University of Nebraska - Lincoln

DigitalCommons@University of Nebraska - Lincoln

2008

Electronic Medical Records in Nebraska Security, Privacy, and Health Care Quality

"Electronic Medical Records in Nebraska Security, Privacy, and Health Care Quality" (2008). *Publications of the University of Nebraska Public Policy Center*. 108.
https://digitalcommons.unl.edu/publicpolicypublications/108

Electronic Medical Records in Nebraska
Security, Privacy, and Health Care Quality

This is a background document to prepare you for the November 17th discussion about electronic health records. This discussion guide is intended to serve as a jumping-off point for our upcoming conversation. The discussion is not a test of facts, but rather a chance to offer your perspectives on the issues with other Lincoln residents.

Electronic Medical Records: Where Are We Now?

On April 26, 2004, President Bush urged the country to pursue new initiatives in education, energy, and technology. Particular focus was placed on new developments in Health Information Technology (HIT)—and more specifically—Electronic Medical Records (EMRs): "Within ten years, every American must have a personal electronic medical record," asserted the President.[1]

The promise of digitizing personal medical information may have many benefits: increasing efficiency in our nation's sprawling health care system, decreasing medical errors caused by a lack of information about patients, decreasing unnecessary tests and examinations, and increasing overall quality of care.[2] "Paper kills," warned former House Speaker Newt Gingrich, in reference to the thousands of Hurricane Katrina survivors who were plagued by the destruction of their paper medical records after the flood.[3] The Katrina disaster is but one example some point to which supports the need for electronic medical records. In more normal day-to-day use, many physicians support the use of EMRs. In a nationwide survey conducted in 2008, some 82% of doctors reported that EMRs improve the quality of medical decisions, and 86% said they help prevent errors.[4]

Nearly five years after President Bush's declaration that every American have a personal EMR by 2014, where do we stand now? Nationally, it is estimated that less than a quarter of doctors' offices use EMRs.[5] The vast majority of doctors in small, private practices—with whom most Americans interact with for health care needs—still rely on paper records and files. Only 9% of practices with less than three doctors are estimated to use EMRs.[6] The barriers to expanding the use of EMRs are many. There are significant costs for installing new technology and software.[7] There are different and competing forms of technological standards for EMRs. There are many state and federal policies that must be successfully navigated. And finally, there are concerns about individual privacy and confidentiality.

---

[1] President George W. Bush, *President Unveils Tech Initiatives for Energy, Health Care, Internet: Remarks by the President at American Association of Community Colleges Annual Convention, Minneapolis Convention Center*, April 26, 2004, *available at* http://www.whitehouse.gov/news/releases/2004/04/20040426-6.html.

[2] F. Michael Gloth et al., *Using Electronic Health Records to Improve Care: Will "High Tech" Allow a Return to "High Touch" Medicine?* Journal of the American Medical Directors Association, Vol. 6, July/August 2005.

[3] The Economist, *From clipboards to keyboards; Health care*, May 19, 2007 (U.S. Edition).

[4] Steve Lohr, *Most Doctors Aren't Using Electronic Health Records*, The New York Times, June 19, 2008, *available at* http://www.nytimes.com/2008/06/19/technology/19patient.html?_r=1&partner=rssuserland&emc=rss&pagewanted=all &oref=slogin.

[5] Marianne Kolbasuk McGee, *Urgent Care: The Health Care Industry is Making Painfully Slow Progress Ditching Paper for Electronic Health Records: Time to Pick Up the Pace*, Information Week, May 28, 2007, page 40.

[6] Steve Lohr, *Most Doctors Aren't Using Electronic Health Records*, The New York Times, June 19, 2008, *available at* http://www.nytimes.com/2008/06/19/technology/19patient.html?_r=1&partner=rssuserland&emc=rss&pagewanted=all &oref=slogin.

[7] *Id*.

