Congressional Research Service
Informing the legislative debate since 1914

HIPAA Privacy, Security, Enforcement, and Breach Notification Standards

C. Stephen Redhead
Specialist in Health Policy

April 17, 2015

Congressional Research Service
7-5700
www.crs.gov
R43991

CRS REPORT
Prepared for Members and
Committees of Congress

c11173008

Summary

The Privacy Rule, which was promulgated pursuant to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, comprises a set of federal standards governing the use of personal health information. The Privacy Rule generally applies to individually identifiable health information created and maintained by payers and providers of health care, collectively referred to as covered entities. The rule establishes certain individual rights, including the right to inspect and obtain a copy of one's health information; describes the circumstances under which covered entities are permitted to use or disclose health information; and requires covered entities to put in place administrative, physical, and technical safeguards to protect health information from unauthorized access, use, or disclosure.

Broadly speaking, the Privacy Rule prohibits a covered entity from using or disclosing "protected health information" (PHI) except as expressly permitted or, in two instances, required by the rule. The Privacy Rule describes a wide range of circumstances under which it is permissible to use or disclose PHI. In so doing, the rule seeks to preserve the discretion that health care professionals have traditionally exercised when using or disclosing patient information. For all uses or disclosures of PHI that are not otherwise permitted or required by the rule, a covered entity must obtain a patient's written authorization.

Under the Privacy Rule, covered entities generally may use or disclose PHI for the purposes of treatment, payment, and other routine health care operations. Under certain other circumstances, the rule requires covered entities to give individuals the opportunity to object to the use or disclosure of their PHI. The rule also permits the use or disclosure of PHI for various specified activities not directly connected to treatment (e.g., research, law enforcement, public health).

The Privacy Rule does not specify the types of safeguards that need to be implemented to protect PHI from misuse. That is the purpose of the companion HIPAA Security Rule, under which each of the safeguards—administrative, physician, and technical—is composed of a number of standards. The security standards are designed to be scalable to the size and complexity of the covered entity, as well as technology-neutral. They include implementing security management policies and procedures, workforce security procedures, facility access controls, and controls on access to information technology (IT) systems. Each standard consists of one or more implementation specifications (i.e., detailed instructions for implementing the standard). Covered entities have considerable discretion and flexibility in how they implement the security standards.

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 included a series of modifications to the HIPAA privacy and security standards. Many of the changes were enacted to address the concerns of privacy advocates and other stakeholders. The HITECH Act created a notification requirement for breaches of unsecured (i.e., unencrypted) PHI, increased the civil monetary penalties for violating HIPAA, and expanded and strengthened enforcement activities by the Office for Civil Rights. It also made business associates of covered entities (i.e., companies and consultants with whom covered entities share PHI to help them operate) directly liable and subject to civil and criminal penalties for HIPAA violations.

Contents

Tables

Appendixes

Contacts

Introduction to the HIPAA Administrative Simplification Standards

The Health Insurance Portability and Accountability Act (HIPAA) of 1996[1] was enacted to improve the availability and continuity of health insurance coverage; promote long-term care insurance and the use of health savings accounts; and combat waste, fraud, and abuse, particularly in Medicare and Medicaid. Many of those provisions have since been expanded and superseded by other laws, most notably by the Patient Protection and Affordable Care Act (ACA).[2]

HIPAA also included a series of requirements under the subtitle "Administrative Simplification" to promote electronic record-keeping and claims processing in the health care system and to protect the privacy of electronic health information.[3] The Secretary of Health and Human Services (HHS) was instructed to adopt electronic format and data standards for certain administrative and financial transactions that occur routinely between health care providers and payers (e.g., patient eligibility, claims processing), and list the code sets that must be used in these electronic transactions to identify specific diagnoses and clinical procedures. The Secretary also was directed to adopt unique identifiers (ID numbers) for health care providers, health plans, and employers for use in standard electronic transactions. Finally, the Secretary was required to adopt security standards—administrative, physical, and technical safeguards—to ensure the integrity and confidentiality of electronic health information and protect it against unauthorized access, use, or disclosure.

HIPAA specified that the Administrative Simplification standards apply to the following three types of entities, collectively referred to as covered entities: (1) health plans, (2) health care clearinghouses, and (3) health care providers.[4]

Health Information Privacy

At the end of the Administrative Simplification subtitle, lawmakers added language instructing the HHS Secretary to submit to Congress within 12 months of the law's enactment detailed recommendations for standards to protect the privacy of individually identifiable health information. The recommendations were to address patient privacy rights, procedures for

[1] P.L. 104-191, 110 Stat. 1936, August 21, 1996.

[2] P.L. 111-148, 124 Stat. 119, March 23, 2010, as amended.

[3] P.L. 104-191, Title II, Subtitle F, Sections 261-264. HIPAA's Administrative Simplification provisions added new sections 1171-1179 to the Social Security Act; codified at 42 U.S.C. §§1320d et seq.

[4] Section 1172(a) of the Social Security Act, 42 U.S.C. §1320d–1(a). A *health plan* is "an individual or group plan that provides, or pays the cost of, medical care." The term encompasses private and government plans. A *health care clearinghouse* is an entity (e.g., billing service) that (1) receives nonstandard health information and processes, or facilitates the processing of, the information into a standard format required for electronic transaction; or (2) receives a standard transaction and processes, or facilitates the processing of, the information into nonstandard format for the recipient. A *health care provider* is a person (e.g., physician, nurse) or entity (e.g., hospital, clinic) who "furnishes, bills, or is paid for health care in the normal course of business." For HIPAA to apply, a provider must conduct one or more HIPAA-specified standard electronic transactions. Providers who rely on third-party billing services to conduct such electronic transactions on their behalf are also covered. However, a provider who operates solely on a paper basis and does not submit insurance claims electronically is not subject to the HIPAA standards. 45 C.F.R. §160.103.

exercising those rights, and uses and disclosures of patient information that should be authorized or required. Lawmakers also included a three-year deadline for enacting health privacy legislation. If Congress and the President were unable to enact such legislation by the deadline, the Secretary was instructed by regulation to adopt privacy standards based on the recommendations. HIPAA stipulated that the standards would not preempt (i.e., supersede) state health privacy laws that are more protective of medical information.

