

Bloomberg

States' Hospital Data for Sale Puts Privacy in Jeopardy

By Jordan Robertson - Jun 5, 2013

Hospitals in the U.S. pledge to keep a patient's health background confidential. Yet states from [Washington](#) to [New York](#) are putting privacy at risk by selling records that can be used to link a person's identity to medical conditions using public information.

[Graphic: Your Not-So-Anonymous Medical Records](#)

Consider Ray Boylston, who went into diabetic shock while riding his motorcycle in rural Washington in 2011. He careened off the road and was thrown into the woods, an accident that was covered only briefly, in the local newspaper. Boylston disclosed his medical condition and history to a handful of loved ones and the hospital that treated him.

After Boylston's discharge, Washington collected the paperwork of his week-long stay from [Providence Sacred Heart Medical Center](#) in Spokane and added it to a database of 650,000 hospitalizations for 2011 available for sale to researchers, companies and other members of the public. The data was supposed to remain anonymous. Yet because of state exemption from federal regulations governing discharge information, Boylston could be [identified](#) and his medical background exposed using only publicly available information.

"I don't really feel that the public has a right to read up on my medical history," said Boylston, who is 62 and a veteran. "I feel I've been violated."

He agreed to share his story when contacted by [Bloomberg News](#).

The potential for a patient's hospital record to be made public by anyone buying data compiled by states adds to ways privacy is vulnerable in an age of digitized health record keeping and increasingly sophisticated hacking.

China, Twitter

Security concerns have been heightened recently by the breach of the Associated Press Twitter Inc. account, which resulted in a temporary stock-market decline, U.S. accusations that the Chinese military is engaged in a cyber espionage campaign and attacks on financial institutions that have led to losses of tens of millions of dollars in the past year.

Laws governing medical-information sharing were intended to protect the privacy of patients like Boylston. People can lose out on jobs, pay more for insurance, fare poorly in custody battles and suffer personal embarrassment. The trouble is that state [public-health](#) agencies received an exemption from the federal law, formally the Health Insurance Portability and Accountability Act, or HIPAA, [enacted](#) in 1996. The [privacy](#) rules took effect in 2003, though they apply only to health-care providers, insurers, billing and claims processors and their contractors.

Potential Compromise

Some states voluntarily follow the law's strict privacy guidelines, which require that discharge data be shorn of details -- such as age, ZIP codes or admission and discharge dates -- that could be used to connect it to a specific person.

Washington and at least 25 other states release some combination of these identifying markers, increasing the likelihood that patient privacy can be compromised, according to records reviewed by Bloomberg News and [Latanya Sweeney](#), director of Harvard University's [Data Privacy Lab](#).

"All I have to know is a little bit about a person and when they went to a hospital, and I can find their medical record in this kind of data," Sweeney said. "The real takeaway is we can do better than this."

Some of the states, including New York, require purchasers to sign [affidavits](#) saying that they won't use information to identify individuals. Washington has no such requirement.

\$2.7 Trillion

The medical-data industry is projected to surpass \$10 billion by 2020, [according](#) to McKinsey & Co., driven largely by President Obama's health-care overhaul, which mandates the maintenance of electronic medical records and data sharing to rein in growth of U.S. health care costs, [estimated](#) at \$2.7 trillion in 2011.

[Companies that benefit](#) from buying states' hospital records include IMS Health Inc., the provider of prescription data that was taken private by TPG Capital and Canada Pension Plan Investment Board for \$5.1 billion in 2010. Other buyers are OptumInsight, a division of [UnitedHealth Group Inc. \(UNH\)](#), the biggest U.S. health insurer, and [WebMD Health Corp. \(WBMD\)](#), which supplements its consumer website with services advising companies and insurers.

Buyers can use the information to better understand hospital costs, analyze prescription-drug use and help recruiters identify top-performing physicians. A major target is helping the pharmaceutical industry tailor ads to doctors and potential patients. Drug companies spent \$10.5 billion on advertising last year, according to IMS.

'Nuclear Energy'

“Electronic health information is like nuclear energy,” said Jim Pyles, principal of Powers Pyles Sutter & Verville PC in Washington, who specializes in health law and policy. “If it’s harnessed and kept under tight control, it has potential for good. But if it gets out of control, the damage is incalculable.”

Using only public record searches, Bloomberg News collected information about how hospital data is distributed from the most populous states and, with Sweeney’s help, analyzed it. Her research will be presented today at the [International Summit on the Future of Health Privacy](#) in Washington.

Along with Washington, records in New York, [New Jersey](#), [Tennessee](#) and [Arizona](#) were particularly vulnerable. Those states also include some combination of age, ZIP codes and admission and discharge dates.

No breaches of personal privacy were uncovered. Still, the information would have enormous value in the wrong hands, said Jim Adler, former [chief privacy officer](#) of Intelius Inc., an online background-check provider.

Data ‘Leverage’

“People will use that information if they can move the needle with it,” Adler said. “It’s all about leverage, and medical data is leverage.”

Health information obtained through other means, such as computer hacking or insider theft, is already abused for insurance fraud and [identity theft](#). Data breaches have also exposed millions of patient records. The ability to find a person’s medical file in public data represents a new danger.

Boylston is one of several dozen people who could be identified by reference to public records, which were purchased by Harvard’s Sweeney in a bundle for \$50.

Many other identified patients requested anonymity.

An executive treated for assault was found to have a painkiller addiction. A businessman who had gone missing was shown to have poisoned himself in a suicide attempt and had been diagnosed with pancreatic cancer. A retiree who crashed his motorcycle was described as arthritic and morbidly obese.

Blood Clotting

Dick Zais, 63, a former city manager of Yakima, Washington, was in there too -- for a blood-clotting emergency. He said he wasn’t concerned that details of that incident were disclosed, since he himself [revealed](#) the condition to the press. He did ask that an older condition included in his record remain private.