Nebraska's Adoption of Health Information Technology

In Nebraska, a 2007 survey of all licensed physicians in the state conducted by the Nebraska Medical Association and Creighton University found that 23% of respondents had fully implemented electronic medical records in their practices. Thirteen percent were in the process of doing so, 35% were planning on doing so within the next few years, and 42% of responding physicians had no plans to implement EMRs.[8] Among doctors who had not yet moved to using EMRs, 77% had not done so due to the high financial costs of transitioning to EMRs. The lack of single standards in health exchange information was another large obstacle (59%).[9]

Like many other states, in Nebraska there are partnerships that are planning to implement "health information exchanges." Although all but one of these partnerships are not operating currently, in the future, they would all be able to electronically exchange medical information within their defined regions to improve health care. These partnerships include:

The Nebraska Health Information Initiative: A statewide partnership between public and private hospitals and clinics across Nebraska, Blue Cross and Blue Shield of Nebraska, and other health care entities.

The Western Nebraska Health Information Exchange: A partnership between all the hospitals in Western Nebraska, the Panhandle Public Health District, Region I Behavioral Health, and other health care entities.

The Southeast Nebraska Behavioral Health Information Network: A partnership between the Heartland Health Alliance, Blue Valley Mental Health Center, Region V Systems, BryanLGH Medical Center, Health Partners Initiative, and other entities to share behavioral health information in the Lincoln and southeast Nebraska area.

The Southeast Nebraska Health Information Exchange: A partnership between the Thayer County Health System and community partners including emergency medical services, the local pharmacy, and long-term health care facilities.

Security and Privacy

The sharing of Electronic Medical Records poses a number of complicated questions about security, privacy, and health care quality. Most people can agree that the use of EMRs can greatly benefit both patients and providers, but there have also been reservations. In a national survey conducted by the Employee Benefit Research Institute, most survey respondents believed it was extremely (27%) or very (33%) important for personal health information to be electronically stored. However, 62% of respondents were not confident that their electronic health records would remain confidential.[10]

---

[8] Kimberly Galt et al., *How Many Physicians Have Adopted Electronic Health Records in Nebraska? An Update on the Nebraska Medical Association Project*, June 27, 2007, *available at* http://chrp.creighton.edu/Documents/NMA_Publication_and_Report.pdf.
[9] EHRNebraska, Status of Health Information Technology in Nebraska: Focus on Electronic Health Records in Physician Offices, March 2008, page 20, *available at* http://chrp.creighton.edu/Documents/EHR_Report/Status_of_Health_Information_Technology_in_Nebraska_March_2008.pdf.
[10] Employee Benefit Research Institute, NOTES, October 2008, Vol. 29, No. 10, page 7, *available at* http://www.ebri.org/pdf/notespdf/EBRI_Notes_10-2008.pdf.

Public concern over privacy and security should be no surprise. Over the years, frequent news stories have appeared about mishandled or lost electronic data, internet hackers bypassing security measures to access confidential data, leaks of information to employers or the media, and other mistaken or intentional breaches of privacy. Examples include:

● In 1996, a Florida health worker stole electronic records listing 4,000 HIV-positive people, brought it to a bar, and offered to look up the names of friends.[11]

● In 1999, the City of New York planned to use personal Medicaid records to pressure welfare recipients into drug or alcohol treatment programs. The plan was later dropped after wide-scale protests.[12]

● In 2000, medical records of thousands of University of Michigan Medical Center patients were mistakenly placed on an unsecure website on the internet for two months.[13]

● In 2001, a pharmaceutical company mistakenly exposed the e-mail addresses of over 600 individuals with depression, bulimia, or obsessive-compulsive disorder, through an automated e-mail message.[14]

● In 2002, computers containing the names, contact information, and social security numbers of over 500,000 U.S. troops were stolen from a private, military health care contractor in Phoenix, AZ.[15]

● In 2008, unauthorized employees at the University of California, Los Angeles Medical Center were discovered to have looked at the medical records of Governor Arnold Schwarzenegger, First Lady Maria Shriver, Farah Fawcett, Britney Spears, and hundreds of other celebrities, politicians, and patients. Information about Farah Fawcett's treatment for cancer was subsequently leaked to tabloid newspapers.[16]

Clearly, these examples indicate that data theft, hacking, or other violations of security and privacy are real possibilities. Yet they are still isolated ones. Electronically stored data does offer security advantages over paper records. When managed properly, electronic data records can only be accessed by authorized personnel following stringent security measures, and that access can be logged and audited in a way that is not possible with paper records. On the contrary, with a little imagination and determination, anyone could access paper files locked in an office cabinet.