On September 11, 1997, the Secretary submitted to Congress a framework and set of recommendations for health privacy legislation (see text box).[5] Several legislative proposals were introduced and debated, but lawmakers could not reach agreement and were unable to meet the deadline (i.e., August 21, 1999) they had set for themselves to enact legislation. Consequently, the Secretary proposed and finalized a set of health privacy standards by regulation.

Privacy of Individually Identifiable Health Information
Recommendations of the HHS Secretary, September 11, 1997

- Allow for the smooth flow of identifiable health information for treatment, payment, and related operations, and for specified additional purposes related to health care that are in the public interest.
- Prohibit the flow of identifiable information for any additional purposes, unless specifically and voluntarily authorized by the subject of the information.
- Put in place a set of fair information practices that allow individuals to know who is using their health information, and how it is being used.
- Establish fair information practices that allow individuals to obtain access to their records and request amendment of inaccurate information.
- Require persons who hold identifiable health information to safeguard that information from inappropriate use or disclosure.
- Hold those who use individually identifiable health information accountable for their handling of this information, and provide legal recourse to persons harmed by misuse.

The HIPAA Privacy Rule was published by the Clinton Administration in December 2000 and modified by the Bush Administration in August 2002.[6] The compliance deadline for most covered entities was April 14, 2003. A companion Security Rule, composed of a set of standards to safeguard health information from unauthorized access, use, or disclosure, was published in February 2003, with a compliance deadline for most covered entities of April 20, 2005.[7]

The HHS Office for Civil Rights (OCR) administers and enforces the Privacy and Security Rules. HIPAA established civil monetary penalties for failure to comply with the Administrative Simplification standards, including the privacy and security standards. It also created criminal penalties for certain instances involving the wrongful acquisition or disclosure of individually identifiable health information in violation of the standards. OCR refers such cases to the

[5] Department of Health and Human Services, Confidentiality of Individually-Identifiable Health Information: Recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996, September 11, 1997, http://aspe.hhs.gov/admnsimp/pvcrec0.htm.

[6] Department of Health and Human Services, Office of the Secretary, "Standards for Privacy of Individually Identifiable Health Information," Final rule, 65 *Federal Register* 82462, December 28, 2000; Department of Health and Human Services, Office of the Secretary, "Standards for Privacy of Individually Identifiable Health Information," Final rule, 67 *Federal Register* 53182, August 14, 2002.

[7] Department of Health and Human Services, Office of the Secretary, "Health Insurance Reform: Security Standards," Final rule, 68 *Federal Register* 8334, February 20, 2003.

Department of Justice (DOJ) for criminal prosecution. OCR maintains an extensive website with information on the HIPAA privacy and security standards, including information on compliance and enforcement activities.[8]

HHS finalized a HIPAA Enforcement Rule in February 2006. The rule addressed the investigation of noncompliance with the Administrative Simplification standards and the imposition of civil monetary penalties. It covered the investigation process, bases for liability, determination of the penalty amount, grounds for a waiver, conduct of hearings, and the appeals process.[9]

Concerns About the HIPAA Privacy and Security Standards

The Privacy and Security Rules have been contentious and the subject of ongoing debate since they were first implemented. Privacy advocates have complained about the limited scope of the rules. HIPAA applies all the Administrative Simplification standards to three entities—health plans, health care clearinghouses, and health care providers—but personal health information is handled by many other types of organizations that are not covered under the law. In an effort to address this issue, HHS took steps when it promulgated the Privacy and Security Rules to broaden their scope so that they apply to the business associates of HIPAA-covered entities. These actions were further strengthened by Congress in subsequent legislative action (discussed later in this report) to expand the HIPAA standards.

Another key concern is whether the Privacy Rule strikes the right balance between protecting individual privacy and supporting important societal goals. The Secretary's 1997 recommendations recognized the importance of balancing the privacy rights of individuals and the amount of control they have over the use and disclosure of their health information, with the need to permit health information to be used not just for routine health care activities (e.g., treatment and payment) but also for other purposes related to health care that are in the public interest (e.g., oversight, research, law enforcement, public health and safety).[10]

Researchers, in particular, have criticized the Privacy Rule. They claim its privacy protections are unnecessarily impeding their access to and use of health information.[11] These concerns, some of which have been addressed administratively by HHS, are part of a broader set of challenges posed by the rapid digitization of medical information. Since 2009, the federal government has spent over $30 billion to promote the adoption of electronic health records (EHRs) and the development of an infrastructure that allows providers, patients, and other stakeholders to share electronic health information in ways that improve health care quality and outcomes.[12] But in order to realize the full value of EHR use, researchers need to be able to access and analyze clinical data

[8] http://www.hhs.gov/ocr/privacy/index.html.

[9] Department of Health and Human Services, Office of the Secretary, "HIPAA Administrative Simplification: Enforcement," 71 *Federal Register* 8390, February 16, 2006.

[10] See footnote 5 and accompanying text box above.

[11] Institute of Medicine, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, Washington, DC, February 2009, http://www.nap.edu/openbook.php?record_id=12458.

[12] This spending has been pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, which authorized Medicare and Medicaid incentive payments to hospitals, physicians, and other health care providers who become "meaningful users" of EHR technology. The HITECH Act was incorporated as Division A, Title XIII and Division B, Title IV of the American Recovery and Reinvestment Act of 2009 (ARRA; P.L. 111-5).

from patient records to identify best practices, and then share those findings with others to create a learning health care system.

To ensure public trust in the analytic uses of health data for learning purposes, patient privacy concerns must be effectively addressed. A lack of trust in the privacy of medical information can have important implications for both individual and population health. Surveys show that individuals may avoid needed care, withhold information from providers, or lie about their medical conditions if they are concerned about the privacy and security of their health information.[13]

The HIPAA privacy standards were developed in the late 1990s, when most medical information was still paper-based. While many privacy advocates view the Privacy Rule as a good start, one that creates a foundation of privacy protections, they are concerned that the rule does not sufficiently protect digital health information maintained and exchanged by EHR systems.

