 shows all of the information that is contained in the APCD in Massachusetts. While Data Use Agreements with the APCD must included minimum data necessary for the study, physical security of the data files, and prohibition against re-identification, and the security of the APCD will be an ongoing concern.[26] Furthermore, a member of the APCD council noted that HIPAA only "typically" applies to the release of information from the database, and only some of the release data is manipulated to comply with HIPAA.[27]

National EHR History

The Obama administration was not the first to push for national use of EHRs. Former President George W. Bush announced a proposal for the implementation of HIT in 2004, which included the goal of the majority of Americans having EHRs by 2014.[28] In 2009, during a speech at George Mason University, President Obama confirmed that his administration planned to continue

Figure 1: All-Payer Claims Database



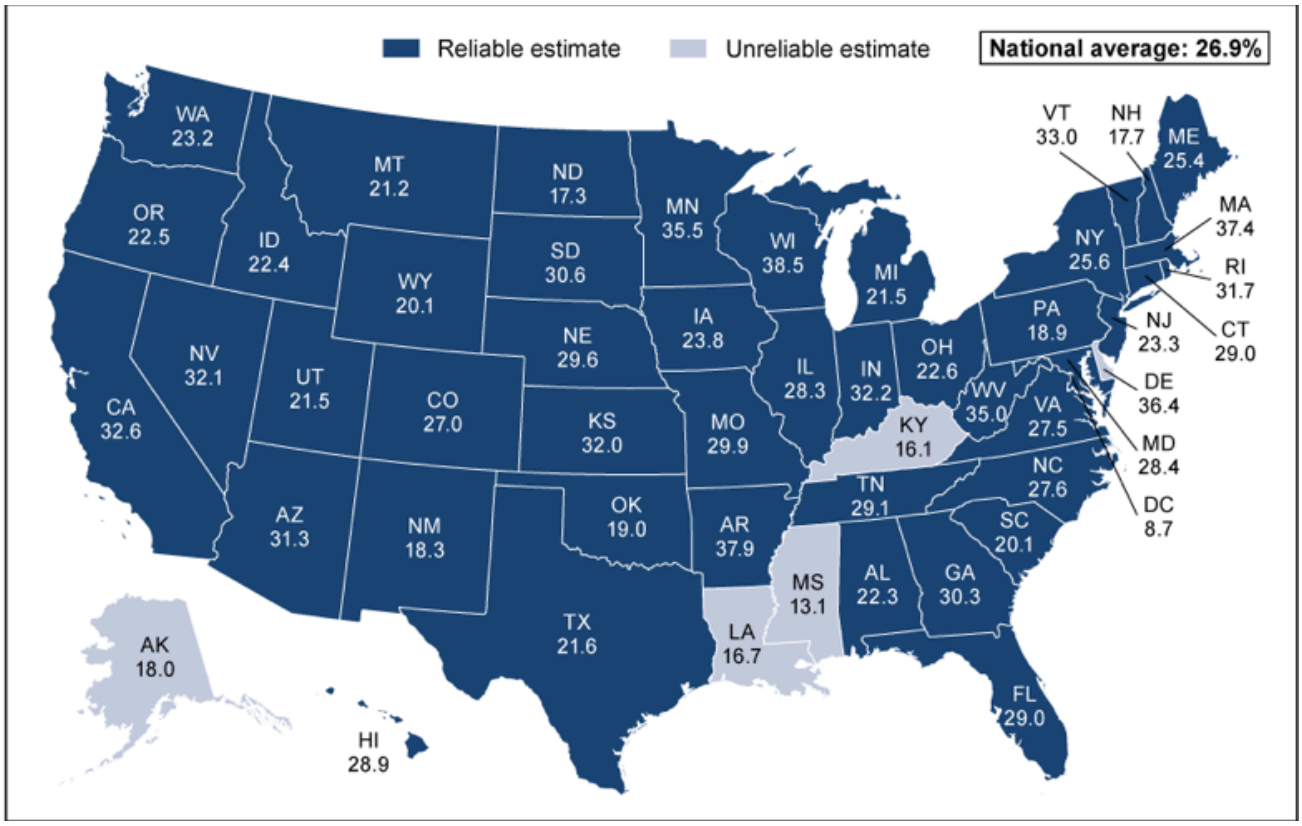
Slide taken from the presentation "Overview: All-Payer Claims Database" by the Center for Health Information and Analysis (http://www.mass.gov/chia/docs/p/apcd/apcd-overview-updated-2013-04-11.pdf)

pushing for that deadline.[29] The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009, provides $19 billion in federal grant money to promote the adoption and "meaningful use" (MU) of HIT.[30] The requirements for Stage 1 (of 3) MU of EHR include 15 core objectives for eligible professionals and 14 core objectives for hospitals.[31] Some of these objectives include computerized provider order entry, electronic prescribing, drug-drug and drug-allergy interaction checks, maintaining an up-to-date problem list, and implementing one clinical decision support rule (such as being able to report all patients due for a particular intervention, like a mammogram).[32]

