Data Security Breach Notification Laws

Gina Stevens
Legislative Attorney

April 10, 2012

Congressional Research Service
7-5700
www.crs.gov
R42475

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

A data security breach occurs when there is a loss or theft of, or other unauthorized access to, sensitive personally identifiable information that could result in the potential compromise of the confidentiality or integrity of data. Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have laws requiring notification of security breaches involving personal information. Federal statutes, regulations, and a memorandum for federal departments and agencies require certain sectors (healthcare, financial, federal public sector, and the Department of Veterans Affairs) to implement information security programs and provide notification of security breaches of personal information. In response to such notification laws, over 2,676 data breaches and computer intrusions involving 535 million records containing sensitive personal information have been disclosed by data brokers, businesses, retailers, educational institutions, government and military agencies, healthcare providers, financial institutions, nonprofit organizations, utility companies, and Internet businesses. As a result, a significantly large number of individuals have received notices that their personally identifiable information has been improperly disclosed.

This report provides an overview of state security breach notification laws applicable to entities that collect, maintain, own, possess, or license personal information. The report describes information security and security breach notification requirements in the Office of Management and Budget's "Breach Notification Policy," the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the Gramm-Leach-Bliley Act (GLBA).

The Senate Judiciary Committee marked up three data security bills and reported the three bills with substitute amendments. See CRS Report R42474, *Selected Federal Data Security Breach Legislation*, by Kathleen Ann Ruane. S. 1151 (Leahy), the Personal Data Privacy and Security Act of 2011, would apply to business entities to prevent and mitigate identity theft, ensure privacy, provide notice of security breaches, and enhance criminal penalties. It would provide law enforcement assistance and other protections against security breaches, fraudulent access, and misuse of personally identifiable information. S. 1408 (Feinstein), the Data Breach Notification Act of 2011, would require federal agencies and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such information. S. 1535 (Blumenthal), the Personal Data Protection and Breach Accountability Act of 2011, would protect consumers by mitigating the vulnerability of personally identifiable information to theft through a security breach, provide notice and remedies to consumers, hold companies accountable for preventable breaches, facilitate the sharing of post-breach technical information, and enhance criminal and civil penalties and other protections against the unauthorized collection or use of personally identifiable information. The House Subcommittee on Commerce, Manufacturing and Trade marked up H.R. 2577 (Bono Mack), the SAFE Data Act, to protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a security breach. Several subcommittee Democrats objected to the bill's definition of personal information, arguing that the description is limited and does not adequately protect consumers from identity theft. The House Commerce, Manufacturing and Trade Subcommittee approved H.R. 2577 by voice vote and the measure was referred to the full committee for consideration. H.R. 1707 (Rush) and H.R. 1841 (Stearns) were also introduced to protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information and providing for nationwide notice in the event of a breach. Congress may address data security during its consideration of cybersecurity legislation.

Contents

Contacts

Data Breaches

A data breach occurs when there is a loss or theft of, or other unauthorized access to, data containing sensitive personal information that results in the potential compromise of the confidentiality or integrity of data.

The first state data security breach notification law was enacted in California in 2002. In response to state security breach notification laws enacted thereafter in numerous jurisdictions, over 2,676 data breaches and computer intrusions have been disclosed by the nation's largest data brokers, businesses, retailers, educational institutions, government and military agencies, healthcare providers, financial institutions, nonprofit organizations, utility companies, and Internet businesses.[1]

A brief chronology of significant data breaches follows. In February 2005, the data broker ChoicePoint disclosed a security breach, as required by the California Security Breach Act, involving the personal information of 163,000 persons.[2] In 2006, the personal data of 26.5 million veterans was breached when a VA employee's hard drive was stolen from his home. In 2007, the retailer TJX Companies revealed that 46.2 million credit and debit cards may have been compromised during the breach of its computer network by unauthorized individuals.[3] In 2008, the Hannaford supermarket chain revealed that approximately 4 million debit and credit card numbers were compromised when Hannaford's computer systems were illegally accessed while the cards were being authorized for purchase.[4] In 2009, 130 million records from credit card processor Heartland Payment Systems Inc. of Princeton, N.J., were breached. Also, in 2009, personal information from Health Net on almost half a million Connecticut residents and 1.5 million patients nationally was breached.[5] In 2011, another breach of patient data occurred when data for 20,000 emergency room patients from Stanford Hospital in California was posted on a commercial website for nearly a year.[6] In January 2012, New York State Electric & Gas and Rochester Gas and Electric, subsidiaries of Iberdrola USA, sent notices to customers advising them of unauthorized access to customer data on the companies' customer information systems,

[1] The Privacy Rights Clearinghouse reports that as of September 11, 2011 over 2,676 data breaches were made public since 2005 involving 535 million records containing sensitive personal information. Privacy Rights Clearinghouse, Chronology of Data Breaches Security Breaches 2005 – Present, at http://www.privacyrights.org/data-breach.

[2] United States v. ChoicePoint, Inc., No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006), http://www.ftc.gov/os/caselist/choicepoint/stipfinaljudgement.pdf (stipulated order imposing $15 million judgment); United States v. ChoicePoint, Inc., No. 1:06-CV-0198-JTC (N.D. Ga. Oct. 14, 2009), http://www.ftc.gov/os/caselist/choicepoint/100902choicepointstip.pdf (stipulated order imposing additional $275,000 civil penalty).

[3] U.S. Securities and Exchange Commission, *Form 10-K Annual Report: The TJX Cos., Inc.,* http://www.sec.gov/Archives/edgar/data/109198/000095013507001906/b64407tje10vk.htm.

[4] Ross Kerber, Hannaford Case Exposes Holes In Law, Some Say "Identity Theft" Criteria Called Too Narrow, at http://www.boston.com/business/articles/2008/03/30/hannaford_case_exposes_holes_in_law_some_say/?page=full.

[5] Former Connecticut Attorney General Richard Blumenthal sued Health Net of Connecticut for failing to secure private patient medical records and financial information involving 446,000 Connecticut enrollees and 1.5 million consumers nationwide and promptly notify consumers exposed by the security breach. Connecticut Attorney General's Office, Press Release: Attorney General Announces Health Net Settlement Involving Massive Security Breach Compromising Private Medical and Financial Info, July 6, 2010 at http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=462754.

[6] Kevin Sack, "Patient Data Posted Online in Major Breach of Privacy, *The N.Y. Times*, Sep. 8, 2011, at http://www.nytimes.com/2011/09/09/us/09breach.html?pagewanted=all.

which contained Social Security numbers, dates of birth, and financial institution account numbers.[7]

Data breaches are caused by computer hacking, malware, payment card fraud, employee insider breach, physical loss of non-electronic records and portable devices, and inadvertent exposure of confidential data on websites or in e-mail. Data breaches are expensive, time consuming, and can damage a company's reputation.[8] U.S. companies are reportedly reticent about buying cyber liability insurance even though data breaches have cost companies millions of dollars.[9] Data breaches involving sensitive personal information may also result in identity theft and financial crimes (e.g., credit card fraud, phone or utilities fraud, bank fraud, mortgage fraud, employment-related fraud, government documents or benefits fraud, loan fraud, and health-care fraud). Identity theft involves the misuse of any individually identifying information to commit a violation of federal or state law. With continued media reports of data security breaches, concerns about identity theft are widespread.[10]

Cloud computing[11] also poses particular data security challenges as illustrated by the 2011 Epsilon, Sony, and Amazon data breaches.[12] E-mail marketing company Epsilon announced in April 2011 that its databases had been hacked, compromising customer names and e-mail addresses for companies that outsource their marketing communications to Epsilon. E-mails concerning the breach from companies including Citibank, Chase, Capital One, Walgreens, Target, Best Buy, TiVo, TD Ameritrade, Verizon, and Ritz Carlton were sent after Epsilon announced the data breach.[13] About 2% of Epsilon's estimated 2,500 clients were affected by the attack, which amounted to millions of exposed records.

