Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated January 30, 2015

Cyber Laws: Healthcare Information Technology (HIT)

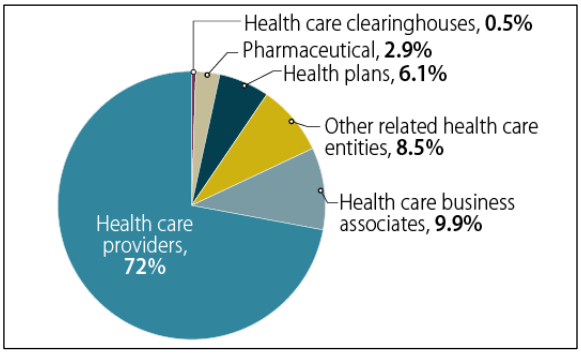
The federal government has undertaken several initiatives to promote healthcare information technology (HIT), which involves the exchange of health information in an electronic environment. Many are increasingly concerned about the protection of healthcare information and technology from cyberattacks.

"Some 94 percent of medical institutions said their organizations have been victims of a cyber attack, according to the Ponemon Institute. Now, with the push to digitize all health care records, the emergence of HealthCare.gov and an outpouring of electronic protected health information (ePHI) being exchanged online, even more attack surfaces are being exposed in the health care field." SANS Institute, SANS Health Care Cyberthreat Report 2, Feb. 2014.

Forbes Magazine, http://www.forbes.com/sites/danmunro/2014/12/21/the-top-u-s-healthcare-story-for-2014-cybersecurity/, selected cybersecurity as the top U.S. healthcare story for 2014 because of:

- The SANS healthcare cyberthreat report, which characterized the data as alarming, confirmed the industry's vulnerability, and revealed that the industry was far behind in cybersecurity.
- The FBI Private Industry Notification (PIN) to the healthcare industry, which warned healthcare providers that their cybersecurity systems are lax compared with other sectors.
- The breach of 4.5 million health records at Community Health Systems—the second largest U.S. hospital chain.
- The Sony Pictures breach—which included detailed employee, spouse and dependent medical information.

Figure 1. Categories in Healthcare Compromised



Source: CRS prepared chart. Data from SANS Institute, SANS Health Care Cyberthreat Report, Feb. 2014, http://pages.norse-corp.com/rs/norse/images/Norse-SANS-Healthcare-Cyberthreat-Report2014.pdf.

Laws to Promote HIT

What began in 1996 with Congress's passage of the Health Insurance Portability and Accountability Act (HIPAA) to facilitate the development of a health information system. This was followed in 2004 by President Bush's initiative to make electronic health records (EHRs) available to most Americans within 10 years and the signing of the American Recovery and Reinvestment Act of 2009 (ARRA) by President Obama, which authorized $22 billion for HIT efforts. Included in ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which promotes health information technology through codification of the role of the Office of the National Coordinator for Health Information Technology (ONCHIT); adoption of standards for health information technology; creation of grants and loan programs to promote wider HIT use among health care practitioners; and expansion of privacy and security requirements for protected health information. The HITECH Act also includes financial incentives for Medicare and Medicaid health care providers who make meaningful use of electronic health records.

HealthCare.gov: Privacy and Security

HealthCare.gov was created by the Patient Protection and Affordable Care Act (ACA; P.L. 111-148, as amended) to help individuals purchase health insurance. HealthCare.gov is the federal "Data Services Hub," which collects voluntarily submitted, personally identifiable information (PII) from consumers; routes the applicant's PII to federal agencies for verification; and shares the PII with the state Exchanges, health plans, and state and local agencies for enrollment. The Hub connects to existing federal and state databases, using computer matching programs, to verify identity, citizenship, income, family size, immigration status, incarceration, and minimum essential coverage.

The ACA Privacy and Security Rule provides that, where the Exchange creates or collects PII for eligibility determinations, the Exchange may only use or disclose such PII to the extent necessary to carry out an Exchange function. An Exchange is not permitted to create, collect, or disclose PII for authorized functions unless the creation, collection, use, or disclosure is consistent with ACA's privacy and security standard. Other privacy and security laws and regulations applicable to HealthCare.gov provide as follows:

- The Privacy Act governs the means by which federal agencies and their contractors collect, maintain, use, and disclose PII in a system of records. 5 U.S.C. § 552a.
- The Health Insurance Exchanges (HIX) system of records notice (SORN) regulates the collection, creation, use and disclosure of PII on individuals who apply for

eligibility determinations, and the performance of Exchange functions. 78 Fed. Reg. 8538.

