Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

September 19, 2016

Digital Health Information and the Threat of Cyberattack

The number of cyberattacks targeting sensitive health information maintained by health care providers and health plans has increased significantly in the past two years. This trend is raising concerns about the vulnerability of electronic health data. Cybersecurity experts predict that the number of cyberattacks involving health information will continue to grow because the data are so valuable.

Health information often contains a rich set of personal identifiers. These can be used to create false identities for various illegal purposes, including submitting fraudulent insurance claims. Stolen health data fetches higher prices than stolen credit card numbers, which can be quickly deactivated.

Health care cybersecurity involves more than just safeguarding patient data from medical identity theft. Many hackers are now using ransomware to attack hospitals and other health care facilities in an effort to extort money by disrupting their daily operations. Ransomware is a type of malicious software that prevents the victim from accessing their data—usually by encrypting the data using a key known only to the hacker—until a ransom is paid. By denying a health care facility access to its own data, ransomware attacks may put patients' lives at risk.

Health care facilities also are concerned about the cybersecurity of medical devices used to monitor and support patients. Increasingly, such devices are connected to the Internet and other networks.

Health care providers and health plans that handle health information in electronic form (as opposed to paper-based records) are subject to the Health Insurance Portability and Accountability Act (HIPAA) security standards. Information security experts question whether the HIPAA security standards are sufficiently protective of electronic health data. They argue that the standards fail to address modern cybersecurity challenges.

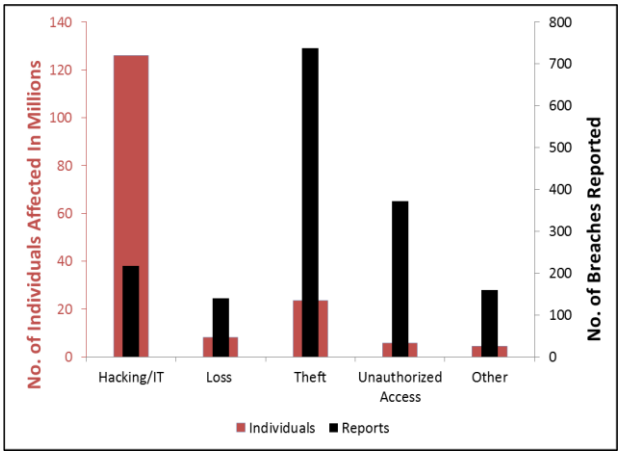
The HIPAA standards are administered and enforced by the Office for Civil Rights (OCR) within the Department of Health and Human Services (HHS). OCR is working with other HHS agencies to provide guidance and compliance tools for HIPAA-covered entities.

Millions Affected by Health Care Cyberattacks

Any breach of unsecured health information affecting 500 or more individuals must be reported to OCR. A breach is the "acquisition, access, use, or disclosure of protected health information in a manner not permitted under the [HIPAA privacy standards] which compromises [its] security or privacy." Information is unsecured if "it is not rendered unusable, unreadable, or indecipherable to unauthorized persons," for example, by using encryption.

Figure 1 shows the cumulative number of breaches reported and number of individuals affected, by type of breach, since reporting began in October 2009.

Figure 1. Breaches of HIPAA-Protected Health Data



Source: CRS analysis of HHS/OCR data through August 24, 2016.

To date, almost half of all reported breaches have been the result of *theft*—either theft of equipment and devices (e.g., servers, laptops, flash drives) that store electronic health information, or theft of paper records. Breaches due to theft account for 738 (45%) of the total of 1,627 reported breaches. However, these incidents have affected only about 24 million (14%) of the more than 167 million individuals who have been affected by all types of reported breaches.

By comparison, breaches due to a *hacking/IT* incident (i.e., cyberattack)—in which electronic health information is impermissibly accessed through technical intrusion using malicious software to attack or penetrate a system—represent a relatively small percentage of reported breaches. But some of these cyberattacks have affected millions of individuals, far more than other types of breaches. Altogether, the 217 hacking/IT incidents (13%) have affected almost 126 million individuals, or about 75% of the total number of affected individuals.

Breaches also occur as a result of *loss* of equipment or paper records, *unauthorized access* to (and disclosure of) health information that does not involve technical intrusion, as well as by *other* means (e.g., improper disposal).

The cumulative data on hacking/IT incidents mask an important trend. A majority of these incidents were reported in the past two years. During the same period, the number of reports of some of the other types of breaches (e.g., theft, loss, improper disposal) has been declining.

