New data spill shows risk of online health records

August 21 2011, By JORDAN ROBERTSON , AP Technology Writer

Until recently, medical files belonging to nearly 300,000 Californians sat unsecured on the Internet for the entire world to see.

There were insurance forms, Social Security numbers and doctors' notes. Among the files were summaries that spelled out, in painstaking detail, a trucker's crushed fingers, a maintenance worker's broken ribs and one man's bout with sexual dysfunction.

At a time of mounting computer hacking threats, the incident offers an alarming glimpse at privacy risks as the nation moves steadily into an era in which every American's sensitive medical information will be digitized.

Electronic records can lower costs, cut bureaucracy and ultimately save lives. The government is offering bonuses to early adopters and threatening penalties and cuts in payments to medical providers who refuse to change.

But there are not-so-hidden costs with modernization.

"When things go wrong, they can really go wrong," says Beth Givens, director of the nonprofit Privacy Rights Clearinghouse, which tracks data breaches. "Even the most well-designed systems are not safe. ... This case is a good example of how the human element is the weakest link."

Southern California Medical-Legal Consultants, which represents doctors and hospitals seeking payment from patients receiving workers' compensation, put the records on a website that it believed only employees could use, owner Joel Hecht says.

The personal data was discovered by Aaron Titus, a researcher with Identity Finder who then alerted Hecht's firm and The Associated Press. He found it through Internet searches, a common tactic for finding private information posted on unsecured sites.

The data were "available to anyone in the world with half a brain and access to Google," Titus says.

Titus says Hecht's company failed to use two basic techniques that could have protected the data - requiring a password and instructing search engines not to index the pages. He called the breach "likely a case of felony stupidity."

One of the patients affected was Paul Thompson, who learned of the breach from Titus.

The Sugarloaf, Calif., electrician blew out his shoulder four years ago on a job wiring up a multiplex movie theater. His insurance company denied his claim, which led to a protracted dispute. He eventually settled.

Thompson says his injury has been a "long, painful road."

Unable to afford surgery in the U.S. to fix his torn rotator cuff, he paid a medical tourism company that was supposed to schedule a cheaper procedure in Costa Rica. The company went bankrupt, however, and Thompson said he lost nearly $7,300.

To have his personal information exposed on top of that was a final

indignity.

"I'm totally disgusted about everything," he said, calling the breach "another kick in the stomach."

Thomson is worried that hackers may have spotted his information online and tagged him for future financial scams. He contacted his bank and set up a fraud alert with the credit reporting agencies.

He says the prospect of all health records going electronic - which federal law mandates should happen by 2014 - "scares the living hell out of me."

When mistakes occur, the fallout can be more severe than the typical breach of email addresses or credit card numbers.

In the wrong hands, health records can be used for blackmail and public humiliation. The information can also be used by insurance companies to inflate rates, or by employers to deny job applicants.

Usually when personal data are exposed, it's the result of a network break-in by a hacker or a theft of computer equipment. Sometimes, it can be a simple case of someone mishandling the information.

Leaks are more likely the more data are passed around within the health industry's increasingly interconnected networks.

Dozens of companies can be authorized to handle a single person's medical records. The further away from the health care provider the records get, the flimsier the enforcement mechanisms for ensuring the data are protected.

That's exactly what happened at Hecht's company. "Our internal security

policies and procedures weren't followed," Hecht says. "When we were notified, we took immediate steps to remediate the situation and took long-term steps to make sure it never happened again."

The firm has since put the information behind a password, an approach that has its own security risks.

Hecht declined to go into further detail about how the information ended up online. He says many of the Social Security numbers and basic details about people's injuries were part of a database his firm compiled from information regularly sent by the state.

Patricia Ortiz, spokeswoman for the state Division of Workers' Compensation, says doctor's notes and other documentation in such cases are publicly available, but they have to be requested one by one.

The state stopped including Social Security numbers in those files in 2008; the exposed data came from older files.

Ortiz said that once workers' compensation information leaves the state's control, its security is the recipient's responsibility.

California, like most states, has a law requiring companies to notify consumers when their information has been breached. Hecht did not return calls from the AP seeking an update on how many patients had been notified.

Large-scale medical data breaches have been on the rise in recent years.

In one of the biggest, government health data was at risk in 2006 when a laptop with data on 26.5 million veterans was stolen from a government employee's home. The computer equipment was recovered, and the FBI said the sensitive files weren't accessed.

This year, hard drives containing health histories, financial information and Social Security numbers of 1.9 million Health Net insurance customers disappeared from an office. State regulators launched investigations into Health Net's security procedures.

The California company declined to comment, saying the incident was still under investigation.

The latest incident is "an eye-opener, and we're going to get eye-opener after eye-opener," says Jim Dempsey, a security and public policy expert at the Center for Democracy & Technology.

As instances of data mishandling become more commonplace, government officials may seek greater control over security policies of companies with access to health care records that aren't currently regulated.

"It should be yet another warning bell for companies: You've got your reputation on the line, and you're also facing enforcement action if you don't pay attention to the security of the data you collect and process," Dempsey says.