CRS Insights

Anthem Data Breach: How Safe Is Health Information Under HIPAA?
C. Stephen Redhead, Specialist in Health Policy (credhead@crs.loc.gov, 7-2261)
February 24, 2015 (IN10235)

The recent data breach at Anthem Inc.—the nation's second-largest health insurer, with more than 37 million enrollees in its health plans—raises new concerns about the vulnerability of electronic health information. Security experts question whether the Health Insurance Portability and Accountability Act (HIPAA) privacy and security standards are sufficiently protective of sensitive patient information.

On February 4, Anthem announced that it had been the subject of a "very sophisticated external cyberattack." After several prior attempts, the hackers succeeded in accessing a company database containing as many as 80 million records of current and former Anthem customers as well as employees. A company website indicates that the hackers accessed names, dates of birth, member IDs and Social Security numbers, home and email addresses, and employment information. They do not appear to have gained access to any credit card or medical information. Even though the compromised data may not include any clinical information, it is still protected under HIPAA because it relates to the payment of health care.

According to Anthem, the hackers obtained the security credentials of one or more computer system administrators. They used those credentials to log into the company system and access the data, which was not encrypted. Encryption is commonly used to protect data transmitted from one location to another, but encrypting data at rest (i.e., stored in place and not being transmitted) is controversial. Encryption can add cost and make day-to-day management and use of the data more burdensome.

Some security experts argue that encryption, by itself, would not have thwarted the Anthem breach because the hackers were able to access the credentials of someone inside the company. They note that an attacker with sufficiently elevated security credentials (including access to the encryption and de-encryption keys) would be able to access encrypted data. While encryption helps protect sensitive information, the Anthem breach shows the importance of having other safeguards in place, including strong data access controls.

The Anthem breach has led to renewed criticism of the HIPAA security standards, which are intended to protect electronic information—both at rest and during transmission—from unauthorized access, use, or disclosure. The standards are technology-neutral and scalable, based on the size and complexity of the organization. They include security management, data access controls, and data transmission security.

Payers and providers of health care have considerable discretion in how they implement the HIPAA security standards. Each standard is accompanied by one or more implementation specifications. Some implementation specifications are required; for example, to meet the security management standard, each organization must conduct an accurate and thorough data risk assessment. Other implementation specifications are "addressable." Organizations must assess each addressable specification to determine if it is "a reasonable and appropriate safeguard in its environment" before deciding whether to adopt it. Encryption is one of the addressable measures. Entities that choose not to use encryption must document the reasons and implement an "equivalent alternative measure if reasonable and appropriate."

The Anthem breach calls into question whether health care payers and providers should be permitted such latitude in implementing the HIPAA security standards versus a more prescriptive, mandatory approach.

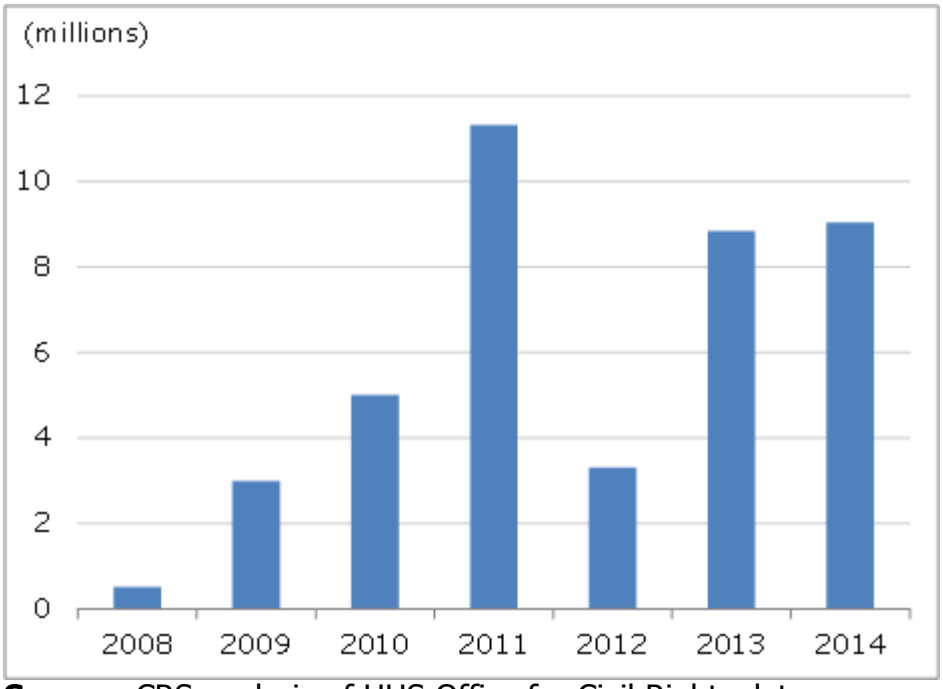
Since 2009, HIPAA-covered entities—payers and providers of health care and their business associates—must notify all individuals affected by a breach of unsecured (i.e., unencrypted) health data. The law

created an exemption for entities that secure their data through encryption in an effort to encourage the practice.

Any breach affecting 500 or more individuals must be reported to the Secretary of Health and Human Services (HHS) within 60 days of its discovery. Entities can maintain a log of smaller breaches and submit the log to HHS annually. The HHS Office for Civil Rights, which administers and enforces the HIPAA privacy and security standards, is waiting for Anthem's breach report before beginning an investigation. In the meantime, the FBI has launched its own investigation.

OCR is required to maintain a website listing all the major breaches affecting 500 or more individuals. A total of 1,141 breaches are listed affecting more than 41 million individuals (see **Figure 1**), making the Anthem breach potentially twice as large as all previous reported incidents.

Figure 1. Number of Persons Affected by Health Information Breaches



Source: CRS analysis of HHS Office for Civil Rights data (accessed February 17, 2015), https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Digital security experts predict that data breaches in the health care sector are likely to get larger and become more frequent. They think hackers may be turning toward the health sector as retail companies improve their security after recent breaches at Target and Home Depot involving tens of millions of customers. Also, medical information fetches higher prices than credit card numbers, which can quickly be deactivated.

Medical identity theft is on the increase. It occurs when someone uses an individual's name and personal identity to receive medical services and prescription drugs fraudulently, including attempts to submit fraudulent insurance claims. This trend is happening at a time when the federal government is spending billions of dollars to promote electronic health records and the exchange of digital health information. A new report finds that almost 500,000 people in 2014 were victims of medical identity theft, up 22% from the previous year. Unlike credit card fraud, victims of medical identity theft often pay significant amounts—an average of $13,500 in 2014—to resolve the crime. They may end up paying health care providers or insurers for services obtained deceitfully by others.

Some experts question whether the incentives are sufficiently strong for health insurers to improve digital security. A highly publicized data breach at a large retailer can have an immediate financial impact as customers take their business elsewhere. But health insurers may not be subject to the same

level of risk. Most individuals receive health insurance through their employers who have long-term contracts with insurers that may be difficult to break unless there is clear evidence of wrong-doing by the insurer. Moreover, it is not the employers but the employees who generally are affected by breaches.

Adam Salazar, Research Assistant, provided assistance with this Insight and prepared Figure 1.