Sony announced that in April 2011 certain PlayStation Network and Qriocity service user account information was compromised in connection with an illegal and unauthorized intrusion into its network.[14]

---

[7] State of New York Public Service Commission, PSC Investigates Consumer Data Breach At NYSEG, RG&E (Jan. 23, 2012); at http://www3.dps.ny.gov/pscweb/WebFileRoom.nsf/ArticlesByCategory/1986D5ECA1917A8A8525798E005F81DD/$File/pr12007.pdf?OpenElement.

[8] Ponemon Institute, Five Countries: Cost of Data Breach, April 19, 2010, at http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf.

[9] Douglas McLeod, "A Surprising Reticence: Computer Network Risk Coverage Is Growing, But Not As Fast As One Would Expect Given The Recent Spate Of Corporate Data Breaches," CBS Interactive Business Network Resource Library (Oct. 15, 2011).

[10] According to the Federal Trade Commission (FTC), identity theft is the most common complaint from consumers in all 50 states. Between January and December 2010, the Consumer Sentinel Network (CSN), a database of consumer complaints, received more than 1.3 million consumer complaints. Identity theft tops the list accounting for 19% of the complaints. Federal Trade Commission, "Consumer Sentinel Network Data Book for January—December 2010," March 2011, at http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf. See also CRS Report R40599, *Identity Theft: Trends and Issues*, by Kristin M. Finklea.

[11] Cloud Computing is a form of computing that relies on Internet-based services and resources to provide computing services. Examples include web-based e-mail applications (Gmail) and business applications that are accessed online through a browser, instead of a local computer.

[12] "Cloud Computing's Growing Pains: Break-Ins And Breakdowns," *The Economist*, April 28, 2011, at http://www.economist.com/node/18620774/print.

[13] Elinor Mills, "Who Is Epsilon And Why Does It Have My Data?," *cnet News*, April 6, 2011, at http://news.cnet.com/8301-27080_3-20051038-245.html.

[14] Sony Computer Entertainment and Sony Network Entertainment, Sony Customer Notification US States (excluding Puerto Rico and Massachusetts), at http://us.playstation.com/news/consumeralerts/#us.

The Amazon Web Services cloud computing platform, Amazon Elastic Compute Cloud (Amazon EC2), suffered a partial failure when one of Amazon's giant server farms (the northern Virginia data center—"US-East"), whose storage and processing facilities it rents to other companies, suffered a lengthy outage.[15] Customers whose information technology was hosted by Amazon EC2 were down. These included applications like Foursquare, Formspring, HootSuite, and Reddit, among others.[16] In addition, the failure propagated across multiple "availability zones." It was also reported that Amazon permanently lost some customer data.

Litigation and enforcement actions arising from security breaches of personal information are becoming common.[17] Lawsuits seeking class action status are proceeding against retailers, credit card issuers, payment processors, and banks. The Federal Trade Commission (FTC) has brought enforcement actions,[18] along with states' attorneys general, for violations of consumer protection laws amounting to unfair practices. Consumers have sued complaining that merchants, banks, and payment processors were negligent in their failure to protect their personal information.

State Security Breach Notification Laws

The imposition of data security and security breach notification obligations on entities that own, possess, or license personal information is a recent phenomenon. California was the first jurisdiction to enact a data breach notification law in 2002, requiring notification when unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[19] There followed the emergence of numerous federal and state bills modeled after the California law imposing notification requirements on entities that own, license, or process personal information. Many states, however, included an element of harm as a trigger for notification rather than simply unauthorized acquisition. For example, under Alaska law "disclosure is not required if, after an appropriate investigation and after written notification to the attorney general of this state, the covered person determines that there is not a reasonable

[15] Amazon Elastic Compute Cloud (Amazon EC2) at http://aws.amazon.com/ec2/.

[16] Jonathan Eunice, The Cloud Backlash (Apr. 29, 2011) at http://news.cnet.com/8301-31114_3-20058674-258.html#ixzz1LPsfKptq.

[17] Picanso, Kathryn E. , Protecting Information Security Under A Uniform Data Breach Notification Law, 75 Fordham L. Rev. 355 2006-2007. This Note examines state and federal responses to information security issues and suggests a framework for legislation. Part I discusses the problems posed by poor information security, describes current federal and state efforts to secure information networks and disclose any breaches, and comments on the relationship between state and federal laws. Part II considers potential judicial and statutory approaches to protecting data security at the federal and state level and examines state litigation and analyzes issues confronting plaintiffs who seek to recover damages under a negligence theory. Federal proposals for a uniform data security and breach law are also considered, along with their potential impact on current state models. Finally, Part III concludes with a recommendation for a regulatory framework that addresses the concerns for uniform data security regulations while maintaining the consumer protections guaranteed under state legislation.

[18] See A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Dec. 1, 2010), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[19] The California Security Breach Notification Act requires a state agency, or any person or business that owns or licenses computerized data that include personal information, to disclose any breach of security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Exemptions are provided for encrypted information, for criminal investigations by law enforcement, and for breaches that are either immaterial or not "reasonably likely to subject the customers to unauthorized disclosure of personal information." Cal. Civil Code §1798.29, 1798.80-1789.84.

likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach."[20]

The majority of states have enacted laws requiring notice of security breaches of personal data.[21] As of January 2012, 46 states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted laws requiring notification of security breaches involving personal information.[22] According to the National Conference of State Legislatures, in 2011 at least 14 states introduced legislation expanding the scope of laws, setting additional requirements related to notification, or changing penalties for those responsible for breaches. Several states have reportedly considered legislation to hold retailers liable for third-party companies' costs arising from data breaches.[23]

The Massachusetts security breach and data destruction law and security regulations[24] are considered to "constitute one of the most comprehensive sets of general security regulations yet seen at the state level.... [And] are clearly modeled after aspects of developing data security law at the federal level."[25] Alabama, Kentucky, New Mexico, and South Dakota do not have security breach notification laws. In September 2012, when the amended Texas breach notification law goes into effect, breach notification obligations will exist in all states because Texas will then require entities doing business within the state to provide notification of data breaches to residents of states that have not enacted their own breach notification law.[26] Thus, breach notification

[20] Alaska Stat. §45.48.010.

