# Anthem breach: A gap in federal health privacy law?

February 6 2015, byRicardo Alonso-Zaldivar


In this Feb. 5, 2015 file photo, the Anthem logo hangs at the health insurer's corporate headquarters in Indianapolis. Insurers aren't required to encrypt consumers' data under a 1990s federal law that remains the foundation for health care privacy in the Internet age _ a striking omission in light of the cyberattack against Anthem, the nation's second-largest health insurer. (AP Photo/Michael Conroy, File)

(AP)—Insurers aren't required to encrypt consumers' data under a 1990s

federal law that remains the foundation for health care privacy in the Internet age—an omission that seems striking in light of the major cyberattack against Anthem.

Encryption uses mathematical formulas to scramble data, converting sensitive details coveted by intruders into gibberish. Anthem, the second-largest U.S. health insurer, has said the data stolen from a company database that stored information on 80 million people was not encrypted.

The main federal health privacy law—the Health Insurance Portability and Accountability Act, or HIPAA—encourages encryption, but doesn't require it.

The lack of a clear encryption standard undermines public confidence, some experts say, even as the government plows ahead to spread the use of computerized medical records and promote electronic information sharing among hospitals, doctors and insurers.

"We need a whole new look at HIPAA," said David Kibbe, CEO of DirectTrust, a nonprofit working to create a national framework for secure electronic exchange of personal health information.

"Any identifying information relevant to a patient ... should be encrypted," said Kibbe. It should make no difference, he says, whether that information is being transmitted on the Internet or sitting in a company database, as was the case with Anthem.

The agency charged with enforcing the privacy rules is a small unit of the federal Health and Human Services Department, called the Office for Civil Rights.

The office said in a statement Friday that it has yet to receive formal notification of the hack from Anthem, but nonetheless is treating the

case as a privacy law matter. Although Anthem alerted mainline law enforcement agencies, the law allows 60 days for notifying HHS.

The statement from the privacy office said the kind of personal data stolen by the Anthem hackers is covered by HIPAA, even if it does not include medical information.

"The personally identifiable information health plans maintain on enrollees and members—including names and Social Security numbers—is protected under HIPAA, even if no specific diagnostic or treatment information is disclosed," the statement said.

A 2009 federal law promoting computerized medical records sought to nudge the health care industry toward encryption. Known as the HITECH Act, it required public disclosure of any health data breach affecting 500 or more people. It also created an exemption for companies that encrypt their data.

Encryption has been seen as a controversial issue in the industry, particularly with data that's only being stored and not transmitted. Encryption adds costs and can make day-to-day operations more cumbersome. It can also be defeated if someone manages to decipher the code or steals the key to it.

In fact, Anthem spokeswoman Kristin Binns said encryption would not have thwarted the latest attack because the hacker also had a system administrator's ID and password. She said the company normally encrypts data that it exports.

Under the HITECH law, the government set up a public database listing major breaches, known informally as the "hall of shame." Breaches on that list affected more than 40 million people over a decade, meaning that the Anthem case could be twice as damaging as all previous reported

incidents combined.

Indiana University law professor Nicolas Terry said it seemed at the time of the 2009 law that the government had struck a reasonable balance, creating incentives for encryption while stopping short of imposing a one-size-fits-all solution. Now he's concerned that the compromise has been overtaken by events.

"In today's environment, we should expect all health care providers to encrypt their data from end to end," said Terry, who specializes in health information technology.

If the voluntary approach isn't working, "HHS should amend the security rule to make encryption mandatory," he said.

The federal government also is investigating whether the personal information of Medicare and Medicaid beneficiaries was stolen. Those government programs are a major contract business for Anthem.

The federal health care privacy law "was written largely for what was going on in the '90s," said Kibbe, the cyberstandards expert. "It was updated in 2009, but that wasn't an overhaul. It was a tuneup."

**More information:** HHS breach database - tinyurl.com/o4wd6ym