Implementation of the Privacy Rule continues to challenge covered entities. The rule is complex and seeks largely to preserve the traditional right of health care providers to exercise discretion and professional judgment in deciding whether and how to use or disclose patient information. Providers who are unsure of the rule's requirements, and who perhaps have been warned of the potential penalties for violating it, will sometimes err on the side of caution. They will refuse to disclose health information in an otherwise routine situation—for example, to a family member who calls inquiring about a hospital inpatient—claiming (incorrectly) that the disclosure is prohibited by HIPAA. In fact, the Privacy Rule accommodates such routine circumstances and neither requires nor prohibits the provider from using or disclosing health information. Instead, the rule leaves that decision up to the provider.

The growing number of breaches of electronic health data also has led to renewed criticism of the Security Rule, whose standards are intended to protect electronic information when stored in place and during transmission from one location to another.[14] The standards are technology-neutral and scalable, based on the size and complexity of the organization. HIPAA-covered entities have considerable latitude in how they implement them.

Congress addressed some of the concerns about the Privacy and Security Rules in the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.[15] The HITECH Act expanded and strengthened the privacy and security standards, principally by addressing enforcement of the standards and by establishing a breach notification requirement. The Genetic Information Nondiscrimination Act (GINA) of 2008 also amended the Privacy Rule.[16] In addition, HHS has made other changes through administrative (non-statutory) action.

[13] See, for example, Israel T. Agaku et al., "Concern about Security and Privacy, and Perceived Control over Collection and Use of Health Information are Related to Withholding of Health Information from Healthcare Providers," *J. Am. Med. Inform. Assoc.,* vol. 21, no. 2 (2014), pp. 374-378.

[14] See CRS Insight IN10235, *Anthem Data Breach: How Safe Is Health Information Under HIPAA?* February 24, 2015, by C. Stephen Redhead.

[15] P.L. 111-5, Division A, Title XIII and Division B, Title IV, 123 Stat. 226, 467.

[16] P.L. 110-233, 122 Stat. 881.

Report Roadmap

This report is intended to introduce the reader to the HIPAA Privacy and Security Rules, and the accompanying enforcement and breach notification requirements. It begins with an overview of each rule as it was originally promulgated. Those sections are followed by a discussion of the HITECH Act and other significant modifications that have been made. A list of all the HIPAA Administrative Simplification standards and their location in the Code of Federal Regulations (CFR) is provided in the **Appendix**.

An Overview of the HIPAA Privacy Standards

The HIPAA Privacy Rule established a set of federal standards for the protection of personal health information. First, it required covered entities (i.e., health plans, health care clearinghouses, and health care providers that conduct HIPAA electronic transactions) to put in place safeguards to protect health information from unauthorized access, use, or disclosure.[17] Second, it described the circumstances under which covered entities are permitted to use or disclose an individual's health information.[18] Finally, the rule gave individuals certain rights with respect to their health information. Those rights include the right of access to inspect and obtain a copy of their medical information,[19] the right to amend inaccurate or incomplete information,[20] and the right to an accounting of certain types of disclosures of the information.[21]

The Privacy Rule covers "protected health information" (PHI) that is created or received by a covered entity. PHI is broadly defined as individually identifiable information in any form or format—oral, paper-based, electronic—that "[r]elates 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."[22]

The rule includes a de-identification standard. Health information is de-identified if 18 specified types of identifiers are removed, or if a qualified statistician, using accepted principles, determines that the re-identification risk is very small.[23] De-identified information that meets this standard is not subject to the rule and may be used or disclosed by covered entities without regard to the rule's requirements.

General Requirements for Use and Disclosure

In the broadest sense, *the Privacy Rule prohibits a covered entity from using or disclosing PHI except as expressly permitted or required by the rule.*[24] The rule specifies only two circumstances

[17] 45 C.F.R. §164.530(c).

[18] 45 C.F.R. §164.502(a).

[19] 45 C.F.R. §164.524.

[20] 45 C.F.R. §164.526.

[21] 45 C.F.R. §164.528.

[22] 45 C.F.R. §160.103.

[23] 45 C.F.R. §164.514(b). The 18 types of identifiers include names; physical and email addresses; social security, medical record, health plan, and account numbers; photographic images; and biometric identifiers.

[24] 45 C.F.R. §164.502(a).

when a covered entity is *required* to disclose PHI. A covered entity must disclose PHI to the individual who is the subject of the information (i.e., patient right of access), and to HHS officials investigating potential violations of the rule.[25] The rest of the rule describes a wide range of circumstances under which it is *permissible* to use or disclose PHI. In all such instances, covered entities can choose whether to use or disclose PHI based on their professional ethics and using their own best judgment. Thus, the Privacy Rule seeks to preserve the discretion that health care professionals have traditionally exercised when using or disclosing patient or beneficiary information. *For all uses or disclosures of PHI that are not otherwise permitted or required by the rule, covered entities must obtain a patient's written authorization.*[26]

Minimum Necessary

The Privacy Rule includes a minimum necessary standard for the use or disclosure of PHI. It requires a covered entity that uses or discloses PHI, or requests such information from another covered entity, to make reasonable effort to limit the information to the minimum amount necessary to accomplish the intended purpose of the use or disclosure. There are several circumstances in which the minimum necessary standard does not apply. These include health care providers sharing a patient's PHI for treatment purposes, disclosures to individuals who request access to their information, any use or disclosure for which an authorization was obtained, and uses or disclosures that are required by other law.[27]

In most instances, covered entities do not need to make a minimum necessary determination for each separate use or disclosure. The rule instructs covered entities to implement policies and procedures governing routine and recurring uses and disclosures of PHI. These include identifying persons or categories of persons within an organization who need specific types of information and limiting their access to just that information. Disclosures that are not made on a routine and recurring basis must be individually reviewed to determine the minimum amount of PHI necessary to accomplish the specified purpose.[28]

Business Associates

Health plans and health care providers routinely hire companies and consultants to help them operate as businesses and meet their responsibilities to patients and beneficiaries. These third parties provide claims processing, billing, legal, actuarial, accounting, transcription, data management, peer review, quality assurance, accreditation, and financial services, among others. Most of them need access to at least some patient information in order to perform those functions. Initially, the Privacy Rule did not directly regulate such "business associates" of covered entities. However, HHS in its rulemaking required covered entities to manage their business associates through contractual relationships. Covered entities were required to obtain satisfactory written assurance in the form of a Business Associate Agreement, or BAA, that their business associates would, among other things (1) use PHI only for the purposes permitted or required by the contract, and (2) implement appropriate safeguards to prevent misuse of PHI.[29]

[25] Ibid.