A federal law called the Health Information Portability and Accountability Act (HIPAA) provides broad security and privacy requirements for the management of people's health information. HIPAA allows for the sharing of necessary information between health care providers and other entities for treatment, payment, health care operations, and for other purposes permitted by law. [17]

---

[11] John Bacon, Nationline: *AIDS Confidentiality*, USA Today, October 10, 1996, page 3A.
[12] *Opinion: Misuse of Drug Treatment Records*, The New York Times, September 29, 1999, *available at* http://query.nytimes.com/gst/fullpage.html?res=9C05EFD81F3FF93BA1575AC0A96F958260.
[13] Julie Appleby, *File Safe? Health Records May Not Be Confidential*, USA Today, March 23, 2000, page 1A.
[14] Robert O'Harrow, Jr., *Prozac Maker Reveals Patient E-Mail Addresses*, The Washington Post, July 4, 2001, page E01.
[15] Adam Clymer, *Threats and Responses: Privacy; Officials Say Troops Risk Identity Theft After Burglary*, The New York Times, October 13, 2008, *available at* http://query.nytimes.com/gst/fullpage.html?sec=health&res=9804EFDB1731F931A25752C0A9659C8B63.
[16] Charles Ornstein & Dan Morain, *More UCLA Records Abuses*, Los Angeles Times, April 7, 2008, page A-1.
[17] Laura Dunlop, *Electronic Health Records, Interoperability Challenges Patients; Right to Privacy*, Shidler Journal of Law, Commerce & Technology, Spring, 2007.

Policymakers in Nebraska and other states are aware that the use and possible expansion of EMRs rests on concerns the public has about security and privacy. In 2006, Lieutenant Governor Rick Sheehy formed the Nebraska Health Information Security and Privacy Committee (HISPC). In its 2007 report to the State of Nebraska, HISPC recognized the need to engage and educate both health care professionals and ordinary consumers across the state about security and privacy issues, and examine existing laws and regulations that impede exchange of health data.[18]

Still, important questions remain for the public about EMRs, how they are used, and what policies should be enacted to address these evolving issues:

■ **Sensitive Medical Information:** How should electronic information about particularly sensitive medical conditions be handled? Who should have access to records documenting an individual's mental health history, HIV status, and drug or alcohol abuse treatment? How should consumers authorize release of such data? And in what circumstances is authorization not necessary?

■ **The Role of the Private Sector:** Private entities have recently unveiled online EMR projects such as Google Health and Microsoft Health Vault.[19] Placing EMRs online might be a way to get around problems associated with having multiple and competing EMR formats, but raise questions about security and vulnerability to internet outages. How should EMRs in the private sector be regulated?

■ **The Role of the Public Sector:** Government can obviously play a large role in regulation of EMR exchange. Should the government have a large role in oversight of EMR exchange, or a less intrusive one? To what extent should public tax dollars be used to fund expansion of EMR? To what extent should the government's public health infrastructure rely on EMRs?

Clearly, the trend towards digitizing personal health information will continue—a development that could have major implications for individual quality of life, and the nation's massive health care industry in general. What role should Nebraska play in these important developments?

~ ( ) ~

---

[18] Health Information Security and Privacy Committee State of Nebraska, *Security and Privacy Barriers to Health Information Interoperability, Final Report for the state of Nebraska,* June 2007.
[19] Andrew Smith, *Google, Microsoft Pushing for Electronic Medical Records*, The Dallas Morning News, June 17, 2008, *available at* http://www.dallasnews.com/sharedcontent/dws/bus/ptech/stories/061708dnbuswebhealth.3d a3ab5.html.