- The ACA Privacy and Security Rule for Health Exchanges includes standards to safeguard PII collected, used, and disclosed by Healthcare.gov and the state health Exchanges; and require the Exchanges to implement privacy and security policies., 45 C.F.R. Part 155. For example, the DC Health Benefit Exchange Authority ("Authority"), http://hbx.dc.gov/, has adopted privacy and security policies.
- The E-Government Act requires federal agencies to conduct Privacy Impact Assessments (PIA) prior to sharing PII. P.L. 107-347.
- Federal agencies and their contractors must adhere to the Federal Information Security Management Act (FISMA) in developing, documenting, and implementing programs to provide security for federal government information and information systems. 44 U.S.C. Chapter 35, Subchapters II and III.
- Exchanges and their contractors must adhere to the taxpayer privacy and data safeguard requirements of the Internal Revenue Code, 26 U.S.C. § 6103.

At its launch, HealthCare.gov was heavily criticized for its security flaws. Recently, it has come under renewed criticism for sharing sensitive personal information with private companies that specialize in advertising and data analysis. More than 50 companies are reported to have gained access to the personal information of millions. HealthCare.gov's privacy policies state that "no personally identifiable information" is collected by third-party web measurement tools. In response, HHS announced that it would launch a review of its privacy policies, contracts for third-party tools and URL construction.

HIPAA Privacy, Security, and Breach Notification Rules, 45 C.F.R. Part 160

The HIPAA Privacy Rule. HHS issued the final Privacy Rule on April 14, 2003, applicable to health plans, health care clearinghouses, and health care providers who transmit financial and administrative transactions electronically. The rule regulates protected health information (PHI) that is "individually identifiable health information" transmitted by or maintained in electronic, paper, or any other medium.

The HIPAA Privacy Rule limits the circumstances under which an individual's protected health information may be used or disclosed by covered entities. A covered entity is permitted to use or disclose protected health information without patient authorization for treatment, payment, or health care operations. For other purposes, a covered entity may only use or disclose PHI with patient authorization subject to certain exceptions. Exceptions permit the use or disclosure of PHI without patient authorization or prior agreement for public health, judicial, law enforcement, and other specialized purposes.

The HIPAA Security Rule. HIPAA also required adoption of a national security standard for the protection of individually identifiable health information. HHS issued the HIPAA Security Rule in 2003. The Security Rule applies only to protected health information in electronic form (EPHI), and requires a covered entity to ensure the confidentiality, integrity, and availability of all EPHI the covered entity creates, receives, maintains, or transmits. Covered entities must protect against any reasonably anticipated threats or hazards to the security or integrity of such information and any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule and ensure compliance by their workforces. The Centers for Medicare and Medicaid Services (CMS) has been delegated authority to enforce the HIPAA Security Rule. The Security Rule establishes "standards" that covered entities must meet, accompanied by implementation specifications for each standard. The Security Rule identifies three categories of standards: administrative, physical, and technical.

Notice of Unauthorized Disclosure of PHI. The HITECH Act requires a covered entity to notify affected individuals when it discovers that their unsecured PHI (defined in HHS guidance) has been, or is reasonably believed to have been, breached. This requirement applies to covered entities that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information. The scope of notification is dependent upon the number of individuals involved. The Secretary of HHS must be notified, and must list on the website covered entities with breaches involving more than 500 individuals. Generally, notice must be given without unreasonable delay, but no later than 60 days after the breach is discovered. Delayed notification is permitted for law enforcement purposes if notice would impede a criminal investigation or cause damage to national security. Notification of a breach must include a description of what occurred; the types of information involved; steps individuals should take; what the covered entity is doing to investigate, mitigate, and protect against further harm; and contact information. Annually, the Secretary is required to submit a report to Congress on the breaches and actions.

Notice of Unauthorized Disclosure of PHRs. The HITECH Act also includes a breach notification requirement for personal health records (PHR) vendors, service providers to PHR vendors, and PHR servicers that are not covered entities or business associates. These entities are required to notify citizens and residents of the United States whose unsecured "PHR identifiable health information" has been, or is believed to have been, breached. Covered entities are also required to notify the Federal Trade Commission (FTC). The requirements regarding notifications are identical to the requirements applicable to breaches of unsecured PHI.

Gina Stevens, Legislative Attorney

IF10114

Disclaimer