Privacy Law Watch™

April 10, 2018

Bloomberg BNA

Data Security

Medicare Patient Data Vulnerable to Hackers

BNA Snapshot

- Medicare isn't doing enough to protect security of patient data
- A systemwide data breach would do immeasurable harm to Medicare beneficiaries

By James Swann

Medicare's massive trove of patient data may be vulnerable to a systemwide data breach as hackers take advantage of security lapses and lax oversight.

A congressional watchdog agency identified several Medicare data security vulnerabilities, including a lack of timely software updates and a failure to address low-risk security issues. Roughly 58 million patients are enrolled in Medicare, and the federal government spent $696 billion on benefit payments in fiscal year 2017.

A full-blown data breach of Medicare patient information as predicted by the federal agency would be catastrophic, undermining both the legitimacy of the program and wreaking financial disaster on both patients and health-care providers.

Patient data from Medicare's private fee-for-service plan make an attractive target for hackers and cybercriminals, and it makes more sense to conduct a proactive assessment of the program's vulnerability rather than identify problems after a major breach, W. Reece Hirsch, a health-care attorney with Morgan, Lewis & Bockius LLP in San Francisco, told Bloomberg Law.

The April 5 Government Accountability Office report encourages both enhanced data security oversight by the Centers for Medicare & Medicaid Services as well as better oversight by Medicare payment contractors and qualified entities that evaluate Medicare providers, Hirsch said.

“I wouldn't say the report is harshly critical, but it does lay out a road map for enhancing CMS security,” Hirsch said.

It's frightening to imagine an Equifax-type breach involving Medicare data, but the risk is real and it's probably just a matter of time until one occurs, Colin Zick, a health-care attorney with Foley Hoag LLP in Boston, told Bloomberg Law. State-level health-care hacks have already happened, Zick said, noting a 2009 hack of the Virginia state prescription monitoring program.

In September 2017, Equifax announced a cybersecurity breach in which hackers accessed about 145.5 million U.S. Equifax consumers’ personal data, including full names, Social Security numbers, birth dates, addresses, and, in some cases, driver license numbers.

The CMS didn't respond to a request for comment on the report.

Perfect Storm

Medicare patient data represents a perfect storm of vulnerability, as it's highly sensitive and attractive to hackers, there are many different users and transmitters of the data, and the Medicare program is so large, Laura Hammargren, a health-care attorney with Mayer Brown LLP in Chicago, told Bloomberg Law.

However, Medicare enforces many regulations and levies penalties associated with the care of beneficiary data, and some of the security risks cited by the GAO seem to be lower risk in terms of security systems, Hammargren said. The GAO identified weaknesses with Medicare Administrative Contractors keeping an up-to-date inventory of hardware and software and having an effective data security strategy. MACs are responsible for processing Medicare claims and making reimbursement payments.

It's critical that the CMS ensure its data security is ironclad, because the consequences of a widespread Medicare data breach could be significant, Hammargren said.

Medicare data is likely no more susceptible to hacks or security incidents than other medical or financial data, but the amount of Medicare data on individual beneficiaries makes the program an attractive target for criminals, Ellen Janos, a health-care attorney with Mintz, Levin, Cohn, Ferris, Glovsky and Popeo PC, in Washington, told Bloomberg Law.

“A widespread data breach would be very problematic for the millions of elderly beneficiaries who might not have the tools and resources to protect against the identity theft that could result from such a breach,” Janos said.

The CMS needs to perform regular data security audits and closely monitor all data systems that are shared among the CMS and its contractors, Janos said.

To contact the reporter on this story: James Swann in Washington at jswann1@bloomberglaw.com

To contact the editor responsible for this story: Kendra Casey Plank at kcasey@bloomberglaw.com

For More Information

The GAO report is at https://www.gao.gov/assets/700/690481.pdf.