HITECH also established 62 Regional Extension Centers (RECs) tasked to encourage EHR implementation through the provision of federal grants. Since 2010, the proportion of hospitals having a basic EHR system with met MU objectives has tripled, reaching a national average of 27% by 2012.[33] The following Figure 2 shows a map of the United States labeled with each state's *intended* EHR adoption percentage in 2012, with Massachusetts being the second highest in the nation (after Arkansas).[34]

The vast amounts of money being put on the table by the federal government to encourage the adoption of EHRs has raised legitimate questions about the long-term sustainability of EHRs when providers must sustain the investment to maintain and update systems. Time will tell how many providers can afford future commitments without public assistance.

Figure 2: Map of Estimated EHR Adoption Rates



SOURCE: CDC/NCHS, National Ambulatory Medical Care Survey, 2012.

Massachusetts EHR History

Massachusetts has independently been very active in their EHR implementation strategy. The Commonwealth's designated entity responsible for the adoption of EHRs in all health care provider settings, networked through a statewide HIE, is the Massachusetts eHealth Institute (MeHI).[35] To support Massachusetts providers in their adoption of EHRs, MeHI receives federal grants through the Regional Extension Center program. As of 2013, Massachusetts is ranked #3 in the nation for its incentive payments to eligible professionals and hospitals who adopt Stage 1 EHR systems. Roughly 6,000 providers and hospitals have applied for the monetary incentives for the adoption of EHRs, respectively resulting in $101 million and $72 million being paid.[36] Under Chapter 224 of the Acts of 2012, Massachusetts has also established the Health Policy Commission (HPC), charged with administering the Distressed Hospital Fund that gives grants to poor community hospitals.[37] Part of the $135 million expected to be collected over the next four years by the HPC to be given out of the fund will be used to help those hospitals implement EHR systems.[38]

While 93% of Massachusetts providers use an EHR system, only 38% of providers have achieved Stage 1 MU.[39] Although states have latitude to accept or change the MU guidelines, Massachusetts follows the objectives set on the federal level.[40]

Chapter 224 of the Acts of 2012 mandated proficiency for all physicians in EHRs.

> "the board [of Registration in Medicine] shall require, as a standard of eligibility for [medical] licensure, that applicants demonstrate proficiency in the use of computerized physician order entry, e-prescribing, electronic health records and other forms of health information technology, as determined by the board. As used in this section, proficiency, at a minimum shall mean that applicants demonstrate the skills to comply with the 'meaningful use' requirements."[41]

Thus, if the current 62% of Massachusetts physicians who do not utilize a federally certified EHR that meets MU requirements continue to not meet that standard, they would be denied a license to practice medicine in 2015.[42] This has been a huge unintended consequence of the Chapter 224 law.

Massachusetts eHealth Institute

MeHI was originally established in Chapter 305 of the Acts of 2008, which outlines the following MeHI obligations:

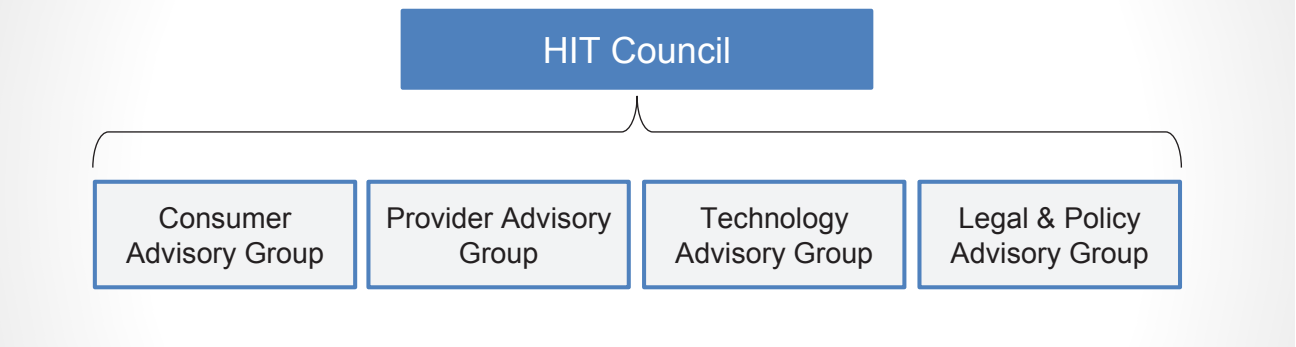
1) allow seamless, secure electronic exchange of health information among health care providers, health plans and other authorized users;
2) provide consumers with secure, electronic access to their own health information;
3) meet all applicable federal and state privacy and security requirements, including requirements imposed by 45 C.F.R. §§160, 162 and 164;
4) meet standards for interoperability adopted by the institute with the approval of the council;
5) give patients the option of allowing only designated health care providers to disseminate their individually identifiable information;
6) provide public health reporting capability as required under state law; and
7) allow reporting of health information other than identifiable patient health information for purposes of such activities as the secretary of health and human services may from time to time consider necessary.[43]

