ALL OF YOUR MEDICAL RECORDS WILL BE HACKED - DO NOT ALLOW YOUR DATA TO APPEAR ONLINE

Mon, 29 Aug 2022 13:26:44, newstips66, [category: afghanistan, post_tag: all-of-your-medical-records-will-be-hacked-do-not-allow-your-data-to-appear-online, category: brotopia, category: community-service-programs, category: energy-dept-slush-fund, category: facebook-meta, category: google-alphabet, category: hired-assassins]

ALL OF YOUR MEDICAL RECORDS WILL BE HACKED - DO NOT ALLOW YOUR DATA TO APPEAR ONLINE

With a dearth of resources, the Office for Civil Rights is struggling with an overflowing caseload.


Hands type on a backlit computer keyboard.

Cyber criminals steal tens of millions of dollars a year in health care data, but HHS' Office for Civil Rights has a shoestring budget and overworked investigators. | Sean Gallup/Getty

By Ben Leonard

-

Cyber crooks steal medical information of tens of millions of people in the U.S. every year, a number that is rising fast as health care undergoes its digital transformation.

It leads to millions of dollars in losses for hospitals, insurers and other health care organizations, threatens care delivery and exposes patients to identity theft.

But the Department of Health and Human Services' Office for Civil Rights, which is tasked with investigating breaches, helping health care organizations bolster their defenses, and fining them for lax security, is poorly positioned to help. That's because it has a dual mission — both to enforce the federal health privacy law known as HIPAA and to help the organizations protect themselves — and Congress has given it few resources to do the job.

"They're a fish out of water … They were given the role of enforcement under HIPAA but weren't given the resources to support that role," said Mac McMillan, CEO of CynergisTek, a Texas firm that helps health care organizations improve their cybersecurity.

Due to its shoestring budget, the Office for Civil Rights has fewer investigators than many local police departments, and its investigators have to deal with more than a hundred cases at a time. The office had a budget of $38 million in 2022 — the cost of about 20 MRI machines that can cost $1 million to $3 million a pop.

Another problem is that the office relies on the cooperation of the victims, the institutions that hackers have targeted, to provide evidence of the crimes. Those victims may sometimes be reluctant to report breaches, since HHS could then accuse them of violating HIPAA and levy fines that come on top of costs stemming from the breach and the ransoms often demanded by the hackers.

Depending on the circumstances, it can seem like blaming the victim, especially since the hackers are sometimes funded or directed by foreign governments. And it's raised questions about whether the U.S. government should be doing more to protect health organizations.

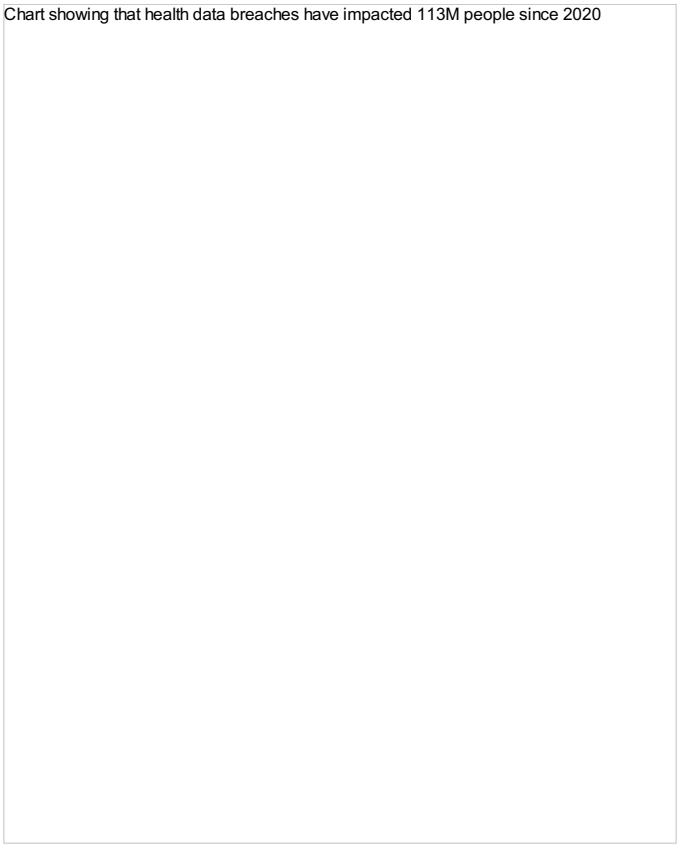
In an Aug. 11 letter to HHS Secretary Xavier Becerra, Sen. Angus King (I-Maine) and Rep. Mike Gallagher (R-Wis.), past co-chairs of a cybersecurity commission that examined the danger, raised that point, questioning the government's "lack of robust and timely sharing of actionable threat information with industry partners."

'A stronger hammer'

The scope of the threat is massive and the consequences of breaches severe. According to a 2021 survey by the Healthcare Information and Management Systems Society, more than two-thirds of health care organizations had a "significant" incident in the previous year — mostly phishing or ransomware attacks.