[21] Alaska Stat. §45.48.010 et seq.; Ariz. Rev. Stat. §44-7501; Ark. Code §4-110-101 et seq.; Cal. Civ. Code §§56.06, 1785.11.2, 1798.29, 1798.82; Colo. Rev. Stat. §6-1-716; Conn. Gen Stat. 36a-701(b); Del. Code tit. 6, §12B-101 et seq.; Fla. Stat. §817.5681; Ga. Code §§10-1-910, -911; Haw. Rev. Stat. §487N-2; Idaho Stat. §§28-51-104 to 28-51-107; 815 ILCS 530/1 et seq.; Ind. Code §§24-4.9 et seq., 4-1-11 et seq.; Iowa Code §715C.1; Kan. Stat. 50-7a01, 50-7a02; La. Rev. Stat. §51:3071 et seq.; Me. Rev. Stat. tit. 10 §§1347 et seq.; Md. Code, Com. Law §14-3501 et seq.; Mass. Gen. Laws §93H-1 et seq.; Mich. Comp. Laws §445.72; Minn. Stat. §§325E.61, 325E.64; Mississippi 2010 H.B. 583 (effective July 1, 2011); Mo. Rev. Stat. §407.1500; Mont. Code §§30-14-1704, 2-6-504; Neb. Rev. Stat. §§87-801, -802, -803, -804, -805, -806, -807; Nev. Rev. Stat. 603A.010 et seq.; N.H. Rev. Stat. §§359-C:19, -C:20, -C:21; N.J. Stat. 56:8-163; N.Y. Gen. Bus. Law §899-aa; N.C. Gen. Stat §75-65; N.D. Cent. Code §51-30-01 et seq.; Ohio Rev. Code §§1347.12, 1349.19, 1349.191, 1349.192; Okla. Stat. §74-3113.1 and §24-161 to -166; Oregon Rev. Stat. §646A.600 et seq.; 73 Pa. Stat. §2303; R.I. Gen. Laws §11-49.2-1 et seq.; S.C. Code §39-1-90; Tenn. Code §47-18-2107, 2010 S.B. 2793; Tex. Bus. & Com. Code §521.03; Utah Code §§13-44-101, -102, -201, -202, -310; Vt. Stat. tit. 9 §2430 et seq.; Va. Code §18.2-186.6, §32.1-127.1:05 (effective January 1, 2011); Wash. Rev. Code §19.255.010, 42.56.590; W.V. Code §§46A-2A-101 et seq.; Wis. Stat. §134.98 et seq.; Wyo. Stat. §40-12-501 to -502; D.C. Code §28- 3851 et seq.; 10 Laws of Puerto Rico §4051 et. seq.; V.I. Code §2208. See State Security Breach Notification Laws, Nat'l Conference Of State Legislatures, http://www.ncsl.org/issues-research/telecommunications-information-technology/security-breach-notification-laws.aspx (last updated Oct. 12, 2010).

[22] The Commercial Law League of America, State Data Security / Breach Notification Laws (As of December 2011), at http://www.clla.org/. Click "Resources," Click "Data Breach Notification Laws By State."

[23] California, Connecticut, Illinois, Massachusetts, Minnesota, New Jersey, Texas, and Wisconsin.

[24] 201 CMR 17.00 *et seq*. The Massachusetts regulations require "all persons that own, license, store or maintain personal information about a resident of Massachusetts" to protect the security and confidentiality of personal information about residents and require companies to implement a comprehensive written information security program (based on listed requirements) and to deploy security safeguards (encryption). By March 1, organizations holding the personal information of Massachusetts residents (including customers, employees and others, regardless of which state the data is stored in) must amend their vendor contracts to require compliance. 201 CMR 17.03(f)(2

[25] Smedinghoff, Thomas J. , "New State Regulations Signal Significant Expansion Of Corporate Data Security Obligations," *BNA Privacy & Security Law Report*, October 20, 2008, at http://www.wildman.com/article/New_State_Regulations_Signal_Significant_Expansion.pdf.

[26] Kristen J. Mathews, Proskauer Privacy Law Blog: Breach Notification Obligations In All 50 States?, at http://privacylaw.proskauer.com/2011/08/articles/security-breach-notification-l/breach-notification-obligations-in-all-50-states/.

obligations will exist in all states because Texas's consumer notification obligations will apply not only to residents of Texas, but also to residents of states that don't have security breach notice requirements.[27]

Variations in state security breach notification law have been described as "so numerous that it is virtually impossible to convert these state laws into the more manageable format of fifty-state surveys."[28] Because states have different requirements, businesses engaged in interstate commerce are confronted with compliance challenges and cite the lack of uniformity as justification for a national security breach notification standard. State security breach notification laws have been criticized for creating "a fragmented, incoherent liability scheme."[29]

> The nature of any causal connection between security breaches and concrete harms suffered by consumers such as identity theft remains unclear. Because American consumers are not protected by a general right of information privacy, mere notice that a security breach has occurred is not associated with any right to compensation. Attempts to establish a right to damages following receipt of a security breach notice through class action lawsuits have generally only succeeded in clarifying the degree to which no such right exists, although many businesses suffering breaches have chosen on a voluntary basis to provide their customers with credit monitoring services to reduce the risk of harm from identity theft.[30]

Proponents of state security breach notification laws believe that state laboratories can provide stronger protection for sensitive personal information.[31]

Elements of Security Breach Notification Laws

State security breach notification laws generally follow a similar framework and can be categorized into several standard elements: (1) delineating who must comply with the law; (2) defining the terms "personal information" and "breach of security"; (3) establishing the elements of harm that must occur, if any, for notice to be triggered; (4) adopting requirements for notice; (5) creating exemptions and safe harbors; (6) clarifying preemption and relationships to other federal laws; and (7) creating penalties, enforcement authorities, and remedies.

State security breach notification laws vary regarding who is subject to the law—covered entities include businesses, state agencies, for profits, non-profits, information brokers, or persons conducting business within the state that own, license, or maintain the personal information of state residents. Twenty-nine states impose similar duties for the public and private sectors, 14 states do not, and Oklahoma's law applies only to the public sector.[32] State security breach notification laws generally apply to electronic or computerized data.

---

[27] Tex. Bus. & Com. Code 521.03.

[28] Tom, Jacqueline May, A Simple Compromise: The Need for a Federal Data Breach Notification Law, 84 St. John's L. Rev. 1569 (2010) The author argues that a strict federal data breach notification law would appease business and increase incentives to disclose by reducing compliance costs and compliance risks.

[29] Winn, Jane K., Are "Better" Security Breach Notification Laws Possible? 2-3 (June 8, 2009). Berkley Technology Law Journal, Vol. 24, 2009. Available at SSRN: http://ssrn.com/abstract=1416222.

[30] *Id.*

[31] U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, *The Threat Of Data Theft To American Consumers*, Hearing, 112th Cong., 1st sess., May 4, 2011, S. Hrg. 112–44 (Washington: GPO, 2011), p. 60.

[32] Kristen J. Mathews, Proskauer Privacy Law Blog: Breach Notification Obligations In All 50 States?, at
(continued...)