Per Chapter 224, the MeHI also has a council housed within the Executive Office of Health and Human Services (EOHHS) tasked with "coordinating with state agencies, including the commission, other governmental entities, and private stakeholders to develop a statewide health information exchange."[44] Consisting of 21 members, 14 appointed by the Governor and 7 designated by position, the council is chaired by the Secretary of Health and Human Services.[45]

Chapter 224 gives the Secretary extraordinary power to determine the kind of information that can be transferred in the health information exchange (HIE), since the plan for the statewide EHR system "allows reporting of health information other than identifiable patient health information for purposes of such activities as the secretary of health and human services may consider necessary."[46] Under the HIT council is four groups, as seen in the following Figure 3: the consumer advisory group, provider advisory group, technology advisory group, and the legal and policy advisory group.[47]

The Massachusetts Health Information Highway (Mass HIway) is the title for the statewide HIE established by the collaborative efforts of the EOHHS and

Figure 3: Composition of Massachusetts HIT Council

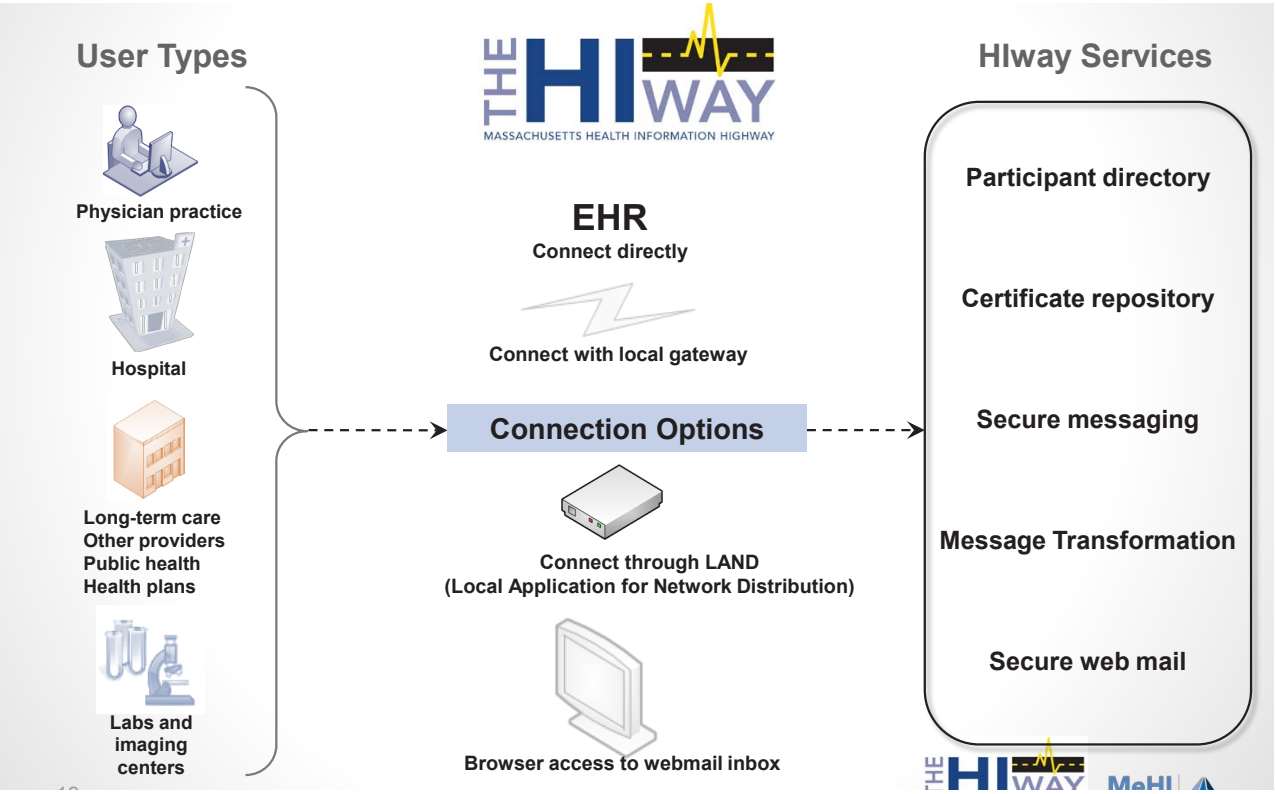


Slide taken from the presentation "The Mass HIway: Overview of the State-wide Health Information Exchange" by the Massachusetts eHealth Institute (http://mehi.masstech.org/sites/mehi/files/documents/MassHIway-Overview.pdf).