These episodes pose potentially significant financial consequences and can threaten patients' lives. A recent report from cybersecurity company Cynerio and the Ponemon Institute, a cybersecurity research center, found that about 1 in 4 cyberattacks resulted in increased mortality by delaying care.

Experts said the health care sector is particularly vulnerable to attacks, partly due to its digital transformation and partly due to its vulnerability to ransomware. Disrupting care could endanger patients' lives, which can leave health care organizations feeling forced to fork over ransoms. In 2021 alone, hackers accessed records of nearly 50 million people, raising privacy concerns and leaving many vulnerable to fraud.



The HHS office expects to see 53,000 cases in the 2022 fiscal year. As of 2020, it had 77 investigators, some of whom are assigned to other things, like civil rights violations.

The Biden administration official who runs the Office for Civil Rights, Melanie Fontes Rainer, said her investigators have to pick their battles because they are "under incredible resource constraints and incredibly overworked."

She frames the problem as one of funding and the Biden administration has asked Congress to give the agency a roughly 58 percent budget increase in fiscal 2023, to $60 million, that would allow it to hire 37 new investigators.

But advocates for victims want to be sure those new hires would favor helping them prevent future attacks over penalizing them for failing to stop past ones.

"If OCR is looking for money that will protect hospitals … good. That's HHS' role — not just to penalize the victim," said Greg Garcia, executive director of the Healthcare and Public Health Sector Coordinating Council, which represents a number of sectors within health care targeted by the hackers.

For the most part, that's what the office does, but fines are always a possibility and Fontes Rainer said more resources will yield more enforcement that will encourage health care organizations to meet their obligations under HIPAA. Tim Noonan, a high-ranking official under Fontes Rainer, also expects it will bolster the agency's ability to offer guidance and technical assistance.

A budget increase "will give us a stronger hammer," Fontes Rainer said. "Enforcement … stops the conduct, but is also a deterrent for others."

In July, HHS levied its first major fine on breaches since President Joe Biden took office, $875,000 on Oklahoma State University's Center for Health Services. Agency investigators found that the center may not have reported a breach in a timely manner and that it also had failed to take steps to protect data.

And Fontes Rainer is pressing to increase fines following a legal setback at the end of the Trump administration.

In January 2021, the 5th Circuit Appeals Court struck down a $4.3 million penalty that the Office for Civil Rights had assessed the University of Texas M.D. Anderson Cancer Center over data breaches. The court called it "arbitrary" and "capricious," giving ammunition to critics of the office's enforcement efforts.

The Trump administration levied more than $50 million in fines related to breaches over four years. But the director of the Office for Civil Rights at the time, Roger Severino, also moved to reduce fines for entities that weren't found in "willful neglect" of the privacy law or had taken corrective action, saying the office had misinterpreted the law.

'A cop on the side of the road'

If HHS were to further back off from enforcement, it could prompt more negligence, some experts said.

More than half of the health care industry is "woefully underprepared" to protect against cyber threats, said Carter Groome, CEO of First Health Advisory, a health care risk management consulting firm.

At organizations with few resources, that lack of preparedness is understandable. But it's not at large health systems.

"We know of a CIO in a small rural facility … he's also in charge of … everything from snow shoveling to making sure the air conditioning is working," said Tom Leary, head of government relations at the Healthcare Information and Management Systems Society. "But if they're well-resourced and they're not meeting their responsibilities, [enforcement] absolutely needs to be a part of the process."

Leary's group has found that cybersecurity budgets are often meager.

Stepped-up enforcement could prompt health care organizations to increase them.

"You see a cop on the side of the road, you slow down. When you don't, you may not necessarily be paying as much attention to how fast you're going."

Deven McGraw, lead of data stewardship and sharing at biotech firm Invitae

Others are more skeptical. "HHS enforcement is like ninth on the list of reasons to have a good security program," Kirk Nahra, a privacy attorney at law firm WilmerHale said, adding that aggressive enforcement could hamper data sharing that the government is otherwise trying to encourage. "Why would I open up access to you ... if there's a risk it could go wrong and I could get hammered."

There are other ways government could help health care organizations improve their cybersecurity. Advocates for industry point to two key areas: cash for better defense systems and funding for workforce development.

John Riggi, the national adviser for cybersecurity and risk at the American Hospital Association, has called for federal support in training workers and grants to help organizations boost their security efforts. And in testimony to Congress, Erik Decker, chief information security officer at hospital chain Intermountain Healthcare, called for the Centers for Medicare & Medicaid Services to look into developing payment models to "directly fund" cyber programs.

In contrast to King and Gallagher, many in the industry said they are encouraged by progress on information sharing. HHS' Health Sector Cybersecurity Coordination Center has helped, they said, and the public-private 405(d) Program and Task Group has received high marks for its work to develop guidelines to help health care organizations defend themselves. Congress called for the collaboration in section 405(d) of a 2015 law.

Still, King and Gallagher in their letter to Becerra said they worried the information sharing was not robust enough, given the growth in cyberattacks. They called for an urgent briefing from HHS and suggested they'd be willing to propose funding and laws extending the agency new powers to take on the hackers.

Wireless carriers keep location data for years -- provide to police...

Broker tracked church, health visits...