The Switch

2015 is already the year of the health-care hack — and it's only going to get worse.

By Andrea Peterson March 20

Last year, the fallout from a string of breaches at major retailers like Target and Home Depot had consumers on edge. But 2015 is shaping up to be the year consumers should be taking a closer look at who is guarding their health information.

Data about more than 120 million people has been compromised in more than 1,100 separate breaches at organizations handling protected health data since 2009, according to Department of Health and Human Services data reviewed by The Washington Post.

"That's a third of the U.S. population -- this really should be a wake-up call," said Deborah Peel, the executive director of Patient Privacy Rights.

The data may double-count some individuals if they had their information compromised in more than incident, but it still reflects a staggering number of times Americans have been affected by breaches at organizations trusted with sensitive health information. And the data does not yet reflect the hack of Premera, which announced this week that hackers may have accessed information, including medical data, on up to 11 million people.

*[**Read:** Premera Blue Cross says data breach could affect 11 million people]*

Most breaches of data from health organizations are small and don't involve hackers breaking into a company's computer system. Some involve a stolen laptop or the inappropriate disposal of paper records, for example -- and not all necessarily involve medical information. But hacking-related incidents disclosed this year have dramatically driven up the number of people exposed by breaches in this sector.

When Anthem, the nation's second-largest health insurer, announced in February that hackers broke into a database containing the personal information of nearly 80 million records related to consumers, that one incident more than doubled the number of people affected by breaches in the health industry since the agency started publicly reporting on the issue in 2009.

"We are certainly seeing a rise in the number of individuals affected by hacking/IT incidents," Rachel Seeger, a spokesperson for HHS's Office for Civil Rights, said in a statement. "These incidents have the potential to affect very large numbers of health care consumers, as evidenced by the recent Anthem and Premera breaches."

And some cybersecurity experts warn this may only be the beginning. "We're probably going to see a lot more of these happening in the coming few months," said Dave Kennedy, the chief executive of TrustedSEC.

Health organizations are targets because they maintain troves of data with significant resale value in black markets, Kennedy said, and their security practices are often less sophisticated than other industries. Now that some major players in the market have come forward as victims of cyberattacks other organizations are likely to take a close look at their own networks -- potentially uncovering other compromises, he said.

"The information that companies like Anthem and Premera had is more valuable than just payment card information held by retailers or financial institutions," said Scott Vernick, who heads up the data security and privacy practice at law firm Fox Rothschild. Credit card information has a relatively short shelf life, with new cards issued on a regular basis, he explained. But a health organizations often have complete profiles of people including Social Security numbers and medical health information that is much more difficult if not impossible to change.

*[**Related:** Yes, we're still using dumb passwords. But not nearly as much as before.]*

Some of the data can be used to pursue traditional financial crimes -- like setting up fraudulent lines of credit, Kennedy said. But it can also be used for medical insurance fraud, like purchasing medical equipment for resale or obtaining pricey medical care for another person.

This type of scheme is often not caught as quickly as financial fraud, experts said, and could have a lasting affect if it results in a person's medical history containing false information. "In theory you could end up in an emergency situation, and if your records are contaminated by someone else's information that could cause serious problems -- like medical professionals believing you have a different blood type," said Peel.

If a hacker is able to obtain information about a person's medical condition, as it appears may have happened in the Premera breach but not the Anthem breach, there are additional risks. Information about mental health or HIV treatments could be made public, and there's no way to truly make the information private again. "There's almost no way to remedy this; there's no recourse," said Peel.

Health care providers already have to comply with government rules on protecting patient privacy, including HIPAA, which are enforced by HHS.

"Health care organizations need to make data security central to how they manage their information systems and to be vigilant in assessing and addressing the risks to data on a regular basis," said Seeger, the HHS official. "In addition, organizations need to ensure they are able to identify and respond appropriately to security incidents when they do happen to mitigate harm to affected individuals and prevent future similar incidents from occurring."

State-level officials are also increasingly involved in enforcement in this area, said Vernick, and consumers may have additional legal avenues depending on state laws.

But privacy and cybersecurity advocates say the industry and the government still aren't doing enough to protect consumers.

"HIPAA required security be addressed, but it wasn't spelled it out exactly how, so there was no culture of using ironclad security," said Peel. "We have systems that are engineered as though this data is not sensitive and valuable."

Health organizations sometimes rely on legacy systems, and some have not invested in cybersecurity at a rate that matches the urgency of the threats they face, Kennedy said. "The medical industry is years and years behind other industries when it comes to security."

Even before the Anthem breach, major health insurers had become aware of the rising risk of cyberattacks. Aetna and United Health Group both cited the risks of hackers and breaches in their respective 2013 financial reports.

And the industry is already taking steps to coordinate how it responds to such incidents through groups designed to share information about digital threats -- like the National Health Information Sharing and Analysis Center, or NHISAC. The organization is one of several efforts related to critical infrastructure that works with the Department of Homeland Security to share data about current threats, such as what sort of tactics are used and forensic information about attackers.

Members are able to share details about security incidents in "machine time" using an automated system, according to NHISAC executive director Deborah Kobza, and the group sends out daily threat updates. When a major cyberattack is disclosed, NHISAC erupts into a flurry of activity -- trying to find out as much as possible so its members have information that can make it easier to see if they've been the victims of a similar attack.

And 2015 has already kept NHISAC busy: "We just caught our breath from the Anthem hack, and here we go again," said Kobza about responding to the Premera breach.

Read more:

China suspected in major hacking of health insurer Anthem

How tax sites like TurboTax can better protect customers

Target data breach victims could get up to $10,000 each from court settlement

Andrea Peterson covers technology policy for The Washington Post, with an emphasis on cybersecurity, consumer privacy, transparency, surveillance and open government.