MeHI.[48] As of October 16, 2012, designated the "Golden Spike Day," Mass HIway opened to all interested organizations within the health care community. The following Figure 4 shows a map of how Mass HIway connects various users to a variety of different services. Because it is yet to be seen how the Mass HIway will react against a data breach, the privacy and security protocols used in the system should be consistently held under scrutiny.

Chapter 224 also assessed a tax on particular hospitals to fund the CHART (Community

Figure 4: Overview of Mass HIway Users and Services



Slide taken from the presentation "The Mass HIway: Overview of the State-wide Health Information Exchange" by the Massachusetts eHealth Institute (http://mehi.masstech.org/sites/mehi/files/documents/MassHIway-Overview.pdf).

Hospital Acceleration, Revitalization, Transformation) grant program. The Health Policy Commission, created under Chapter 224, will administer those grants to hospitals to help them transition over to EHRs among a few other policy changes.

History of Privacy Rights in the Medical Field

As the sharing of sensitive medical information through HIEs becomes more extensive, it is essential that legislation guarding the security and privacy of those medical records be followed. The primary law that establishes the US legal framework for health information privacy is the Health Insurance Portability and Accountability Act (HIPAA) of 1996.[49] Initially, HIPAA only applied to medical records maintained by health care providers and health plans, thus putting the abundance of health information outside of health care facilities beyond HIPAA's reach.[50]

HITECH amended HIPAA in 2009 to include security and privacy standards for EHR systems, such as requiring access control to see the medical information. Additionally, HITECH mandated the public notification by the EHR providers when there is any breach of unsecured protected health information of over 500 victims.

The final additional regulation concerning health record privacy and security was the Omnibus Final Rule issued in January 2013. This rule modified HITECH by making business associates of covered entities directly liable for compliance with HIPAA requirements, expanding individuals' rights to copies of their own health information, and strengthening limitations on the use of health information for marketing and fundraising purposes without individual authorization.[51]

Currently, there is a cultural acceptance of medical records being in the hands of institutions—a default setting for who gets to see those records internally that has largely remained more or less unchallenged. However, security and privacy concerns escalate as more people within and beyond the medical world have access to the data. The more players involved in the EHR world, the greater the risk of data leak—either intentional or unintentional. Though an organization sharing data may have adequate security, the one receiving it may not. Because all the organizations in several layers of government are integrated in one system, with potentially thousands of individuals having access to the medical records, those vulnerabilities compound and can be exploited.[52]

Efforts to Make Medical Data More Secure and Private

Fortunately, there are methods being developed by both the private and public sectors that seek to take a more balanced approach, addressing security and privacy concerns while simultaneously allowing all the benefits of EHRs to be achieved.

Microsoft

Microsoft is one such private sector group that has developed a means by which patient privacy can be protected while still enabling EHRs to improve health care. They have termed their method Patient Controlled Encryption (PCE).[53] PCE is an encryption approach in which patients generate and store their own encryption keys to their medical records, which allows the records to be secured and private. For providers to access a patient's records, they must be authorized

by the patient to have the decryption key. While the research done at Microsoft is promising, there are still questions about whether PCE would enable the appropriate health care providers to view medical records at crucial times when patients are unable to give authorization.

athenahealth, Inc.

Another private EHR provider that has developed a new model for securely sharing medical information is athenahealth, Inc. Rather than using installed software, athenahealth uses a cloud-based model to store and exchange medical data.[54] When a health care provider uses an EHR system managed by athenahealth, the records do not reside on computers within the provider's office or hospital, but rather in a remote database accessible by the internet. In this kind of system, employees at athenahealth can monitor everything that is occuring across their network in real time, making it easier to catch unusual activity. Additionally, athenahealth has participated in private audit programs and designed its own code of conduct, agreeing to uphold high standards of patient safety and ethical use of HIT.[55] Using cloud-based computing for EHR systems appears to be a promising way to catch and address security threats and data breaches. Nonetheless, general concerns about cloud-based computing, including the danger of authorized users within the company stealing information, remain.[56]

The work being done by Microsoft and Athena highlight just two ways in which private companies are seeking to create more secure and private systems. However, it is not just the private sector that is trying to protect medical records; federal and state governments have also taken action to reduce EHR privacy concerns.

