www.freep.com

February 12, 2012

ID theft, mixed-up records consequences of growing problem of stolen medical information

By Robin Erb
Detroit Free Press Medical Writer

For every dollar a stolen Social Security number is worth, your stolen medical information -- a partial medical history, your insurance number -- is worth $50, according to some experts.

Yet at least 11 times since 2009, Michigan health care providers lost or otherwise accidentally breached the health data of more than 118,000 patients in all. A report released in December concluded that breaches nationally climbed 32% last year, in part, because doctors are more often relying on smartphones and other electronic devices to update files.

It's unclear whether any of the information in the 11 breaches was misused; it might simply have been discarded. But lost or stolen medical information also can be used to file fraudulent claims or cost you years in rebuilding your credit history or reclaiming your health insurance. And if your medical file ends up containing information that is not yours -- say an addict uses your information to get drugs -- that could mean life-threatening mix-ups if a doctor prescribes the wrong medicine or sees the wrong blood type.

The reasons for the Michigan breaches were human error rather than hacking: a lost laptop, misplaced jump drives.

Now, the head of the nation's effort to enforce health privacy laws says it's time to get tough.

Two years after the U.S. stepped up penalties for such breaches, Leon Rodriguez, head of the U.S. Health and Human Service's Office of Civil Rights, told the Free Press that it's time to crack down on security lapses: "Enforcement promotes compliance," he said.

Health info breaches put patients at risk as hospitals, doctors scramble for solutions

Walk into a doctor's office and chances are that some of your most private information -- from your Social Security number to the details of your last cervical exam and your family's cancer history -- is stored electronically.

Your doctor might access the information on a cell phone that could slip into the wrong hands. The staff might take it home on a laptop or a flash drive.

So as local health care providers take multimillion-dollar steps toward electronic records, they're talking about more than efficiency and better care. They're talking security, too.

"It's a great concern," said Dr. Matthew Zimmie, who is heading an $80-million conversion to electronic records at Oakwood Healthcare System. Part of the initiative is a five-person team and "that's all their job is -- to make sure this information is secure," he said.

Oakwood's security measures include passwords and security profiles -- allowing a radiology tech, for

example, to look only at information for radiology patients.

"We definitely take this seriously," Zimmie said.

They have to. According to a recent report by the Ponemon Institute, a Traverse City-based firm that conducts research about privacy and security:

• Data breaches nationally grew 32% last year, mostly because of employee negligence and lack of oversight.

• Nearly all of the 72 organizations surveyed reported at least one incident of lost or stolen information in the previous year.

• And although four out of five doctors use smartphones, more than half say they are not taking precautions to encrypt information.

• The top three causes for a data breach were lost or stolen computing devices, unintentional release of information by contractors and unintentional employee action, according to the report.

• More than half of the respondents reported they had little or no confidence that their organization would be able to detect all breaches.

"It's almost a matter of time before anyone can be a victim. The key is catching it early," said Dennis Doherty, an assistant prosecutor who handles fraud cases for Wayne County.

Among recent cases: a health care employee who stole information from cancer patients to apply for credit, he said.

"These ... people are dealing with enough, and now they have to deal with ID theft," he said.

A growing problem

Michigan has had at least 11 breaches of medical data since 2009 involving information for more than 500 people -- the threshold at which those incidents must be publicly reported. In all, the cases involved personal medical information for more than 118,000 people.

The largest involved Providence Hospital when an external hard drive used to back up data, including patient information, was reported missing at the Southfield hospital, according to a statement at the time.

The hard drive was never recovered, but the hospital received no reports that the data had been used inappropriately, spokesman Brian Taylor said Friday.

In fact, throughout the U.S., more than 390 such breaches involving the records of more than 19 million people have been reported since September 2009, when the new federal Health Information Technology for Economic and Clinical Health (HITECH) Act boosted penalties for providers whose data are stolen, lost or otherwise breached, according to the U.S. Department of Health and Human Services' Office of Civil Rights.

Thousands of smaller breaches occur annually.

"I think most consumers are still in the dark about this," said Deven McGraw, director of the Health Privacy Project at the Washington-based Center for Democracy & Technology.

Not Jane Doe.

That's the name used by a metro Detroit woman who filed a lawsuit last week after a transcription service for Henry Ford Health System inadvertently put her medical information on the Internet -- her name, medical record number and diagnosis of "cervical dysplasia secondary to HPV (human papillomavirus)," according to the suit.