HIPAA Security Standards Under Scrutiny

The stated purpose of the HIPAA security standards is to ensure the confidentiality, integrity, and availability of electronic health information; prevent its unauthorized use and disclosure; and protect it from reasonably anticipated security threats, including cyberattacks. The standards were issued in 2003 and have not been modified since.

Health care entities have considerable discretion in how they implement the 18 separate standards, which cover such areas as security management, security incident procedures, access controls, and data transmission security.

Each security standard is accompanied by one or more implementation specifications. Some of these are required. To meet the security management standard, for example, each covered entity must conduct an accurate and thorough security risk analysis to identify potential threats and vulnerabilities. This is the first and most important step that needs to be taken, as it forms the foundation upon which all subsequent HIPAA security activities are based.

Other implementation specifications are addressable, allowing the entity to implement equivalent alternative measures if reasonable and appropriate.

The standards are designed to be flexible and scalable, as they must apply to entities ranging from the largest health care organization to the smallest provider practice. When implementing the standards, each entity must take into account its size and complexity, its technical infrastructure and capabilities, the security risks and vulnerabilities that it faces, and implementation costs. Moreover, the standards are technology neutral, allowing entities to take advantage of the continual emergence of new technologies.

The HIPAA security standards face growing criticism. Health care providers complain that the standards are not sufficiently prescriptive. Each standard describes what to do but not how to do it. For example, each entity must implement a security training and awareness program for its workforce. But there are no specific instructions about the content and frequency of such programs. In light of recent cyberattacks, some information security experts question whether heath care payers and providers should be given so much latitude in implementing the HIPAA standards versus having to meet a more prescribed set of requirements.

Other experts argue that the standards do not capture the realities of today's digital technology and fail to address modern cybersecurity challenges. While recognizing that HIPAA's one-size-fits-all approach provides a basic road map for organizations with little or no information security experience, they maintain that the standards have not kept pace with cyber technology. For example, the standards say nothing about malware and ransomware, intrusion detection, or specific cyber incident responses.

New Focus on Medical Device Cybersecurity

Medical devices are often connected to networks to facilitate patient care. Networked devices, like other networked computer systems, incorporate software that can make them vulnerable to cyberattack.

Large hospitals, which may have thousands of networked devices running on multiple software platforms, are especially concerned about device cybersecurity. A dozen hospitals recently volunteered to participate in a test in which cybersecurity experts attempted and were able to hack into and control patient monitors and ventilators. The hackers also triggered false alarms, which under normal circumstances might have prompted doctors and nurses to administer unnecessary or adverse treatments.

Hospital officials complain that medical device manufacturers are not taking sufficient steps to address cybersecurity and, instead, are shifting that responsibility to those who purchase and use their products. Many health care providers would like to see the Food and Drug Administration (FDA) make cybersecurity a requirement for premarket approval of new medical devices.

In 2014, FDA issued nonbinding guidance on medical device cybersecurity. As part of the required process of software validation and risk analysis, the agency recommended that manufacturers also address cybersecurity and incorporate appropriate controls during the design and development of new (and upgraded) devices.

Earlier this year, FDA sought public comment on draft guidance for managing the cybersecurity of marketed medical devices. It recommended that device manufacturers monitor, identify, and respond to cybersecurity vulnerabilities and cyberattacks throughout a product's life cycle. FDA emphasized that cybersecurity is the collective responsibility of all stakeholders and encouraged cybersecurity information sharing and collaboration.

Congress Acts on Health Care Cybersecurity

The Cybersecurity Act of 2015, enacted last December (P.L. 114-113, Division N), included three sets of provisions aimed specifically at the health care sector. First, it instructed the HHS Secretary, by December 2016, to report to Congress on the preparedness of the department and the health care industry to respond to cyberattacks.

Second, the law established a Health Care Industry Cybersecurity Task Force and instructed it to (1) analyze how other industries are addressing cybersecurity threats; (2) examine the challenges that the health care industry faces in resisting cyberattacks, including securing networked medical devices; and (3) provide the Secretary with information for public dissemination on improving cybersecurity preparedness and response. The task force is expected to report its findings and recommendations to Congress by April 2017.

Finally, the law required the Secretary to oversee the development of a common set of voluntary, consensus-based, industry-led guidelines and best practices for reducing the cybersecurity risks faced by health care organizations.

C. Stephen Redhead, Specialist in Health Policy

IF10473

Disclaimer