Department of Veterans Affairs

The Department of Veterans Affairs (VA) has been particularly active in integrating tough safeguards into its daily operations with HIT. The VA is responsible for the development and maintenance of the Veterans Health Information Systems and Technology Architecture (VistA), which is the department's EHR system.[57] After a May 2006 incident in which a laptop containing the personal information of millions of veterans was stolen from an employee's home, the VA attempted to establish better information security protection. For example, all VA laptops are now encrypted, and personal data does not flow outside the VA unless it is encrypted. Additionally, the VA reports any information protection incidents on a daily basis, with each incident being examined by an independent privacy breach analysis team to see how it can be prevented in the future.[58]

Another way in which the government is making HIEs more secure and private is by making them "opt-in" programs, where records can only be transmitted electronically over the exchange with patient consent. While a legislative opt-in clause would not prevent a patient's medical records from being transferred into electronic form and kept in a single hospital, it would prevent that medical record from being transferred between different hospitals, pharmacies, laboratories, and other MeHI participants. In Massachusetts, Chapter 224 outlines the following security and privacy requirements with which providers must comply for entrance into the Mass HIway, including the "opt-in" requirement listed first:

1) establish a mechanism to allow patients to opt-in to the health information exchange and to opt-out at any time;
2) maintain identifiable health information in physically and technologically secure environments by means including, but not limited to: prohibiting the storage or transfer of unencrypted and non-password protected identifiable health information on portable data storage devices; requiring data encryption; unique alpha-numerical identifiers and password protection; and other methods to prevent unauthorized access to identifiable health information;
3) provide patients the option of, upon request to a provider, obtaining a list of individuals and entities that have accessed their identifiable health information from that provider;
4) develop and distribute to authorized users of the health information exchange and to prospective exchange participants, written guidelines addressing privacy, confidentiality and security of health information and inform individuals: the information available through the exchange, who may access their information and the purposes for which their information may be accessed; and
5) ensure compliance with all state and federal privacy requirements, including those imposed by the Health Insurance Portability and Accountability Act of 1996, P.L.104-191, the American Recovery and Reinvestment Act of 2009, P.L. 111-5, 42 C.F.R. §§2.11 et seq. and 45 C.F.R.§§160, 162 and 164.[59]

Conclusion

Ensuring that sensitive medical information remains secure in health information exchanges is a daunting but essential task. There will always be a security risk associated with using an electronic network to transfer data; however, by limiting the number of individuals and agencies having access to the network, and giving patients more control over who sees their data, privacy rights can be better protected. While research has been done to find ways of making EHRs more secure, how successful the Mass HIway and their partners will be in implementing best practices remains an open question.

There are several recommendations for policymakers (at least for those with access to high-speed internet) interested in achieving the benefits of EHRs without endangering patient privacy and security.

First, the EHR conversation must be patient-oriented. Personal medical information should be recognized as truly personal by government, with the choice of who has access to that information being in the hands of citizens themselves rather than having medical and federal institutions mandate access to information.

Second, Massachusetts should reconsider or delay the legal requirement for Massachusetts physicians to use a federally certified EHR that meets MU requirements as a condition of licensure. An overwhelming number of physicians will not meet this requirement, and thus by law will have their medical license revoked. Such action would be highly concerning for the future of medical care in the state.

Third, as public dollars dry up for EHR adoption, policymakers and the private

sector need to develop a realistic financial plan to keep EHR systems both viable and well protected. There needs to be assurance that Mass HIway will continue to uphold strict security standards even if MeHI faces budget cuts. One way to do this is by the MeHI's EHR providers abiding by the EHR Developer Code of Conduct written by the HIMSS Electronic Health Record Association, who represents more than 40 national EHR vendors such as athenahealth.[60] The June 2013 document outlines how those who subscribe to the code are "committed to developing and implementing our software, services, and business practices in ways that protect patients' privacy through the secure and trusted handling of personal health information."[61] Adherence to this code would help reassure citizens that that the state is handling their medical records appropriately, maximize the utility of EHRs in our health system, and reduce need for redundant future upgrades.

Finally, to increase the transparency regarding data breaches in the state's HIE, Massachusetts should consider a lower threshold for public notification when a breach has taken place. Currently, Massachusetts is legally obligated under HITECH to report breaches of unsecured medical records if over 500 individuals are affected. A lower number, such as 100 or even 25, should be used instead in a state of our size. In addition, the MeHI should encourage its members to implement the VA's daily reporting of information protection incidents, and appoint an independent panel or commission to review any breach and recommend methods to prevent similar problems in the future. This would hold health care and EHR providers more accountable for ensuring that medical records are secure.

Ultimately, the EHR privacy and security concerns need to be revisited regularly as technology advances and the number of medical data thefts, purchases, and security failures grows.

About the Authors:

Christina England is a graduate student at the University of Maryland, getting a Masters in Public Policy. She graduated from the United States Air Force Academy in 2012 with a BS in Biochemistry, and is now a second lieutenant in the Air Force.

Josh Archambault is a Senior Fellow at Pioneer Institute. Prior to joining Pioneer, Josh was selected as a Health Policy Fellow at the Heritage Foundation. Josh served as a Legislative Director in the State Senate and as Senior Legislative Aide in the Governor's Office of Legislative Affairs. Josh holds a Masters in Public Policy from Harvard University's Kennedy School and a BA in Political Studies and Economics from Gordon College.

About Pioneer:

Pioneer Institute is an independent, non-partisan, privately funded research organization that seeks to change the intellectual climate in the Commonwealth by supporting scholarship that challenges the "conventional wisdom" on Massachusetts public policy issues.

