

[Politics Daily](#)

THE CRAM



[Katie Glueck](#)

[Contributor](#)

## Health Goes Digital: Balancing Privacy and Innovation of Electronic Medical Records



Joe Raedle, Getty Images

Relatively speaking, one of the [least controversial](#) aspects of the health care reform legislation signed by President Obama last week is the proposal for a national transition from paper to electronic medical records.

It's an initiative that [three in four Americans support](#), and the push for digitization has been a long time coming. In 2008, President-elect Obama [advocated](#) digitizing health records, saying, "We will make sure that every doctor's office and hospital in this country is using cutting edge technology and electronic medical records so that we can cut red tape, prevent medical mistakes, and help save billions of dollars each year."

Congress has been talking about electronic medical records since 1996, when members passed the Health Insurance Portability and Accountability Act (HIPAA), designed in part to ["set a national standard for electronic transfers of health data."](#) Last January, Obama [called for](#) electronic health records for all Americans by 2014, and the [stimulus bill](#) set aside \$36 billion for the initiative.

[Get the new PD toolbar!](#)

But some privacy and patients' rights advocates, like Deborah Peel of the organization Patient Privacy Rights, contend that if certain safeguards aren't implemented, digitizing medical records could pose a serious threat to patient privacy.

Writing in the [Wall Street Journal](#) last week, Peel cited a [Kaiser Family Foundation/Harvard School of Public Health/National Public Radio poll](#) from April 2009 which found that 59 percent of people were "not confident" that their "medical records would remain confidential if they were stored electronically and could be shared online." The poll went on to say that "an even larger percentage (76 percent)" think it's "at least somewhat likely that 'an unauthorized person' would get access to their records if they were placed online."

That's problematic, Peel said, because if patients don't trust the security of their medical records, they will be less likely to disclose what could be life-saving information to their doctors.

Dissemination of ostensibly private medical records, however, is nothing new. According to the nonprofit organization [Privacy Rights Clearinghouse](#), records are frequently shared with insurance companies, government agencies and employers, among other entities.

"Generally, access to your records is obtained when you agree to let others see them," the organization [reported](#). "In reality, you may have no choice but to agree to the sharing of your health information if you want to obtain care and qualify for insurance."

[HIPAA established a bare minimum for health record privacy standards](#) -- for example, you can now view your health records and find out who's accessed them for six years prior. But under HIPAA, "private" medical information can still be sent to pharmaceutical companies for marketing purposes, and if your medical information is going to be used for treatment, payment or health care operations, health care providers

don't need your consent to disclose that data.

"In many situations such as emergencies, this makes perfect sense," Privacy Rights Clearinghouse [reported](#). "You don't expect the ambulance driver to get your permission to call the hospital emergency room when you are having a heart attack. On the other hand, since your consent is not required for payment, your health care provider could submit a claim to your insurance company -- even for a procedure you wanted to keep private and intended to pay for yourself."

Then, as with anything online (from the presidential [Twitter account](#) on down), there's the risk of hackers . The non-profit Open Security Foundation [reported](#) that 12 percent of data breaches concern medical organizations (of the more than 260 million data breaches that have occurred since 2005). According to the research and consulting firm [Javelin Strategy & Research](#), more than 275,000 incidents of medical information theft occurred in the United States last year. That number -- a substantial increase from 2008 -- is [primarily attributable](#) to the expanding use of electronic medical records, said Javelin President James Van Dyke in an interview with the business and tech journal [InformationWeek](#).

"We think medical providers aren't up to the task. They won't have security best practices in place to match the incidents of fraud, and we think theft of personal health information is going to get worse," Van Dyke said.

But the Department of Health and Human Services has been looking for best practices since at least 2008, when the institution released a [brief](#) outlining their approach to privacy concerns associated with the process. "The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information" outlined eight guiding privacy principles. They ranged from ensuring individual access to one's medical records to imposing limits on the "type and amount of information collected, used and/or disclosed."

Last year, under the stimulus package, legislators took further steps to protect consumers. [According to the Electronic Privacy Information Center](#), a Washington watchdog organization, the Act cracked down on some medical information sharing practices that raised privacy concerns. Provisions included limiting the marketing of personal information, forbidding the unauthorized sale of medical records with some exceptions, and setting higher standards for using sensitive information.

Under the latest health care legislation, there will likely be additional privacy safeguards, said Jim Harper, the director of information policy studies at the libertarian Cato Institute in Washington. The question is whether those safeguards will serve the interests of the consumer.

"It's not going to be a free-for-all -- you'll likely see the government create rules," Harper said. "But the loopholes they put in will be ones that are convenient for the government. We already see some examples from HIPAA: The government determines that records

should be shared for research purposes. It often should be, but it's a separate question about whether the government should be allowed to take information for research if there aren't privacy protections for people who don't want to be involved in the research."

The [debate raged on](#) in the Wall Street Journal's editorial pages again this week, when health care industry leader Mary Grealley wrote that such privacy concerns are exaggerated and, in fact, dangerous.

"Medical research into lifesaving cures and treatments would be severely hindered by restricted access to health information," wrote Grealley, who is president of the Healthcare Leadership Council, a coalition of chief executives from the health care industry. "Stymieing the necessary transfer of data contained in one diagnosis, one prescription or one lab test could mean the difference between life and death. That is a very high price to pay in order to address overblown privacy concerns."

Furthermore, she argued, if patients did have a say in how their information was disclosed, it's unlikely that they would be knowledgeable enough to make those choices.

"Burdening patients with the responsibility of deciding what health information should be divulged and what should be shielded from medical professionals brings an infinite array of possible consequences," Grealley wrote. "Would the average patient know what information a surgeon needs in order to perform a complex procedure? It's highly doubtful."

From the government's standpoint, balancing patients' privacy concerns with productive medical research is tricky because health regulations are so complex, Harper said.

"There are lots of good reasons to use private health information, and it's really complicated to figure out in a single regulation what information should be used for what," he said. "So when government regulators write a regulation, they have to accommodate different interests and they write in a lot of exceptions. The problem is, consumers don't have a lot of say. A lot of people would share that information, but the individual doesn't have the opportunity to say, 'this is not for me.' "

Peel and her colleagues at Patient Privacy Rights are trying to change that. The organization [launched a petition](#) that asks Congress to pass a law called 'Do Not Disclose,' which they liken to a 'Do Not Call' list. "Instead of stopping marketing companies from calling you, it would stop companies and government from using your most sensitive personal information -- your health data -- without your permission," the organization's Web site states.

The first step in that initiative may be galvanizing the public around an issue that few know much about, Harper said.

"Consumers should be aware [of who sees their medical records]," he said. "But they're basically ignorant."

*Follow PoliticsDaily On [Facebook](#) and [Twitter](#),  
and download the new [Politics Daily toolbar](#)!*