[26] 45 C.F.R. §164.508(a).

[27] 45 C.F.R. §164.502(b).

[28] 45 C.F.R. §164.514(d).

[29] 45 C.F.R. §§164.502(e), 164.504(e).

Authorization

The Privacy Rule specifies the types of information that must be included in an authorization form.[30] Initially, the rule prohibited combining an authorization with any other legal permission to create a "compound" authorization, with a few specified exceptions. However, as discussed later in this report, the restriction on compound authorizations has since been loosened.

Health care providers may not require an individual to sign a HIPAA authorization as a condition of treating the individual, unless the treatment is being provided as part of a research study. However, health plans may condition enrollment in a plan, or eligibility for benefits, on obtaining an authorization prior to an individual's enrollment in the plan, if the plan is seeking access to PHI for eligibility or enrollment determinations, or for other underwriting purposes.[31]

Specific Requirements for Use and Disclosure

In general, covered entities may use or disclose PHI for the purposes of treatment, payment, and other routine health care operations with few restrictions.[32] A covered entity may use or disclose PHI for its own treatment, payment, or health care operations. In addition, a covered entity may disclose PHI for the treatment or payment activities of a health care provider; for the payment activities of another covered entity; and for certain health care operations of another covered entity, if each entity has or had a relationship with the individual who is the subject of the PHI, and the requested information pertains to that relationship. An individual has the right to request restrictions on uses or disclosures of PHI for treatment, payment, or health care operations. For example, an individual may request that a particular medical procedure be kept confidential and not shared with other providers. The covered entity is not required to agree to such a restriction. But if they do, they must abide by the agreement, except in emergency circumstances.[33]

Under certain other circumstances (e.g., disclosures to family members and friends, disclosures from public directories maintained by hospitals and other facilities, fundraising), the Privacy Rule requires covered entities to give the individual the opportunity to object to the disclosure (i.e., opt out).[34] The rule also permits the use or disclosure of PHI for specified "national priority purposes" that are not directly connected to the treatment of the individual.[35] These uses and disclosures, which are summarized in the text box below, are permitted by the rule in recognition of the important uses made of health information outside of the health care context.

---

[30] 45 C.F.R. §164.508(c).

[31] 45 C.F.R. §164.508(b)(4). GINA (see footnote 16) prohibits group health plans and health insurers from using or disclosing genetic information—a subset of PHI—for underwriting purposes, as discussed in the text box "Amendments to HIPAA Privacy and Security Standards: Statutory (i.e., HITECH Act, GINA) and Non-Statutory." This prohibition has been superseded by the broader health insurance nondiscrimination provisions in the Affordable Care Act (ACA; P.L. 111-148, as amended). Under the ACA, group health plans and health insurers may not discriminate against an individual based on various factors related to the health status of the individual or a dependent of the individual. Those factors include genetic information.

[32] 45 C.F.R. §164.506.

[33] 45 C.F.R. §164.522(a).

[34] 45 C.F.R. §§164.510, 164.514(f).

[35] 45 C.F.R. §164.512.

HIPAA Privacy Rule: National Priority Uses and Disclosures
45 C.F.R. §164.512

Required by Law. Generally, the Privacy Rule does not preempt other statutory reporting mandates. Covered entities may use or disclose PHI to the extent that such use or disclosure is required by (federal or state) law and the disclosure complies with and is limited to the relevant requirements of such law.

Public Health Activities. A covered entity may disclose PHI for public health purposes to certain specified recipients, including federal and state public health agencies, and persons subject to the jurisdiction of the Food and Drug Administration (FDA) regarding FDA-regulated products and activities (e.g., adverse event reporting), among others. A covered entity also is permitted to use or disclose a "limited data set" for public health purposes.[36]

Victims of Abuse, Neglect, or Domestic Violence. A covered entity may disclose PHI about victims of abuse, neglect, or domestic violence to a government authority to the extent the disclosure is required by law, or if the individual agrees to such disclosure. In addition, a covered entity may disclose this type of information if such disclosure is expressly permitted by law and certain criteria are met.

Health Oversight Activities. A covered entity may disclose PHI to health oversight agencies for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; and licensure or disciplinary actions, among other activities.

Judicial and Administrative Proceedings. A covered entity may disclose PHI in response to an order of a court or administrative tribunal; or in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, if the covered entity receives satisfactory assurance that the party seeking the information has made reasonable efforts to ensure that the individual has been given notice of the request. Alternatively, the party seeking the information may obtain a protective order.

Law Enforcement Purposes. A covered entity may disclose PHI to law enforcement officials as required by law or pursuant to a court order, court-ordered warrant, or subpoena or summons issued by a judicial officer; a grand jury subpoena; or an administrative request that meets certain standards. In addition, PHI may be disclosed to law enforcement officials for the purpose of identifying or locating suspects, fugitives, or missing persons. Disclosures for other specified law enforcement purposes are also permitted.

Decedents. A covered entity may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person or determining the cause of death. PHI also may be disclosed to funeral directors, as necessary for them to carry out their duties.

Cadaveric, Organ, Eye, or Tissue Donation. A covered entity may disclose PHI to Organ Procurement Organizations or other entities that procure, bank, or transplant tissues and organs.

Research. A covered entity may disclose PHI to researchers without authorization provided an Institutional Review Board (IRB) or equivalent "Privacy Board" waives the authorization based on a determination that (1) the use or disclosure of PHI involves no more than minimal risk to the privacy of the individuals; (2) the research could not practicably be conducted without a waiver; and (3) the research could not practicably be conducted without access to, and use of, the information. Covered entities also may use or disclose a limited data set (see footnote 36) to researchers without authorization or a waiver of authorization from an IRB or Privacy Board.