Recent Pioneer Publications

Have the MBTA's Retirement Plans Gone Off the Rails? White Paper, December 2013

The Logic of Pension Valuation: A Response to Robert Novy-Marx, White Paper, December 2013

The Cost of Cost-of-Living Adjustments in Massachusetts Public Retirement Systems, White Paper, October 2013

A First Step Toward Retiree Healthcare Reform, But Much More is Needed, Public Testimony, October 2013

School Vouchers in Washington, D.C.: Lessons for Massachusetts, White Paper, October 2013

Follow us on Twitter:
http://twitter.com/PioneerBoston

Find us on Facebook:
http://www.facebook.com/PioneerInstitute

Endnotes

1. Pew Research Center. "Pew Internet: Health." Last modified June 1, 2013. http://www.pewinternet.org/Commentary/2011/November/Pew-Internet-Health.aspx.
2. Centers for Disease Control and Prevention. "Physician Adoption of Electronic Health Record Systems." Last modified July 17, 2012. http://www.cdc.gov/nchs/data/databriefs/db98.htm.
3. Centers for Disease Control and Prevention. "Use and Characteristics of Electronic Health Record Systems Among Office-Based Physician Practices." Last modified December 6, 2012. http://www.cdc.gov/nchs/data/databriefs/db111.htm
4. Council of Economic Advisers. "The Economic Case for Health Care Reform." Executive Office of the President. June 2009. http://www.whitehouse.gov/administration/eop/cea/TheEconomicCaseforHealthCareReform
5. Carroll, Aaron. "Republican Senators Want Changes to Meaningful Use." *The Incidental Economist*, April 18, 2013. http://theincidentaleconomist.com/wordpress/republican-senators-want-changes-to-meaningful-use/.
6. "REBOOT: Re-examining the Strategies Needed to Successfully Adopt Health IT." United States Senate. http://www.thune.senate.gov/public/index.cfm/files/serve?File_id=0cf0490e-76af-4934-b534-83f5613c7370.
7. Conklin, Wm. "Information Security Foundations for the Interoperability of Electronic Health Records." *International Journal Biomedical Engineering and Technology Forthcoming* (2009). Accessed June 20, 2013. http://www.amcleod.com/mcleod11.pdf.
8. Taitsman, Julie. "Protecting Patient Privacy and Data Security." *The New England Journal of Medicine* 368 (2013): 977-979. Accessed 15 June, 2013. http://www.nejm.org/doi/full/10.1056/NEJMp1215258?af=R&rss=currentIssue.
9. Taitsman, Julie. "Protecting Patient Privacy and Data Security." *The New England Journal of Medicine* 368 (2013): 977-979. Accessed 15 June, 2013. http://www.nejm.org/doi/full/10.1056/NEJMp1215258?af=R&rss=currentIssue.
10. Struck, Kathleen. "Better Safeguards Urged for Medical Records." *MedPageToday*, February 28, 2013. http://www.medpagetoday.com/PracticeManagement/Medicolegal/37598.
11. "Cybercrime and the Health Care Industry." RSA Security LLC. Accessed 23 June, 2013. http://www.rsa.com/products/consumer/whitepapers/11030_CYBHC_WP_0710.pdf.
12. Sparrow, Malcolm, *License to Steal: How Fraud Bleeds America's Health Care System* (Colorado: Perseus Books Group, 2000), 40. Also, a personal interview of Mr. Sparrow was conducted.
13. "Cybercrime and the Health Care Industry." RSA Security LLC. Accessed 23 June, 2013. http://www.rsa.com/products/consumer/whitepapers/11030_CYBHC_WP_0710.pdf.
14. Konrad, Walecia. "As Medicare Fraud Evolves, Vigilance is Required." New York Times, September 11, 2012. http://www.nytimes.com/2012/09/12/business/retirementspecial/medicare-fraud-victimizes-patients-and-taxpayers.html?_r=2&.
15. Hillestad, Richard. "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs." *Health Affairs* 24 (2005): 1103-1117. Accessed July 5, 2013. http://www.eecs.harvard.edu/cs199r/readings/RAND_benefits.pdf.
16. Taitsman, Julie. "Protecting Patient Privacy and Data Security." *The New England Journal of Medicine* 368 (2013): 977-979. Accessed 15 June, 2013. http://www.nejm.org/doi/full/10.1056/NEJMp1215258?af=R&rss=currentIssue.

17. Radick, Robert. "EMRs: The New Health Care Fraud Frontier?" *Forbes*, December 4, 2012. http://www.forbes.com/sites/insider/2012/12/04/emrs-the-new-health-care-fraud-frontier/.

18. Ragan, Steve. "Breach at Utah Department of Health Worse Than Originally Thought." *SecurityWeek Network*, April 9, 2012. http://www.securityweek.com/breach-utah-department-health-worse-originally-thought.