Security breach notification laws typically include definitions for "personal information" or "personally identifiable information." In information privacy law, there is no uniform definition of "personally identifiable information."[33] A common definition includes an individual's first name or initial and last name combined with SSN; driver's license or state ID number; account number, credit or debit card number, combined with any required information that allows access to account or any other financial information. A few states include medical information and/or health insurance information. Many states exclude from the definition of personal information any publicly available information that is lawfully made available to the general public from federal, state, or local government records. The term "sensitive personally identifiable information" is a subset of personally identifiable information (PII), the meaning of which also varies, but typically includes any information about an individual (including education, financial transactions, medical history, and criminal or employment history) along with information that can be used to distinguish or trace the individual's identity (including name, address, or telephone number; date and place of birth; mother's maiden name; Social Security number or other government-issued unique identification number; biometric data; or unique account identifiers).

The standard definition for "breach of security" is unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity.

In some states, the standard trigger for notice is the unauthorized access and acquisition of personal information. Some states require a risk of harm assessment to determine the level of harm or the risk of misuse involved. The results of the risk assessment determine whether notice is required.

State security breach notification laws describe who must provide notice (some require third-party service providers to notify the owner or licensor of the data when a breach occurs); recipients of notification (individuals, consumer reporting agencies for large scale breaches, state attorneys general); timing (following discovery or following unauthorized access, promptly, without unreasonable delay); methods (written, mail, email, substitute, mass media); content of notice; and delayed notification for law enforcement or national security purposes.

Many states provide a safe harbor for entities that are regulated under the Gramm-Leach-Bliley Act (GLBA) or the Health Insurance Portability and Accountability Act (HIPAA) and accompanying regulations and guidance. The safe harbor is generally available to entities that are in compliance with those laws, rules, regulations, or guidelines.

(...continued)

http://privacylaw.proskauer.com/2011/08/articles/security-breach-notification-l/breach-notification-obligations-in-all-50-states/.

[33] Schwartz, Paul M. and Solove, Daniel J., The PII Problem: Privacy and a New Concept of Personally Identifiable Information (December 05, 2011). New York University Law Review, Vol. 86, p. 1814, 2011. Available at SSRN: http://ssrn.com/abstract=1909366. ("Personally identifiable information (PII) is one of the most central concepts in information privacy regulation. The scope of privacy laws typically turns on whether PII is involved. The basic assumption behind the applicable laws is that if PII is not involved, then there can be no privacy harm. At the same time, there is no uniform definition of PII in information privacy law. Moreover, computer science has shown that in many circumstances non-PII can be linked to individuals, and that de-identified data can be re-identified.")

Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands exempt encrypted information from notification requirements.[34]

Thirteen states, the District of Columbia, and Puerto Rico permit an individual to bring a private right of action to recover damages and/or obtain equitable relief from businesses for injuries from the breach, for failure to notify customers of a security breach in a timely manner, or under state consumer protection statutes (e.g., unfair or deceptive practices).[35] In some cases, prevailing plaintiffs are permitted to recover reasonable attorneys fees and court costs. Some permit the state attorney general to bring an action; other states only allow attorney general enforcement.[36]

Penalties may be included for failure to promptly notify customers of a security breach. Penalties vary from imposition of a civil penalty of up to $500, but not to exceed $50,000 for each state resident who was not notified; a civil penalty not to exceed $10,000 per breach; assessment of appropriate penalties and damages; $1,000 per day per breach, then up to $50,000 for each 30-day period up to 180 days not to exceed $500,000; $2,500 per violation and for any actual damages; state attorney general actions under state consumer protection laws which permit the imposition of significant fines, injunctive relief, and attorneys' fees; and identity theft penalties.

Federal Information Security and Security Breach Notification Laws

The legal and regulatory framework for the protection of personally identifiable information is complex because businesses, governments, and individuals who process data must comply with the requirements of many differing privacy, information security, and breach notification laws. No single federal law or regulation governs the security of all types of sensitive personal information. Determining which federal law, regulation, and self-regulatory guidance is applicable depends in part on the entity or sector that collected the information, and the type of information collected and regulated.[37] Under federal law, certain sectors are legally obligated to protect certain types of sensitive personal information. These obligations were created, in large part, when federal privacy and security legislation was enacted in the credit, financial services, health care, government, securities, and Internet sectors. Federal regulations were issued to implement information security programs and provide standards for security breach notice to affected persons.[38]

---

[34] See Burdon, M, Low, R and Reid, J, "If its Encrypted its Secure! The Viability of US State-based Encryption Exemptions" (Paper presented at the IEEE International Symposium on Technology and Society, University of Wollongong, 7-9 June 2010). Available at SSRN: http://ssrn.com/abstract=1697930 ("Safe harbours to notification exist if personal information is encrypted....The underlying assumption of exemptions is that encrypted personal information is secure and therefore unauthorized access does not pose a risk. However, the viability of this assumption is questionable when examined against data breaches involving encrypted information and the demanding practical requirements of effective encryption management.")

[35] Alaska, California, Louisiana, Maryland, Massachusetts, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, Tennessee, Virginia, Washington, District of Columbia, and Puerto Rico.

[36] The Commercial Law League of America, State Data Security / Breach Notification Laws (As of December 2011), at http://www.clla.org/. Click "Resources," Click "Data Breach Notification Laws By State."

[37] See CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Stevens.

[38] Smedinghoff, Thomas J. , The State of Information Security Law: A Focus on the Key Legal Trends (May 2008). Available at SSRN: http://ssrn.com/abstract=1114246 or http://dx.doi.org/10.2139/ssrn.1114246.

For example, there are federal information security requirements applicable to all federal government agencies via the Federal Information Security Management Act (FISMA)[39] and a federal information security and security breach notification law applicable to a sole federal department (Veterans Affairs).[40] Federal departments and agencies are obligated by memorandum to provide breach notification, while the Department of Veterans Affairs is statutorily obligated to do so.

Other federal laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA), require private sector entities to maintain security safeguards to ensure the confidentiality, integrity, and availability of personal information, and require notification of security breaches.[41] In the private sector, different laws apply to private sector entities engaged in different businesses (such as HIPAA, the Health Information Portability and Accountability Act, and GLBA, Gramm-Leach-Bliley Act, discussed hereinafter). This is what is commonly referred to as a sectoral approach to the protection of personal information. The Federal Trade Commission Act (the FTC Act) prohibits unfair and deceptive practices in and affecting commerce.[42] The Payment Card Industry Data Security Standards (PCI-DSS) include information security requirements for organizations that handle bank cards.[43]

---

[39] Title III of the E-Government Act of 2002, P.L. 107-347; 44 U.S.C. §3541 *et seq.*

[40] The Veterans Benefits, Health Care, and Information Technology Act of 2006, P.L. 109-461; 38 U.S.C. §§5722 *et seq*. Title IX of P.L. 109-461, the Veterans Affairs Information Security Act, requires the Department of Veterans Affairs (VA) to implement agency-wide information security procedures to protect the VA's "sensitive personal information" (SPI) and VA information systems. In the event of a "data breach" of sensitive personal information processed or maintained by the VA Secretary, the Secretary must ensure that, as soon as possible after discovery, either a non-VA entity or the VA's Inspector General conduct an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information. Based upon the risk analysis, if the Secretary determines that a reasonable risk exists of the potential misuse of sensitive personal information, the Secretary must provide credit protection services.