Averting a Serious Threat to Health or Safety. Consistent with applicable law and standards of ethical conduct, a health care provider may use or disclose PHI if the provider, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

Specialized Government Functions. A covered entity may use or disclose PHI for several specified government functions, including military and veterans' activities, national security and intelligence activities, and coordinating public benefits provided by government agencies and programs that are themselves covered entities.

Workers' Compensation. A covered entity may disclose PHI as authorized by laws relating to workers' compensation or similar programs.

[36] A limited data set is PHI from which all but three specified types of identifiers have been removed. While not meeting the Privacy Rule's standard for de-identified information, a limited data set is considered to pose a reduced risk of identification. Use or disclosure of a limited data set requires a data use agreement. 45 C.F.R. 164.514(e).

Administrative Requirements for Covered Entities

The Privacy Rule established a series of administrative obligations for covered entities. First, they must provide individuals with a written notice that includes the following information: (1) a description of patients' rights under the rule and how to exercise those rights; (2) the legal duties of the covered entity; (3) a description of the required and permissible uses and disclosures of PHI; (4) how an individual can file a complaint with the covered entity or the HHS Secretary; (5) how the covered entity will provide a revised notice if it needs changing; and (6) a contact person for additional information.[37]

Second, covered entities are required to adopt reasonable administrative, technical, and physical safeguards in order to protect PHI from unauthorized access, use, or disclosure.[38] The Security Rule—applicable only to PHI in electronic form—established specific standards for those safeguards.

Finally, the rule requires a covered entity to designate a privacy official to develop and implement its policies and procedures for protecting PHI under the Privacy Rule. Each covered entity must train all members of its workforce on those policies and procedures.[39]

Special Rules for Employers and Other Entities

The Privacy Rule includes provisions that apply to specific types of organizations that perform health care functions covered by the rule but do not fit neatly within the definition of a covered entity. For example, an organization that is a single legal entity and conducts both covered and non-covered functions (e.g., a manufacturing company that operates a health clinic) has the option to become a "hybrid entity" under the rule.[40] This requires the company to designate in writing the segments of its business that perform covered functions as one or more "health care components." Once this designation is made, most of the rule's requirements apply only to the health care components. They are prohibited from sharing PHI with the larger organization unless the disclosure has been authorized by the individual or is otherwise permitted by the rule.

The rule's treatment of employers as sponsors of group health plans is of particular interest given the fact that so many individuals obtain their health insurance coverage through their employer. Employers are not HIPAA-covered entities, but they may need access to individual health information to administer the group health plan that they sponsor. Employees, on the other hand, are concerned that health information shared with employers may be used inappropriately to make employment decisions. In an attempt to reconcile these competing interests, the rule permits a health insurance issuer or HMO (with respect to a group health plan) to disclose certain PHI to the plan sponsor (i.e., employer) for plan administration purposes, but prohibits disclosure for employment-related actions (e.g., promotion, termination).[41]

Specifically, the following PHI may be disclosed to a plan sponsor:

[37] 45 C.F.R. §164.520.

[38] 45 C.F.R. §164.530(c).

[39] 45 C.F.R. §164.530(a)-(b).

[40] 45 C.F.R. §164.105(a).

[41] 45 C.F.R. §164.504(f).

- information on whether an individual is, or is no longer, enrolled in the plan;
- summary claims information stripped of all identifiers other than five-digit zip codes for the sponsor to use to obtain premium bids for providing health insurance coverage through the group health plan, or to modify, amend, or terminate the group health plan; or
- enrollee PHI for the plan sponsor to use to administer the plan. For such disclosures to occur, the plan documents must be amended to limit the uses and disclosures of PHI by the sponsor to those that are consistent with the rule. Furthermore, the sponsor must certify that it will not use the information for employment-related purposes, and that it will establish adequate firewalls so that only those personnel who need the information to perform functions on behalf of the group health plan have access to such information.

Enforcement and Compliance

An individual or organization who believes a covered entity is not complying with the Privacy Rule may file a complaint with OCR. The rule lists the requirements for filing a complaint.[42] It also describes the responsibilities of covered entities to provide records and compliance reports and to permit access to information for investigations and compliance reviews.[43]

HIPAA established civil and criminal penalties for violations of all its Administrative Simplification standards, including the Privacy and Security Rules. Initially, OCR could impose a civil monetary penalty (CMP) on any covered entity that it determined had violated an Administrative Simplification requirement of not more than $100 per violation, up to a maximum of $25,000 per year for multiple violations of the same requirement. CMPs could not be imposed if (1) the violation was a criminal offense under HIPAA's criminal penalty provisions; (2) the person did not have actual or constructive knowledge of the violation; or (3) the failure to comply was due to reasonable cause and not willful neglect, and was corrected within 30 days.[44]

For certain wrongful PHI disclosures, OCR may refer the case to DOJ for criminal prosecution. The criminal penalty for a person who knowingly obtains or discloses PHI in violation of HIPAA is a fine of up to $50,000 and/or up to one year in prison. The penalty increases to $100,000 and/or up to five years in prison if the wrongful conduct involves false pretenses. It further increases to $250,000 and/or up to 10 years in prison if the offense is committed with the intent to sell, transfer, or use the information for commercial advantage, personal gain, or malicious harm.[45]

There is no private right of action under HIPAA. Individuals cannot sue covered entities or business associates for violations of the law. However, HIPAA violations may result in a variety of claims against covered entities and business associates under state law.

[42] 45 C.F.R. §160.306.

[43] 45 C.F.R. §160.310.

[44] Section 1176 of the Social Security Act, as added by Section 262 of HIPAA; 42 U.S.C. §1320d–5. Initial implementing regulations at 45 C.F.R. §§160.400 et seq. established rules for determining the CMP amount and the number of violations, among other things (see footnote 9).

[45] Section 1177 of the Social Security Act, as added by Section 262 of HIPAA; 42 U.S.C. §1320d–6.