19. Fox, Steve. "EHR Hackers Turn to Extortion." *HealthIT Law Blog*, August 23, 2012. http://www.healthitlawblog.com/2012/08/articles/ehr-hackers-turn-to-extortion/.

20. Sweeney, Latanya. "Policy and Law: Identifiability of de-identified data." Research Accomplishments of Latanya Sweeney, Ph.D. Accessed June 28, 2013. http://latanyasweeney.org/work/identifiability.html.

21. Schoen, Seth. "What Information is 'Personally Identifiable'?" *Electronic Frontier Foundation*, September 11, 2009. https://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable.

22. Robertson, Jordan. "States' Hospital Data for Sale Puts Privacy in Jeopardy." *Bloomberg*, June 5, 2013. http://www.bloomberg.com/news/2013-06-05/states-hospital-data-for-sale-puts-privacy-in-jeopardy.html.

23. Robertson, Jordan. "States' Hospital Data for Sale Puts Privacy in Jeopardy." *Bloomberg*, June 5, 2013. http://www.bloomberg.com/news/2013-06-05/states-hospital-data-for-sale-puts-privacy-in-jeopardy.html.

24. Robertson, Jordan. "States' Hospital Data for Sale Puts Privacy in Jeopardy." *Bloomberg*, June 5, 2013. http://www.bloomberg.com/news/2013-06-05/states-hospital-data-for-sale-puts-privacy-in-jeopardy.html.

25. Division of Health Care Finance and Policy. "All-Payer Claims Database: Overview of Efforts in Massachusetts." http://www.mass.gov/chia/docs/p/apcd/apcd-overview.pdf.

26. Center for Health Information and Analysis. "Overview of the All-Payer Claims Database." April 11, 2013. http://www.mass.gov/chia/docs/p/apcd/apcd-overview-updated-2013-04-11.pdf.

27. Center for Health Information and Analysis. "APCD Release 1.0 Appendices." June 2013. http://www.mass.gov/chia/docs/p/apcd/release1/apcd-restricted-release-document-appendices-june-2013.pdf.

28. Hiller, Janine. "Privacy and Security in the Implementation of Health Information Technology." *Boston University Journal of Science and Technology Law* 17 (2011): 1-39. Accessed July 10, 2013, http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume171/documents/Hiller_Web.pdf.

29. Jones, K.C. "Obama Wants E-Health Records in Five Years." *Information Week*, January 12, 2009. http://www.informationweek.com/healthcare/obama-wants-e-health-records-in-five-yea/212800199.

30. U.S. Department of Health and Human Services. "HITECH Act Enforcement Interim Final Rule." Accessed July 21, 2013. http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html.

31. Centers for Medicare and Medicaid Services. "Medicare and Medicaid EHR Incentive Program." Accessed July 4, 2013. https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/MU_Stage1_ReqOverview.pdf.

32. Centers for Medicare and Medicaid Services. "Medicare and Medicaid EHR Incentive Program." Accessed July 4, 2013. https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/MU_Stage1_ReqOverview.pdf.

33. Robert Wood Johnson Foundation. "Health Information Technology in the United States 2013." Last modified July 8, 2013. http://www.rwjf.org/en/research-publications/find-rwjf-research/2013/07/health-information-technology-in-the-united-states-2013.html.

34. Centers for Disease Control and Prevention. "Use and Characteristics of Electronic Health Record Systems Among Office-Based Physician Practices." Last modified December 6, 2012. http://www.cdc.gov/nchs/data/databriefs/db111.htm.

35. Executive Office of Health and Human Services. "Massachusetts eHealth Institute." Commonwealth of Massachusetts. http://www.mass.gov/eohhs/gov/newsroom/masshealth/providers/electronic-records/massachusetts-ehealth-institute-mehi.html.

36. Massachusetts eHealth Institute. "Medicaid EHR Incentive Payment." Massachusetts Technology Collaborative. Accessed July 15, 2013. http://mehi.masstech.org/what-we-do/medicaid-ehr-incentive-payment-program.

37. Health Care Policy Commission. "Overview of Chapter 224." Accessed August 2, 2013. http://www.mass.gov/anf/docs/hpc/hpc-presentation-11-16-12.pdf.

38. Gosline, Anna. "Summary of Chapter 224 of the Acts of 2012." *Blue Cross Blue Shield of Massachusetts Foundation*. September 1, 2012. http://bluecrossmafoundation.org/sites/default/files/download/publication/Chapter%20224%20summary_1.pdf.

39. Massachusetts eHealth Institute. "Electronic Health Record Adoption and Optimization." Massachusetts Technology Collaborative. Accessed July 15, 2013. http://mehi.masstech.org/health-it.

40. A personal interview was conducted with Mr. Brennan, Clinical Relationship Manager at the Massachusetts eHealth Institute. More information about the MeHI and the adoption of EHR with Meaningful Use requirements can be found here: http://www.mehi.masstech.org/meaningful-use-and-incentives.

