Is your doctor's office the most dangerous place for data? (Update)

February 9 2015, byTom Murphy And Brandon Bailey

In this Oct. 10, 2009 file photo, people fill out forms to get a free seasonal flu shot at Memorial Medical Center in Las Cruces, N.M. Those seemingly harmless medical forms everyone fills out before seeing a doctor can plant the seeds for identity theft and other scams if they get into the wrong hands. (AP Photo/Las Cruces Sun-News, Norm Dettlaff, File)

Everyone worries about stolen credit cards or hacked bank accounts, but just visiting the doctor may put you at greater risk for identity fraud.

Those medical forms you give the receptionist and send to your health insurer provide fertile ground for criminals looking to steal your identity, since health care businesses can lag far behind banks and credit card companies in protecting sensitive information. The names, birthdates and—most importantly—Social Security numbers detailed on those forms can help hackers open fake credit lines, file false tax returns and create fake medical records.

"It's an entire profile of who you are," said Cynthia Larose, chair of the privacy and security practice at the law firm Mintz Levin in Boston. "It essentially allows someone to become you."

Social Security numbers were created to track the earnings history of workers in order to determine government benefits. Now, health care companies are, in some cases, required to collect the numbers by government agencies. They also use them because they are unique to every individual and more universal than other forms of identification like driver's licenses, said Dr. Ross Koppel, a University of Pennsylvania professor who researches health care information technology.

But once someone creates a stolen identity with a Social Security number, it can be hard to fix the damage. A person can call a bank to shut down a stolen credit card, but it's not as easy of a process when it comes to Social Security numbers.

"There is no such mechanism with Social Security numbers and our identity," said Avivah Litan, a cybersecurity analyst at the research firm Gartner. "You can't just call the bank and say, 'Give me all the money they stole from my identity.' There's no one to call."

So being that the data is so vital to protect, health care companies are taking every precaution to defend against hackers, right?

Not necessarily. The FBI warned health care companies a year ago that their industry was not doing enough to resist cyberattacks, especially compared with companies in the financial and retail sectors, according to Christopher Budd of security software company Trend Micro. The warning came in a government bulletin to U.S. companies that cited research by a nonprofit security institute, he said.

Last year, more than 10 million people in the U.S. were affected by health care data breaches—including hacking or accidents that exposed personal information, such as lost laptops—according to a government database that tracks incidents affecting at least 500 people. That was the worst year for health care hacking since 2011.

Litan estimates that the health care industry is generally about 10 years behind the financial services sector in terms of protecting consumer information. She figures that it may be twice as easy for hackers to get sensitive financial information out of a health care company compared with a bank. Banks, for instance, are more likely to encrypt personal data, which can garble the information if a hacker gets ahold of it. They also are much more likely to use advanced statistical models and behavior analytics programs that can spot when someone's credit card use suddenly spikes, says Litan, who studies fraud-detection technology. That's a sign of possible fraud that may be worth investigating.

"There's a need for that everywhere now," she said.

Health care companies do have security to protect sensitive patient information. Anthem, the nation's second-largest health insurer, said last week that hackers broke into a database storing information on 80 million people, including Social Security numbers. The company had "multiple layers of security" in place before the attack, said David

Damato, managing director at FireEye, the security company hired by Anthem to investigate the breach.

But the stolen data was not encrypted. An Anthem spokeswoman said encryption wouldn't have helped, because the intruder used high-level security credentials to get into the company's system.

Still, several experts say encryption does help.

Encryption programs can be tuned so that even authorized users can view only one person's account, or a portion of an account record, at a time, said Martin Walter, senior director at cybersecurity firm RedSeal Networks. That makes it harder for an outsider to view or copy a whole stockpile of records.

Even if Anthem's security had proved invulnerable, the health care system offers several other inviting targets with varying levels of security. Hospitals, labs, clinics and doctor's offices all can be attacked. Cybersecurity experts say they expect even more health care hacking problems in the future as those layers of the health care system shift their paper files to electronic medical records, a push that has been boosted by federal funding in recent years.

"A lot of businesses that didn't place a premium on security are now placing this incredibly valuable information online," noted Al Pascual, director of fraud and security at the consulting firm Javelin Strategy & Research.

The experience of a big company like Anthem does not bode well for the broader health care industry, said Budd at Trend Micro.

"They have resources to throw at cyber security," he said. "And if someone with nearly unlimited resources can be breached like this, then it raises serious questions as to what's at risk."

Beth Knutsen still worries about someone using her Social Security number more than a year after she was told that some old patient files of hers had been taken from a doctor's office in Chicago. The 39-year-old New York resident visited that doctor nearly 20 years ago.

She's seen no signs of fraud yet, and she still provides her Social Security number when a doctor's office asks for it—but only because it seems to be required for insurance and billing.

"It's so scary," she said. "Who knows what can happen with that information?"

Citation: Is your doctor's office the most dangerous place for data? (Update) (2015, February 9) retrieved 2 May 2024 from https://phys.org/news/2015-02-health-fertile-field-cyber-crime.html