[41] Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information, 45 C.F.R. Part 164.400 *et seq.* (upon discovery that unsecured protected health information has been, or is reasonably believed to have been breached); Health Breach Notification Rule, 16 C.F.R.§318 ((requiring entities to provide breach notification to an individual if they have a reasonable basis to believe the data can be linked to that individual); Office of Management and Budget Memorandum M-07-16, Memorandum on "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf (requires all federal agencies to implement a breach notification policy to safeguard "personally identifiable information" in electronic systems and paper documents); The Veterans Affairs Information Security Act, Title IX of P.L. 109-461, codified at 38 U.S.C. §23 *et seq.,* 38 C.F. R. Part 75, Information Security Matters ("With respect to individuals found under this subpart by the Secretary to be subject to a reasonable risk for the potential misuse of any sensitive personal information, the Secretary will promptly provide written notification by first-class mail to the individual (or the next of kin if the individual is deceased) at the last known address of the individual."); 12 C.F.R. Part 30, App. B.— Interagency Guidelines Establishing Information Security Standards ("When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible.")

[42] 15 U.S.C. §§41-58. The Federal Trade Commission has used its Section 5 authority of the FTC Act in enforcing the Safeguard Rule of the Gramm-Leach-Bliley Act to determine whether a company's information security measures were reasonable and appropriate. The Safeguards Rule requires companies to develop a written information security plan to protect customer information.

[43] The Payment Card Industry Data Security Standards (PCI DSS) is an industry regulation developed by VISA, MasterCard, and other bank card distributors. It requires organizations that handle bank cards to conform to security standards and follow certain leveled requirements for testing and reporting. The core of the PCI DSS is a group of principles and accompanying requirements designed to build and maintain a secure network, protect cardholder data, (continued...)

Some critics say that current laws focus too closely on industry-specific uses of information rather than on protecting the privacy of individuals.[44] Others believe the sectoral approach to the protection of personal information reflects not only variations in the types of information collected (e.g., government, private sector, health, financial, etc.), but also differences in the regulatory framework for particular sectors. Others advocate a national standard for entities that maintain personal information in order to harmonize legal obligations.[45] Others distinguish between private data held by the government and private data held by others, and advocate a higher duty of care for governments with respect to sensitive personal information in the U.S. public sector and to data breaches.[46]

This section describes information security and data breach notification requirements included in the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the Health Information Technology for Economic and Clinical Health Act. Also discussed are implementing regulations, to the extent that they include data security and breach notification requirements, such as the FTC Safeguards Rule and the Information Security Interagency Guidance issued by the federal banking regulators. Because some of the federal security breach notification bills would also apply to federal agencies, we are including an overview of the Office of Management and Budget's "Breach Notification Policy" for federal agencies.

Office of Management and Budget "Breach Notification Policy" For Federal Agencies

In response to recommendations from the President's Identity Theft Task Force,[47] the Office of Management and Budget issued guidance in May 2007 for federal agencies on "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."[48] The OMB Memorandum M-07-16 requires all federal agencies to implement a breach notification policy to safeguard "personally identifiable information" by August 22, 2007, to apply to both electronic systems and paper documents.[49] To formulate their policy, agencies are directed to review

(...continued)

maintain a vulnerability management program, implement strong access control measures, monitor and test networks, and maintain an information security policy. Available at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml. Washington, Minnesota, and Nevada enacted laws incorporating all or part of the PCI DSS standard. Wash. H.B. 1149 (2010); Minn. Stat. §325E.64; Nev. Rev. Stat. Ch. 603A.

[44] Tom Zeller, Jr., *"Breach Points Up Flaws in Privacy Laws,"* N.Y. Times, Feb. 24, 2005 at A1.

[45] *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* 7, available at http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf. ("Finally, we recommend the consideration of a Federal commercial data security breach notification (SBN) law that sets national standards, addresses how to reconcile inconsistent State laws, and authorizes enforcement by State authorities....This recommendation, however, is not meant to suggest preempting of other federal security breach notification laws, including those for specific sectors, such as healthcare.")

[46] A. Michael Froomkin, "Government Data Breaches," *University of Miami Legal Studies Research Paper No. 2009-20.* Available at SSRN: http://ssrn.com/abstract=1427964.

[47] Exec. Order No. 13,402, 71 FR 27945 (2006); The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 2007 at http://www.identitytheft.gov/reports/StrategicPlan.pdf.

[48] Http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

[49] The memo defines the term "personally identifiable information" as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." *Id.*

existing privacy and security requirements, and include requirements for incident reporting and handling and external breach notification. In addition, agencies are required to develop policies concerning the responsibilities of individuals authorized to access personally identifiable information.

Attachment 1 of the OMB memorandum, *Safeguarding Against the Breach of Personally Identifiable Information*, reemphasizes agencies' responsibilities under existing law (e.g., the Privacy Act and FISMA), executive orders, regulations, and policy to safeguard personally identifiable information and train employees. New privacy and security requirements are established. Agencies are required to review holdings of all personally identifiable information to ensure that they are accurate, relevant, timely, and complete, and reduced to the minimum necessary amount. Agencies must also establish a plan to eliminate the unnecessary collection and use of Social Security numbers. Agencies must implement the following security requirements (applicable to all federal information): encrypt all data on mobile computers/devices carrying agency data; employ two-factor authentication for remote access; use a "time-out" function for remote access and mobile devices; log and verify all computer-readable data extracts from databases holding sensitive information; and ensure that individuals and supervisors with authorized access to personally identifiable information annually sign a document describing their responsibilities.[50]

Attachment 2 of the OMB Memorandum, *Incident Reporting and Handling Requirements*, applies to the breach of personally identifiable information in electronic or paper format. Agencies are required to report all incidents involving personally identifiable information within one hour of discovery/detection, and publish a "routine use"[51] under the Privacy Act applying to the disclosure of information to appropriate persons in the event of a data breach.[52]

Attachment 3, *External Breach Notification*, identifies the factors agencies should consider in determining when notification outside the agency should be given and the nature of the notification. Notification may not be necessary for encrypted information. Each agency is directed to establish an agency response team. Agencies must assess the likely risk of harm caused by the breach and the level of risk. Agencies should provide notification without unreasonable delay following the detection of a breach, but are permitted to delay notification for law enforcement, national security purposes, or agency needs. Attachment 3 also includes specifics as to the content of the notice, criteria for determining the method of notification, and the types of notice that may be used.

Attachment 4, *Rules and Consequences Policy*, directs each agency to develop and implement a policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow these rules. Supervisors may be subject to disciplinary action for failure to take appropriate action upon discovering the breach or failure to take required steps to prevent a breach from occurring. Rules of behavior and corrective actions should address the failure to implement and maintain security controls for personally identifiable information; exceeding authorized access to, or disclosure to unauthorized persons of, personally identifiable

[50] The first four information security requirements were adopted in an earlier memorandum, See OMB Memo 06-16, "Protection of Sensitive Agency Information" at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf.

[51] The Privacy Act defines a routine use to mean "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected." 5 U.S.C. §552a(a)(7).

[52] OMB Memorandum M-07-16, p.11.

information; failure to report any known or suspected loss of control or unauthorized disclosure of personally identifiable information; and for managers, failure to adequately instruct, train, or supervise employees in their responsibilities. Consequences may include reprimand, suspension, removal, or other actions in accordance with applicable law and agency policy.