41. "Session Laws: Chapter 224 of the Acts of 2012." The 188th General Court of the Commonwealth of Massachusetts. https://malegislature.gov/Laws/SessionLaws/Acts/2012/Chapter224.

42. Archambault, Josh. "60% of MA Docs Will Not Meet Ch224 Electronic Medical Record Mandate." Pioneer Institute of Public Policy Research. June 3, 2013. http://pioneerinstitute.org/healthcare/60-of-ma-docs-will-not-meet-ch224-electronic-medical-record-mandate/.

43. "Session Laws: Chapter 305 of the Acts of 2008." The 188th General Court of the Commonwealth of Massachusetts. https://malegislature.gov/Laws/SessionLaws/Acts/2008/Chapter305.

44. "Session Laws: Chapter 305 of the Acts of 2008." The 188th General Court of the Commonwealth of Massachusetts. https://malegislature.gov/Laws/SessionLaws/Acts/2008/Chapter305.

45. Complete list of council members can be found in the January 2013 HIT Council meeting minutes: http://www.mass.gov/eohhs/docs/eohhs/masshiway/20130114-presentation.pdf.

46. "Session Laws: Chapter 224 of the Acts of 2012." The 188th General Court of the Commonwealth of Massachusetts. https://malegislature.gov/Laws/SessionLaws/Acts/2012/Chapter224

47. The Mass HIway. "Overview of the Statewide Health Information Exchange." Massachusetts eHealth Institute. http://mehi.masstech.org/sites/mehi/files/documents/MassHIway-Overview.pdf.

48. Massachusetts eHealth Institue. "Mass HIway." Massachusetts Technology Collaborative. Accessed July 15, 2013. http://mehi.masstech.org/health-information-exchange-0/mass-hiway.

49. Hiller, Janine. "Privacy and Security in the Implementation of Health Information Technology." *Boston University Journal of Science and Technology Law* 17 (2011): 1-39. Accessed July 10, 2013. http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume171/documents/Hiller_WWe.pdf.

50. Privacy Rights Clearinghouse. "Medical Records Privacy." Last modified April 2013. https://www.privacyrights.org/fs/fs8-med.htm#EHR.

51. Leyva, Carols. "HIPAA Omnibus Rule Summary." HIPAA Survival Guide. February 3, 2013. http://www.hipaasurvivalguide.com/hipaa-omnibus-rule.php.

52. Conklin, Wm. "Information Security Foundations for the Interoperability of Electronic Health Records." *International Journal Biomedical Engineering and Technology Forthcoming* (2009). Accessed June 20, 2013. http://www.amcleod.com/mcleod11.pdf.

53. A personal interview was conducted with Ms. Lauter at the Microsoft Research lab. A paper published talking about the technical details of the PCE system can be found here: http://research.microsoft.com/pubs/102475/pce-ccsw.pdf.

54. A personal interview was conducted with Ms. Stephanie Zaremba, Sr. Manager of Government and Regulatory Affairs at athenahealth. More information on athenahealth can be found here: http://www.athenahealth.com/.

55. Athenahealth. "Is Your Code of Conduct Good Enough to Fix Healthcare?" Accessed July 25, 2013. http://www.athenahealth.com/codeofconduct/.

56. Kimery, Anthony. "DHS Awards $95 Million BPA for First Cloud-Based Federal Enterprise Talent Management System." *HSToday*. August 16, 2013. http://www.hstoday.us/single-article/dhs-awards-95-million-bpa-for-first-cloud-based-federal-enterprise-talent-management-system/926871d779fc02a92923a24cb6de1fd1.html.

57. Maduro, Roger. "VistA as an EHR System Core for DoD." *OpenHealthNews*. March 1, 2013. http://www.openhealthnews.com/articles/2013/vista-ehr-system-core-dod.

58. Mosquera, Mary. "6 Lasting Effects of 2006 VA Data Breach on Privacy, Security." *GovernmentHealthIT*. May 24, 2012. http://www.govhealthit.com/news/6-lasting-effects-2006-va-data-breach-privacy-security.

59. "Session Laws: Chapter 224 of the Acts of 2012." The 188th General Court of the Commonwealth of Massachusetts. https://malegislature.gov/Laws/SessionLaws/Acts/2012/Chapter224.

60. iHealthBeat. "HIMSS EHR Association Unveils Developer Code of Conduct." *California Health Care Foundation*. June 11, 2013. http://www.ihealthbeat.org/articles/2013/6/11/himss-ehr-association-unveils-developer-code-of-conduct.

61. "EHR Developer Code of Conduct." EHRA. June 11, 2013. http://www.himssehra.org/docs/EHR%20Developer%20Code%20of%20Conduct%20Final.pdf.

185 Devonshire Street, Suite 1101, Boston, MA 02110 Telephone: 617.723.2277 www.pioneerinstitute.org