“It’s come to the point where we need to think long and hard about whether we can actually expect

privacy anymore,” he said.

The people identified had only two things in common: there were news briefs written about their incidents, usually involving auto accidents or assaults, and they were treated in Washington. A total of 35 patients were identified from 81 subjects of news stories that contain the word “hospitalization.”

Ordinarily, the information patients divulge to health-care providers remains confidential. Doctors, hospitals, insurers and their contractors are tightly restricted in what they can provide third parties under the privacy law.

Strict Guidelines

Patient information that is shared typically has 18 key identifiers removed under a standard known as [Safe Harbor](#).

When applied properly, the standard makes it difficult to link a patient’s name with a health record, said Dan Barth-Jones, an infectious-disease [epidemiologist](#) at the Columbia University Mailman School of Public Health who researches health privacy.

A 2011 [study](#) by [University of Chicago](#) researchers found that of 15,000 hospital records stripped to the Safe Harbor standard, only two could be matched to a marketing list obtained from a third party.

Before HIPAA, there were no federal restrictions on the sale of health records, and only half the states had any rules, according to [Peter Swire](#), who led the creation of the privacy protections under President [Bill Clinton](#).

Weld’s Records

Sweeney, the Harvard researcher, [exposed flaws](#) in the system in 1997 by finding the medical records of former Massachusetts Governor William Weld in a redacted dataset. Her finding served as a catalyst for tighter rules.

States were deliberately exempted from the rules when additional privacy protections were being hammered out more than a decade ago. While the medical establishment wanted states to have consistent rules, consumer advocates pushed for an exemption, said Janlori Goldman, [co-founder](#) of the Center for Democracy and Technology who was involved in the process.

The argument: states were likely to impose stronger restrictions to protect vulnerable populations, such as people with AIDS, she said.

Boylston’s record contains every diagnosis and medical procedure following his accident, from a broken pelvis that forces him to use a walker to a ruptured spleen, [kidney failure](#) and conditions that

led to the removal of his bladder. His doctors, ethnicity and payment information are all there.

Snooping Strangers

A two-tour veteran of the [Vietnam War](#), Boylston said he isn't concerned about insurance or employment discrimination because he has health-care coverage and is retired. But he said he is worried about pharmaceutical and medical-device marketers and snooping strangers obtaining the information.

Boylston was one of nine patients from Providence Sacred Heart Medical Center whose records were identified.

“Providence has significant safeguards in place to protect our patients’ information,” said Brenda Gramling, privacy officer for Eastern Washington and [Montana](#) with Providence Health & Services, which owns the hospital. “We are talking to the Washington State Department of Health to determine if additional safeguards are needed.”

Washington chose to release more data because it is not bound by HIPAA and wanted to make its [Comprehensive Hospital Abstract Reporting System](#), or CHARS, more useful than the federal standard allows, said Donn Moyer, spokesman for the Washington State Department of Health.

Washington Reconsiders

Knowing patients’ ages helps researchers study health trends affecting infants, while ZIP codes and hospitalization dates help track seasonal patterns, such as the flu, Moyer said. Removing all the identifiers required under Safe Harbor would render the data “useless,” Moyer said.

After learning from Bloomberg that data could be traced to individuals, Washington State Secretary of Health John Wiesman said the state is considering limits on the information it discloses and may stop releasing data until a decision is made.

“Patient confidentiality and privacy are priorities for us, and I take it very seriously,” Wiesman said in a statement. “We’re re-looking at the information included in the public data set to determine if changes can legally be made.”

Peter Constantakes, spokesman for the New York State Department of Health, said he could not immediately comment.

Washington and other states don't make much money selling hospital records. They started collecting the records decades ago to facilitate public health research, and costs were intentionally kept low.

Scant Revenue

Twelve of the most populous states generated \$1.91 million from 1,698 requests for data from 2011, the latest year for which figures are available, according to state records reviewed by Bloomberg News. Washington sold its database 95 times in 2011 and generated just \$15,950.

One company that purchased Boylston's record was IMS Health, owner of one of the world's deepest pools of medical information. IMS, based in Danbury, [Connecticut](#), has prescription-drug [dossiers](#) on 260 million people, said Jody Fisher, U.S. marketing director for IMS.

The data is all anonymous, and IMS doesn't try to re-identify patients, Fisher said. IMS's [revenue](#) was \$2.19 billion in 2009, the year before the company was taken private. About 85 percent of the total came from [pharmaceutical companies](#), which use the data to design sales pitches for doctors and craft direct-mail and online-ad campaigns for consumers.

Boylston's record also wound up with [iVantage Health Analytics](#), a Portland, Maine-based firm that measures hospital performance.

'Risky' ZIP

While precise geographic data about patients is useful, disclosing ZIP codes in public records creates unnecessary risk, said John Morrow, [executive vice president](#) at iVantage. The company routinely scrubs such information from its files, he said.

"You might as well have the patient's electronic medical record number," he said. "We think it's potentially as risky to have a patient's ZIP code."

The [U.S. Department of Health](#) and Human Services Office for [Civil Rights](#), which investigates HIPAA violations, has not received complaints about companies identifying patients, said Rachel Seeger, a spokeswoman for the agency.

Boylston, who lives in the tiny town of [Soap Lake](#) in central Washington, has a suggestion for organizations that want to release his health data in an insecure way: ask first.

"If they're going to release that kind of information, they should consult with the patient," he said. "That's personal information about me. It's just not right."

To contact the reporter on this story: Jordan Robertson in [San Francisco](#) at jrobertson40@bloomberg.net

To contact the editor responsible for this story: Tom Giles at tgiles5@bloomberg.net