Preemption of State Laws

Covered entities must comply with both the HIPAA Privacy Rule and any applicable state privacy laws unless the state laws are contrary to the Privacy Rule, in which case they are preempted by it. Contrary means that it would be impossible for a covered entity to comply with both the state and federal requirements, or that the state law is an obstacle to accomplishing the full purpose of HIPAA.[46]

There are a number of exceptions to this general preemption requirement. If the contrary state privacy law is "more stringent" than the Privacy Rule, meaning that it provides greater privacy protection, then the state law takes precedence. A state law is more stringent when it prohibits or restricts a use or disclosure that would be permitted under the Privacy Rule, or when it provides individuals with greater access to their information.[47] *Thus, HIPAA establishes a federal floor for protecting health information privacy that allows states to implement additional privacy protections.*

In addition, the Privacy Rule does not preempt state laws that provide for the reporting of a disease or injury, child abuse, birth, or death, or for conducting public health investigations. Nor does it preempt state laws that require health plans to report or grant access to health information for the purpose of audits, evaluation, or licensure, even if they are less protective of individuals' privacy.[48]

An Overview of the HIPAA Security Standards

The HIPAA Security Rule requires covered entities and business associates to ensure the confidentiality, integrity, and availability of all electronic PHI (ePHI) that they create, receive, maintain, or transmit (see text box). Covered entities and business associates are to protect against any reasonably anticipated threats or hazards to the security of ePHI, and any reasonably anticipated uses or disclosures of such information that are in violation of the Privacy Rule.[49] *Unlike the Privacy Rule, which applies to PHI in any form or format, the Security Rules applies only to ePHI.*

HIPAA Security

Confidentiality: ePHI is accessible only by authorized people and processes.

Integrity: ePHI is not altered or destroyed in an unauthorized manner.

Availability: ePHI can be accessed as needed by an authorized person.

The Security Rule and the Privacy Rule are closely interconnected. While the Privacy Rule established standards for who may have access to PHI, and for what purposes, the Security Rule created the standards for ensuring that only those who should have access to ePHI will in fact have access. When it developed the Security Rule, HHS adhered closely to the requirements of the Privacy Rule. As noted in the previous section, the Privacy Rule requires covered entities to

[46] HIPAA's preemption provisions, which apply to all the Administrative Simplification standards, not just the Privacy Rule, are in Section 1178 of the Social Security Act; 42 U.S.C. § 1320d–7. Implementing regulations are codified at 45 C.F.R. §§160.201-205.

[47] 45 C.F.R. §160.202.

[48] 45 C.F.R. §160.203.

[49] 45 C.F.R. §164.306(a).

adopt reasonable administrative, technical, and physical safeguards in order to protect PHI from unauthorized access, use, or disclosure. But the Privacy Rule does not specify what those safeguards should be. That is the purpose of the Security Rule, under which each of the safeguards—administrative, physical, and technical—is composed of a number of standards.

Implementation Specifications

Covered entities and business associates have considerable discretion and flexibility in how they implement the security standards. Each standard generally consists of one or more implementation specification (i.e., detailed instructions for implementing the standard) that are either "required" or "addressable."[50] If an implementation specification is required, the organization must adopt the policies and/or procedures described for that specification. If an implementation specification is addressable, the organization must assess whether it is a "reasonable and appropriate safeguard in its environment."[51] If the organization chooses not to implement an addressable implementation specification based on its assessment, it must document the reasons and implement an "equivalent alternative measure if reasonable and appropriate."[52]

Table 1 lists all the security standards and provides a brief summary of the policies, procedures, or programs that must be implemented to meet each one. The table also shows the implementation specifications, if any, associated with each standard and indicates whether they are required or addressable.

Table 1. HIPAA Security Standards and Implementation Specifications

45 C.F.R. Part 164, Subpart C

Standards	Implementation Specifications R = Required; A = Addressable	
Administrative Safeguards		
Security Management Process	Risk Analysis	R
Implement policies and procedures to prevent, detect, contain and correct security violations. [§ 164.308(a)(1)]	Risk Management	R
	Sanction Policy	R
	Information System Activity Review	A
Assigned Security Responsibility		R
Identify the security official responsible for developing and implementing security policies and procedures. [§ 164.308(a)(2)]		
Workforce Security	Authorization and/or Supervision	A
Implement policies and procedures to ensure that all members of the workforce have appropriate access to ePHI, as provided under the Information Access Management standard, and to prevent those who do not have access from obtaining it. [§ 164.308(a)(3)]	Workforce Clearance Procedure	A
	Termination Procedures	A

[50] 45 C.F.R. §164.306(d)(1).

[51] 45 C.F.R. §164.306(d)(3).

[52] Ibid.

Standards	Implementation Specifications R = Required; A = Addressable	
Information Access Management *Implement policies and procedures for authorizing access to ePHI, consistent with applicable requirements of the Privacy Rule. [§ 164.308(a)(4)]*	Isolating Clearinghouse Functions	R
	Access Authorization	A
	Access Establishment and Modification	A
Security Awareness and Training *Implement a security awareness and training program for all members of the workforce. [§ 164.308(a)(5)]*	Security Reminders	A
	Protection from Malicious Software	A
	Log-in Monitoring	A
	Password Management	A
Security Incident Procedures *Implement policies and procedures to address security incidents and report them to the appropriate entities. [§ 164.308(a)(6)]*	Incidence Response and Reporting	R
Contingency Plan *Establish policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI. [§ 164.308(a)(7)]*	Data Backup Plan	R
	Disaster Recovery Plan	R
	Emergency Mode Operating Plan	R
	Testing and Revision Procedures	A
	Applications and Data Criticality Analysis	A
Evaluation *Perform a periodic technical and nontechnical evaluation to determine the extent to which security policies and procedures meet the requirements of the Security Rule. [§ 164.508(a)(8)]*		R
Business Associate Contracts *A Business Associate may create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity receives satisfactory written assurance (i.e., BAA) that the Business Associate will safeguard the information. [§ 164.308(b)]*	Written Contract or Other Arrangement	R
Physical Safeguards		
Facility Access Control *Implement policies and procedures to limit physical access to electronic information systems and the facility/facilities in which they are housed, while ensuring that properly authorized access is allowed. [§ 164.310(a)(1)]*	Contingency Operations	A
	Facility Security Plan	A
	Access Control and Validation Procedures	A
	Maintenance Records	A
Workstation Use *Implement policies and procedures that specify the proper functions to be performed at workstations that access ePHI, including at remote locations. [§ 164.310(b)]*		R
Workstation Security *Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users. [§ 164.310(c)]*		R