Though it's the most common sexually transmitted infection, the woman told the Free Press she was "infuriated," worrying that someone might see it and "think I'm the kind of girl that I'm not."

Henry Ford, in a written statement Friday, said its contractor was responsible for the breach, and patients were notified immediately. The statement also apologized to affected patients.

Elizabeth Thomson, Jane Doe's Bloomfield Hills-based attorney, has filed the case as a class action. She said "people get worked up about their Social Security numbers, and understandably so." But in a day of Internet searches and social media, "you can do a lot of damage with a little bit of information, even without a Social Security number."

As in most states, those in Michigan responsible for failing to protect the information haven't been fined or otherwise penalized for the breaches.

But in at least three states, attorneys general have successfully filed actions in cases of large-scale breaches. In the first, then-Attorney General Richard Blumenthal in Connecticut settled for $250,000 a lawsuit against insurer HealthNet. The insurer was accused of losing a computer disk containing information for more than 1.5 million consumers. HealthNet also had to take measures to prevent further incidents under the 2010 settlement.

Vermont and Indiana also have fined or settled suits under the HITECH rules.

Crime goes unnoticed

It's unclear just how often medical information is misused; a person who steals an ID to get prescription drugs might slip through for years unnoticed. A stolen laptop with patient data might be reported to local police but never linked to fraudulent billing in another jurisdiction.

And the theft of medical information is often sifted into the larger category of ID theft -- patients' information stolen to apply for credit cards or stolen credit cards used to get medical services.

Frontline health care workers only recently have begun to understand the value of the information they handle, said Rick Kam, whose company, ID Experts, offers consulting in security. ID Experts financed the Ponemon report: "They're trained and focused on saving lives and health care," Kam said.

One of the simplest fixes is investing in devices that can be encrypted so that only authorized personnel can get to data, said Pam Dixon, founder of the California-based World Privacy Forum who has testified before Congress on the lack of security around people's most personal information.

Medical information, she said, is worth $50 on the street compared with $1 or $2 for a Social Security number. The banking industry has set up safeguards to detect ID theft and financial fraud so, for example, consumers get a call if there are unusual, out-of-country spending sprees. But there are few similar safeguards for medical ID theft, she said.

Perhaps worst of all, breaches of health information erode the public's trust in their doctors.

"If people lose trust in the health care system, they will not get the care they need," said Leon

Rodriguez, head of the HHS's Office of Civil Rights.

Rodriguez said his office has spent much of its time after the passage of the 2009 law pushing providers to shore up security.

"A lot of times you'll hear the covered entities a little overexcited about the cost of complying with the (privacy) rules," he said. But, he added, "when you look at where the breaches are or where the vulnerabilities are, they really are common sense."

Leaked information is unacceptable, he said. Doctors "should expect us to move to a much more enforcement approach," he said.

Henry Ford takes action

Information about patients of the Henry Ford Health System makes up three of Michigan's 11 data breaches involving more than 500 people. Others include two reports by the Detroit health department and one by Blue Cross Blue Shield of Michigan, which said the breach involved "nonmedical information" and occurred on the website of another insurer with whom it does business.

At Henry Ford, an employee's laptop was stolen from an unlocked office in 2010; last year, an employee lost a flash drive and a computer was stolen from a lab.

In each case, the information was just part of patient records -- outcomes of drug therapies, for example, that were being used for research -- and the data most likely was never the target, said Meredith Phillips, Henry Ford's chief privacy officer.

The health system launched iComply, instructing all employees to turn over their flash drives and personal storage devices. The information has been moved to special, encrypted flash drives purchased by Henry Ford. Employees using unauthorized devices can be fired. Smartphones will be encrypted beginning next month.

"If I lose it, if I drop it, if it falls, no one can actually penetrate the device at that point," Phillips said.

Contact Robin Erb: 313-222-2708 or rerb@freepress.com

More Details: What is HITECH?

The Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009 strengthened protection for personal health information:

• It provides $20 billion in funding to help local providers adopt electronic record-keeping. Providers who have not adopted such technology by 2015 will be penalized by a lowering of their Medicaid and Medicare reimbursements.

• It hands state attorneys general the authority to bring civil action on behalf of residents if their health information is inappropriately released or stolen.

• It boosts fines for those who fail to protect information to up to $1.5 million, depending on how egregious the breaches might be.

• It requires public reporting of breaches involving information for more than 500 people.