Health Insurance Portability and Accountability Act

Part C of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[53] requires "the development of a health information system through the establishment of standards and requirements for the electronic transmission of health information."[54] These "Administrative Simplification" provisions require the Secretary of Health and Human Services to adopt national standards to facilitate the electronic exchange of information; establish code sets for data elements; protect the privacy of individually identifiable health information; maintain administrative, technical, and physical safeguards for the security of health information; provide unique health identifiers; and to adopt procedures for the use of electronic signatures.[55]

HIPAA covered entities—health plans, health care clearinghouses, and health care providers who transmit financial and administrative transactions electronically—are required to comply with the national standards and regulations.[56] Under HIPAA, the Secretary is required to impose a civil monetary penalty on any person failing to comply with the national standards and regulations.[57] The minimum civil money penalty (i.e., the fine) for a violation is $100 per violation and up to $25,000 for all violations of an identical requirement or prohibition during a calendar year.[58] The maximum civil money penalty (i.e., the fine) for a violation is $50,000 per violation and up to $1,500,000 for all violations of an identical requirement or prohibition during a calendar year.[59] HIPAA also establishes criminal penalties for any person who knowingly and in violation of the Administrative Simplification provisions of HIPAA uses a unique health identifier, or obtains or discloses individually identifiable health information.[60] Enhanced criminal penalties may be imposed if the offense is committed under false pretenses, with intent to sell the information or reap other personal gain. The penalties include a fine of not more than $50,000 and/or imprisonment of not more than one year; if the offense is under false pretenses, a fine of not more than $100,000 and/or imprisonment of not more than five years; and if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than 10 years.[61] These penalties do not affect other penalties imposed by other federal programs.

---

[53] P.L. 104-191, 110 Stat. 1936 (1996), codified in part at 42 U.S.C. §§1320d *et seq.;* see CRS Report RL33989, *Enforcement of the HIPAA Privacy and Security Rules*, by Gina Stevens.

[54] 42 U.S.C. §§1320d—1320d-8.

[55] 42 U.S.C. §§1320d-2(a)-(d).

[56] 42 U.S.C. §1320d-4(b).

[57] 42 U.S.C. §1320d-5(a).

[58] 42 U.S.C. §1320d-5(a)(1). The HITECH Act, P.L. 111-5, increased civil and criminal penalties for some HIPAA violations. See CRS Report R40546, *The Privacy and Security Provisions for Health Information in the American Recovery and Reinvestment Act of 2009*, by Gina Stevens and Edward C. Liu.

[59] 42 U.S.C. §1320d-5(a)(1).

[60] 42 U.S.C. §1320d-6.

[61] 42 U.S.C. §1320d-6(b).

HIPAA Privacy Rule

HIPAA required adoption of a national privacy standard for the protection of individually identifiable health information.[62] HHS issued final Standards for Privacy of Individually Identifiable Health Information, known as the Privacy Rule, on April 14, 2003.[63] The HIPAA Privacy Rule is applicable to health plans, health care clearinghouses, and health care providers who transmit financial and administrative transactions electronically. The rule regulates "protected health information"[64] that is "individually identifiable health information"[65] transmitted by or maintained in electronic, paper, or any other medium. The Privacy Rule requires covered entities to enter into agreements with business associates who create, receive, maintain, or transmit protected health information (PHI) on their behalf. The Office of Civil Rights (OCR) in HHS enforces the Privacy Rule.[66]

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.[67] For other purposes, a covered entity may only use or disclose PHI with patient authorization subject to certain exceptions.[68] Exceptions permit the use or disclosure of PHI without patient authorization or prior agreement for public health, judicial, law enforcement, and other specialized purposes.[69] In certain situations that would otherwise require authorization, a covered entity may use or disclose PHI without authorization provided that the individual is given the prior opportunity to object or agree.[70] The HIPAA Privacy Rule also requires a covered entity to maintain reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.[71]

HIPAA Security Rule

HIPAA also required adoption of a national security standard for the protection of individually identifiable health information.[72] 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

---

[62] "The term 'individually identifiable health information' means any information, including demographic information collected from an individual, that - (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and - (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." 42 U.S.C. §1320d(6).

[63] 45 C. F.R. Part 164 Subpart E—Privacy of Individually Identifiable Health Information.

[64] The definition of protected health information (PHI) excludes individually identifiable health information contained in certain education records and employment records held by a covered entity in its role as employer.

[65] 45 C.F.R. §160.103.

[66] 65 Fed. Reg. 82381.

[67] 45 C.F.R. §164.506.

[68] 45 C.F.R. §164.508.

[69] 45 C.F.R. §164.512(a)-(l).

[70] 45 C.F.R. §164.510.

[71] 45 C.F.R. §164.530(c).

[72] 42 U.S.C. §§1320d-2 and (d)(4).

entity creates, receives, maintains, or transmits.[73] 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.[74] The Security Rule requires covered entities to enter into agreements with business associates who create, receive, maintain, or transmit EPHI on their behalf.[75] A covered entity is not liable for violations by the business associate unless the covered entity knew that the business associate was engaged in a practice or pattern of activity that violated HIPAA, and the covered entity failed to take corrective action. The Centers for Medicare and Medicaid Services (CMS) has been delegated authority to enforce the HIPAA Security Rule.[76]

The Security Rule allows covered entities to consider such factors as the cost of a particular security measure, the size of the covered entity involved, the complexity of the approach, the technical infrastructure and other security capabilities in place, and the nature and scope of potential security risks. 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.

Health Information Technology for Economic and Clinical Health Act (HITECH Act)

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) was enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA).[77] As part of this new law, sweeping changes to the health information privacy regime were enacted. Most of the privacy provisions are additional requirements supplementing the HIPAA Privacy and Security Rules, but a few provisions deal specifically with electronic health records (EHRs).[78] The HITECH Act extended application of some provisions of the HIPAA Privacy and Security Rules to the business associates of HIPAA-covered entities, making those business associates subject to civil and criminal liability; established new limits on the use of protected health information for marketing and fundraising purposes; provided new enforcement authority for state attorneys general to bring suit in federal district court to enforce HIPAA violations; increased civil and criminal penalties for HIPAA violations; required covered entities and business associates to notify the public and HHS of data breaches; changed certain use and disclosure rules for protected health information; and created additional individual rights.

---

[73] 45 C.F.R. §164.306(a).

[74] Dep't of Health and Human Services, Security 101 for Covered Entities at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf.

[75] Under such agreements, the business associate must: implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the covered entity's electronic protected health information; ensure that its agents and subcontractors to whom it provides the information do the same; and report to the covered entity any security incident of which it becomes aware. The contract must also authorize termination if the covered entity determines that the business associate has violated a material term.

[76] HIPAA Security Standards for the Protection of Electronic Personal Health Information, 45 C.F.R. Part 164.302 – 164.318. See generally, Centers for Medicare and Medicaid Services, *Security Materials* at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.

[77] P.L. 111-5.

[78] An electronic health record is defined as "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff." P.L. 111-5, §13400(5).