Standards	Implementation Specifications R = Required; A = Addressable	
Device and Media Controls *Implement policies and procedures that govern the receipt and removal of hardware and electronic media containing ePHI, into and out of a facility, and the movement of these items within the facility. [§ 164.310(d)(1)]*	Disposal	R
	Media Reuse	R
	Accountability	A
	Data Backup and Storage	A
Technical Safeguards		
Access Control *Implement technical policies and procedures for systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified (see Information Access Management). [§ 164.312(a)(1)]*	Unique User Identification	R
	Emergency Access Procedure	R
	Automatic Logoff	A
	Encryption and Decryption	A
Audit Controls *Implement hardware, software, and/or procedural mechanisms that record and examine activity in systems that contain or use ePHI. [§ 164.312(b)]*		R
Integrity *Implement policies and procedures to protect ePHI from improper alteration or destruction. [§ 164.312(c)(1)]*	Mechanism to Authenticate ePHI	A
Person or Entity Authentication *Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. [§ 164.312(d)]*		R
Transmission Security *Implement technical security measures to guard against unauthorized access to ePHI that is transmitted over an electronic communications network. [§ 164.312(e)(1)]*	Integrity Controls	A
	Encryption	A

Source: Prepared by CRS based on the text of the HIPAA security standards and implementation specifications at 45 C.F.R. §§ 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), and 164.312 (Technical Safeguards).

Flexible and Scalable Standards

The security standards are designed to be flexible and scalable from the largest and most complex organizations to the smallest provider practices. In deciding which security measures to use, a covered entity or business associate must take into account the size, complexity, and capabilities of the organization; its technical infrastructure, hardware, and software security capabilities; the costs of security measures; and the probability and impact of potential risks to ePHI.[53] The security standards are technology-neutral to accommodate the continual emergence of new technologies. They do not prescribe the use of specific technologies.

[53] 45 C.F.R. §164.306(b).

Importance of Risk Analysis and Risk Management

The initial, and most important, actions that covered entities and business associates are required to take under the Security Rule are to conduct an accurate and thorough risk analysis and develop a risk management strategy (see **Table 1**). These actions form the foundation upon which all subsequent security activities are based. The purpose of the risk analysis is to identify all the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI, and to determine the likelihood and magnitude of those risks. Risk management is the process used to identify and implement security measures to reduce risk to a level that is reasonable and appropriate given the organization's circumstances, and that enables it to comply with the general requirements of the Security Rule.[54]

Covered entities and business associates must ensure that risk analysis and risk management are ongoing and dynamic processes—not just a one-time activity—that reflect changes to their operations and environment.

HITECH Act and Other Amendments to the HIPAA Standards

The HITECH Act included a series of provisions designed to expand and strengthen the HIPAA privacy and security standards.[55] Many of the changes were enacted to address the concerns of privacy advocates and other stakeholders. These groups had complained that there was no notification requirement in the event of a breach of PHI, and that OCR was not adequately enforcing the Privacy and Security Rules.

Among its provisions, the HITECH Act (1) established four categories of violations of the rules to reflect increasing levels of culpability, and four corresponding tiers of CMPs that significantly increased the minimum penalty amount for each violation; (2) required HHS to investigate all complaints indicating violations due to willful neglect; (3) made business associates of covered entities—and their subcontractors—directly liable for violations of Privacy and Security Rules; and (4) required covered entities and their business associates to notify individuals whose PHI was breached. In addition, the HITECH Act established new limitations on the use and disclosure of PHI for marketing and fundraising purposes; prohibited the sale of PHI in an otherwise permissible disclosure; and expanded individuals' rights to access their PHI, restrict certain disclosures to health plans, and obtain an accounting of routine disclosures of ePHI.

GINA also amended the Privacy Rule by clarifying that genetic information is PHI, which was already the case, and prohibiting health plans from using or disclosing genetic information for

[54] OCR and other federal agencies have sponsored conferences and produced a variety of guidance documents and other tools to help organizations better understand the risk analysis requirements under the HIPAA Security Rule. In March 2014, OCR, in collaboration with the HHS Office of the National Coordinator for Health Information Technology (ONC), released a security risk assessment tool to help guide small and medium-sized health care providers conduct risk assessments. More information is available at OCR's website, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html.

[55] The HITECH Act's privacy and security provisions are in Title XIII, Subtitle D ("Privacy") of Division A of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5), Sections 13400-13411 and 13421-13424; codified at 42 U.S.C. §§17921 et seq.

eligibility or enrollment determination, or other underwriting purposes.[56] As noted earlier, the Privacy Rule permits health plans to use or disclose PHI—other than genetic information—for such purposes.

Most of the HITECH Act amendments to the HIPAA privacy and security standards and their enforcement, as well as the changes required by GINA, were finalized in a January 2013 "omnibus" rule.[57] The omnibus rule also included technical and other non-statutory revisions to the HIPAA standards to improve their workability and effectiveness, most notably regarding authorizations for the use or disclosure of PHI for research.

The text box summarizes significant changes made by the HITECH Act and GINA to the HIPAA standards. It includes the new requirements for research authorizations. Several of these provisions are discussed in more detail below.

Amendments to HIPAA Privacy and Security Standards:
Statutory (i.e., HITECH Act, GINA) and Non-Statutory

Business Associates. Under the HITECH Act, business associates—and their subcontractors—are directly liable and subject to the HIPAA civil and criminal penalties for (1) uses and disclosures of PHI in violation of their BAAs; (2) failing to comply with the breach notification and other HITECH Act amendments to the HIPAA privacy standards (see below); and (3) failing to comply with the Security Rule. Business associates include Patient Safety Organizations, regional health information organizations, health information exchanges, and e-prescribing gateways. [45 C.F.R. §§164.502(e), 164.504(e)]

Patient Rights. Individuals have a right to receive an electronic copy of their PHI, if it is maintained in an EHR, and can direct a covered entity, in writing, to transmit a copy of their PHI to a designated third party. Health care providers must honor an individual's request not to disclose to a health plan PHI about a specific health care item or service paid for out-of-pocket. [45 C.F.R. §164.524(c); 45 C.F.R. §164.522(a)(1)(vi)] Individuals have a right to an accounting of EHR disclosures for treatment, payment, and other health care operations. ***HHS has yet to finalize its May 31, 2011, proposed rule to implement this accounting requirement.***

Minimum Necessary. Covered entities must limit the use, disclosure, or request of PHI, to the extent practicable, to a limited data set or, if needed, to the minimum necessary. The entity disclosing the PHI (as opposed to the requester) makes the minimum necessary determination.