Business Associates' Civil and Criminal Liability

The HITECH Act provides that covered entities' business associates that obtain or create PHI pursuant to a business associate agreement may only use or disclose that PHI in compliance with its terms.[79] The HITECH Act also requires existing business associate agreements to incorporate the new privacy provisions.[80]

Prior to the HITECH Act, covered entities have been liable for violations of the Privacy Rule that were committed by their business associates, but only if the covered entity had knowledge of "a pattern of activity or practice" of the business associate that violates the Privacy Rule.[81] Under the HITECH Act, business associates are also made liable for violations of the Privacy Rule committed by the covered entities with which they contract, if the business associates are aware of a pattern and practice of unlawful conduct by the covered entity.[82] While business associates are still not defined as covered entities under HIPAA, they are subject to the same civil and criminal penalties for improper uses or disclosures of PHI.[83]

The HITECH Act also extended application of the HIPAA Security Rule's provisions on security safeguards and documentation to business associates of covered entities, making those business associates subject to civil and criminal liability for violations of the HIPAA Security Rule.[84] Under the HIPAA Security Rule, only covered entities can be held civilly or criminally liable for violations. While business associates are still not considered covered entities under HIPAA, they are subject to the same civil and criminal penalties as a covered entity for Security Rule violations.[85] The HITECH Act also requires existing business associate agreements to incorporate the new security requirements.[86]

Unsecured Protected Health Information

The HITECH Act required the HHS Secretary to issue guidance specifying the technologies and methodologies to render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.[87] The HITECH Act also provides a definition.[88]

Guidance on the meaning of "unsecured protected health information" was issued by HHS that became effective upon issuance. It identified two methods for rendering PHI unusable, unreadable, or indecipherable: encryption and destruction (paper and electronic form). Pursuant to this guidance, "if PHI is rendered unusable, unreadable, or indecipherable to unauthorized

[79] P.L. 111-5, §13401(c).

[80] P.L. 111-5, §13404(a).

[81] 45 C.F.R. §164.504(e)(1)(ii).

[82] P.L. 111-5, §13404(b).

[83] P.L. 111-5, §§13401(b), 13404(c).

[84] P.L. 111-5, §13401. The HITECH Act adopts the same definition of business associates as the HIPAA Privacy and Security Rules. 45 C.F.R. §160.103.

[85] P.L. 111-5, §§13401(b), 13404(c).

[86] P.L. 111-5, §13404(a).

[87] P.L. 111-5, §13402(h).

[88] Under the default definition, PHI is unsecured if "it is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and that is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute."

individuals by one or more of the methods identified in this guidance, then such information is not 'unsecured' PHI." Because the HITECH Act's breach notification requirements apply only to breaches of unsecured PHI, this guidance provides the means by which covered entities and their business associates can determine whether a breach has occurred and whether notification obligations apply.[89]

Breach Notification

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) imposed breach notification requirements on covered entities, their business associates, and vendors of personal health records (PHRs).[90] The HITECH Act requires covered entities, business associates, and vendors of PHRs to notify affected individuals in the event of a "breach" of "unsecured protected health information."[91] A "breach" is defined as the "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."[92] A vendor of PHR is defined as "an entity, other than a covered entity ... that offers or maintains a personal health record."[93] The term "unsecured protected health information" means "protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance."[94]

In August 2009, the Department of Health and Human Services (HHS) issued an interim final breach notification regulation.[95] The Breach Notification Interim Final Regulation addresses notification to individuals, the media, and the Secretary, by a business associate; law enforcement delay; and administrative requirements and burdens of proof.

The HITECH Act also directed the Federal Trade Commission (FTC) to issue breach notification regulations for web-based businesses to notify consumers when the security of their electronic health information is breached.[96] The FTC rule applies to both vendors of personal health records—which provide online repositories that people can use to keep track of their health information—and entities that offer third-party applications for personal health records. It applies to breaches by vendors of PHRs, PHR-related entities, and third-party service providers that

[89] *Id.* at 15-16.

[90] A personal health record (PHR) is defined as "an electronic record of identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." P.L. 111-5, §13400(11). A vendor of PHR is defined as "an entity, other than a covered entity ... that offers or maintains a personal health record." P.L. 111-5, §13400(18).

[91] P.L. 111-5, §§13402, 13407.

[92] P.L. 111-5, §13400(1). Not included in the definition of breach are any unintentional acquisition, use, or access of PHI by an employee or other authorized individual of a covered entity or a business associate done in good faith and within the scope of employment or the relationship where such information is not breached any further; or inadvertent disclosures by authorized persons of PHI within the same facility; and information received as a result of such disclosure is not further disclosed without authorization.

[93] P.L. 111-5, §13400(18).

[94] P.L. 111-5, §13402(h).

[95] P.L. 111-5, §13402(j); Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information, 45 C.F.R. Part 164.400 *et seq.*

[96] Health Breach Notification Rule, 16 C.F.R. §318.

maintain information on U.S. citizens or residents.[97] The rule contains provisions discussing timeliness, methods of notification, content, and enforcement of the breach notification requirements.

Notice of Unauthorized Disclosure of Protected Health Information

The HITECH Act requires a covered entity to notify affected individuals when it discovers that their unsecured PHI has been, or is reasonably believed to have been, breached.[98] 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 dependant upon the number of individuals whose unsecured PHI was compromised. Generally, only written notice need be provided if less than 500 individuals are involved. For larger breaches, notice through prominent media outlets may be required. In all cases, the Secretary of HHS must be notified, although breaches involving less than 500 people may be reported on an annual basis. The Secretary of HHS is directed to display on the department's website a list of covered entities with breaches involving more than 500 individuals.[99]

Generally, notice must be given without unreasonable delay, but no later than 60 days after the breach is discovered. If a delay is not reasonable, a covered entity may still have violated this provision even if notice was given within 60 days. In an enforcement action of this provision, the covered entity has the burden of proving that any delay was reasonable. Delayed notification is permitted for law enforcement purposes if a law enforcement official determines that notice would impede a criminal investigation or cause damage to national security.

To the extent possible, notification of a breach must include a description of what occurred; the types of information involved in the breach; steps individuals should take in response to the breach; what the covered entity is doing to investigate, mitigate, and protect against further harm; and contact information to obtain additional information.

Annually, the Secretary is required to submit a report to Congress containing information on the number and nature of breaches for which notice was provided and actions taken in response to such breaches.[100]

Notice of Unauthorized Disclosure of Personal Health Records

The HITECH Act includes a breach notification requirement for PHR vendors (such as Google Health or Microsoft Vault), service providers to PHR vendors, and PHR servicers that are not covered entities or business associates that sunsets "if Congress enacts new legislation."[101] Under this breach notification requirement, these entities are required to notify citizens and residents of the United States whose unsecured "PHR identifiable health information" has been, or is believed

[97] *Id*.

[98] P.L. 111-5, §13402(a).

[99] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

[100] P.L. 111-5, §13402(i).

[101] P.L. 111-5, §13407(g)(2). For further information on electronic personal health records, *see* CRS Report RS22760, *Electronic Personal Health Records*, by Gina Stevens.

to have been, breached. PHR vendors, service providers to PHR vendors, and PHR servicers are also required to notify the Federal Trade Commission (FTC).[102]

The HITECH Act defines several terms specific to the PHR breach notification requirement. A "breach of security" is defined as the unauthorized acquisition of an individual's PHR identifiable health information.[103] PHR identifiable health information is defined as individually identifiable health information, and includes information provided by or on behalf of the individual, and information that can reasonably be used to identify the individual.[104]

The requirements regarding the scope, timing, and content of these notifications are identical to the requirements applicable to breaches of unsecured PHI. Violations of these requirements shall be considered unfair and deceptive trade practices in violation of the Federal Trade Commission Act.

Gramm-Leach-Bliley Act (GLBA)

Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA) requires financial institutions to provide customers with notice of their privacy policies and requires financial institutions to safeguard the security and confidentiality of customer information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[105] Financial institutions are defined as businesses that are engaged in certain "financial activities" described in Section 4(k) of the Bank Holding Company Act of 1956 and accompanying regulations.[106] Such activities include traditional banking, lending, and insurance functions, along with other financial activities. Financial institutions are prohibited from disclosing "nonpublic personal information"[107] to non-affiliated third parties without providing customers with a notice of privacy practices and an opportunity to opt out of the disclosure. A number of statutory exceptions are provided to this disclosure rule, including that financial

[102] The FTC is directed to also notify the Secretary of HHS in the event of a breach.

[103] P.L. 111-5, §13407(f)(1).

[104] P.L. 111-5, §13407(f)(2).

[105] 15 U.S.C. §6801 - 6809. *See* CRS Report RS20185, *Privacy Protection for Customer Financial Information*, by M. Maureen Murphy.

[106] 12 U.S.C. §1843(k).

[107] (4) Nonpublic personal information.

(A) The term "nonpublic personal information" means personally identifiable financial information—

(i) provided by a consumer to a financial institution;

(ii) resulting from any transaction with the consumer or any service performed for the consumer; or

(iii) otherwise obtained by the financial institution.

(B) Such term does not include publicly available information, as such term is defined by the regulations prescribed under section 6804 of this title.

(C) Notwithstanding subparagraph (B), such term—

(i) shall include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but

(ii) shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information. 15 U.S.C. §6809(4).

institutions are permitted to disclose nonpublic personal information to a non-affiliated third party to perform services for or functions on behalf of the financial institution.

GLBA Privacy Rule

Regulations implementing GLBA's privacy requirements published by the federal banking regulators govern the treatment of nonpublic personal information about consumers by financial institutions;[108] require a financial institution in specified circumstances to provide notice to customers about its privacy policies and practices; describe the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and provide a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to exceptions.[109]

FTC Safeguards Rule

This rule implements GLBA's requirements for entities under FTC jurisdiction. The Safeguards Rule applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services. These include, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, real estate appraisers, and professional tax preparers. The Safeguards Rule also applies to companies like credit reporting agencies and ATM operators that receive information about the customers of other financial institutions. The rule requires financial institutions to have an information security plan that "contains administrative, technical, and physical safeguards" to "insure the security and confidentiality of customer information: protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer."[110] Using its authority under the Safeguards Rule, the commission has brought a number of enforcement actions to address the failure to provide reasonable and appropriate security to protect consumer information.[111]

GLBA Information Security Guidelines

Section 501(b) of GLBA requires the banking agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards to ensure the security, confidentiality, and integrity of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

[108] 16 C.F.R. Part 13 (FTC); 12 C.F.R. Parts 40 (OCC), 216 (FRB), 332 (FDIC), 573 (OTS), and 716 (NCUA).

[109] See generally, 12 C.F.R. §225.28, §225.86.

[110] Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information, 16 C.F.R. Part 314.

[111] For information on enforcement actions the Commission has brought involving the privacy of consumer information under Section 5 of the FTC Act, see http://www.ftc.gov/privacy/privacyinitiatives/safeguards_enf.html.

Interagency Guidance issued by the federal banking regulators[112] applies to customer information, which is defined as "any record containing nonpublic personal information ... about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of" a financial institution.[113] The security guidelines direct each financial institution to assess the risks of reasonably foreseeable threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information and customer information systems; the likelihood and potential damage of threats; and the sufficiency of policies, procedures, customer information systems, and other controls. Following the assessment of risks, the security guidelines require a financial institution to manage and control the risk through the design of a program to address the identified risks; train staff to implement the program; regularly test the key controls, systems, and procedures of the information security program; and develop and maintain appropriate measures to dispose of customer information. The security guidelines also direct every financial institution to require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Each financial institution is required to monitor, evaluate, and adjust its information security program as necessary. Finally, each financial institution is required to report to its board at least annually on its information security program, compliance with the security guidelines, and issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security breaches or violations and management's responses, and recommendations for changes in the information security program.

Response Programs for Unauthorized Access to Customer Information and Customer Notice

The security guidelines recommend implementation of a risk-based response program, including customer notification procedures, to address unauthorized access to or use of customer information maintained by a financial institution or its service provider that could result in substantial harm or inconvenience to any customer, and require disclosure of a data security breach if the covered entity concludes that "misuse of its information about a customer has occurred or is reasonably possible."[114] Pursuant to the guidance, substantial harm or inconvenience is most likely to result from improper access to "sensitive customer information."[115]

---

[112] *See* 12 C.F.R. Part 30, App. B (national banks); 12 C.F.R. Part 208, App. D-2 and Part 255, App. F (state member banks and holding companies); 12 C.F.R. Part 364, App. B (state non-member banks); 12 C.F.R. Part 570, App. B (savings associations); 12 C.F.R. Part 748, App. A (credit unions).

[113] See Board of Governors Federal Reserve System, The Commercial Bank Examination Manual, Supp. 27, 984-1034 (May 2007), at http://www.federalreserve.gov/boarddocs/SupManual/cbem/200705/0705cbem.pdf.

[114] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, Part III of Supplement A to Appendix, at 12 C.F.R. Part 30 (OCC), Supplement A to Appendix D-2, at 12 C.F.R. Part 208 (Federal Reserve System), 12 C.F.R. Part 364 (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision), 70 Fed. Reg. 15736 - 15754 (March 29, 2005).

[115] "Sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number." 70 Fed. Reg. 15736-15754 (March 29, 2005).

At a minimum, an institution's response program should contain procedures for assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused; notifying its primary federal regulator when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information; consistent with the Agency's Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement authorities; taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information (e.g., by monitoring, freezing, or closing affected accounts and preserving records and other evidence); and notifying customers when warranted.

The security guidelines note that financial institutions have an affirmative duty to protect their customers' information against unauthorized access or use, and that customer notification of a security breach involving the customer's's information is a key part of that duty. The guidelines prohibit institutions from forgoing or delaying customer notification because of embarrassment or inconvenience.

The guidelines provide that when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. The institution should notify its customers as soon as notification will no longer interfere with the investigation.

If a financial institution can determine which customers' information has been improperly accessed, it may limit notification to those customers whose information it determines has been misused or is reasonably likely to be misused. In situations where the institution determines that a group of files has been accessed improperly, but is unable to identify which specific customers' information has been accessed, and the institution determines that misuse of the information is reasonably possible, it should notify all customers in the group. The guidelines also address what information should be included in the notice sent to the financial institution's customers.

Author Contact Information

Gina Stevens
Legislative Attorney
gstevens@crs.loc.gov, 7-2581