Sale of PHI. An otherwise permissible disclosure by a covered entity is prohibited (without an authorization) if the disclosure involves remuneration, with limited exceptions. [45 C.F.R. §164.502(a)(5)(ii)]

Marketing. A marketing communication by a covered entity relating to an individual's treatment, or to recommend other health products or services, requires the individual's authorization if the covered entity receives payment from a third party whose product or service the covered entity is marketing. Limited exceptions apply. [45 C.F.R. §§164.501, 164.508(a)(3)]

Breach Notification. In the event of a breach of unsecured (i.e., unencrypted) PHI, covered entities must notify each affected individual whose information has been, or is reasonably believed to have been, accessed as a result of the breach. All breaches must be reported to OCR. Those affecting 500 or more individuals must be reported within 60 days of discovery. Covered entities can maintain a log of smaller breaches and submit the log to OCR annually. [45 C.F.R. §§164.400 et seq.] Vendors of personal health records (PHRs), and certain related entities, that are not HIPAA-

[56] Section 1180 of the Social Security Act, as added by Section 105 of GINA; 42 U.S.C. §1320d–9.

[57] Department of Health and Human Services, Office of the Secretary, "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule," 78 *Federal Register* 5566, January 25, 2013. The HIPAA omnibus rule amended the interim final rule published on August 24, 2009 (74 *Federal Register* 42740), to implement the breach notification program (45 C.F.R. §§164.400 et seq.), and the interim final rule published on October 30, 2009 (74 *Federal Register* 56123), which conformed the existing HIPAA Enforcement Rule (45 C.F.R. Part 164, Subparts C-E) to the HITECH Act's tiered and increased CMP structure.

covered entities must report breaches of unencrypted PHR information to the Federal Trade Commission (FTC). Such breaches are treated as violations of the FTC Act. The FTC must notify HHS of any breach notices it receives. [16 C.F.R. §318]

Enforcement and Compliance Audits. The HITECH Act strengthened the HIPAA Enforcement Rule and replaced the existing CMPs with four tiers of new penalties (discussed in the main text). OCR must investigate violations due to willful neglect and impose CMPs, and is authorized to investigate alleged criminal violations if DOJ has not prosecuted the violators. OCR also must use any CMPs collected for HIPAA enforcement activities and, pursuant to GAO recommendations, establish a program for distributing a percentage of any collected penalties to harmed individuals. State attorneys general are authorized to bring a civil action in federal district court against an individual who violates HIPAA. OCR is required to perform periodic audits to ensure compliance with the HIPAA privacy and security standards, as amended. The HITECH Act also clarified that criminal penalties for wrongful disclosure of PHI apply to individuals who without authorization use or disclose such information maintained by a covered entity. [45 C.F.R. Part 164, Subparts C-E] ***HHS has yet to issue a proposed rule to establish a program for distributing collected penalties to harmed individuals.***

Genetic Information. GINA prohibits all health plans that are HIPAA-covered entities, except long-term care plans, from using or disclosing PHI that is genetic information—i.e., genetic tests, family medical history—for underwriting purposes (e.g., eligibility or enrollment determination, premium computation). Note: This prohibition has been superseded by the Affordable Care Act's much broader nondiscrimination provisions that apply to group health plans and health insurers. [45 C.F.R. §164.502(a)(5)(i)]

Research. To better align the Privacy Rule with the Common Rule informed consent requirements,[58] HHS now permits compound authorizations for any type of research activity (with limited exceptions), as well as authorizations for future research, provided the description of the future research is sufficiently clear that it would be reasonable for the individual to expect his or her PHI could be used or disclosed for such research. [45 C.F.R. §164.508(b)(3)]

Business Associates

Prior to the HITECH Act, HIPAA applied directly to covered entities but not to business associates, which as noted earlier were regulated through contractual agreements (i.e., BAAs). Covered entities were not liable for, or required to actively monitor, their business associates. However, if a covered entity found out about a material breach or violation of the BAA, it had to take reasonable steps to remedy the situation and, if unsuccessful, terminate the contract. If termination was not feasible, then the covered entity had to notify HHS.

The HITECH Act made business associates directly liable and subject to civil and criminal penalties for violations of HIPAA or their BAAs (see text box).[59] It also clarified that subcontractors of a business associate are themselves business associates.[60] Thus, subcontractors along the contractual chain are subject to the same compliance obligations and are directly liable for HIPAA violations. Just as business associates may use or disclose PHI only as permitted by the BAA or required by law, and may not use or disclose PHI in a manner that would violate the Privacy Rule, so subcontractors are subject to the same limitations, as documented in subcontracts. A covered entity (or a business associate) that knows of a pattern of activity or practice of its business associate (or subcontractor) that constitutes a material breach or violation of the BAA must take reasonable steps to remedy the problem and, if such steps are unsuccessful, terminate the contract.[61] Neither covered entities nor their business associates (including

[58] 45 C.F.R. §46.116. See also footnote 83.

[59] 45 C.F.R. §164.514(e).

[60] A subcontractor is an entity that "creates, receives, maintains, or transmits PHI on behalf of the business associate." 45 C.F.R. §160.103.

[61] 45 C.F.R. §514(e)(1).

subcontractors) may intimidate, threaten, discriminate against, or take any other retaliatory action against an individual who files a complaint, cooperates with investigators, or opposes unlawful actions.[62]

Pursuant to the HITECH Act, Patient Safety Organizations, health information exchange organizations and e-prescribing gateways are business associates. The omnibus rule also clarifies that while a data transmission service—acting merely as a conduit for the flow of information (including temporary storage that is incidental to the transmission service)—is not a business associate, a service that provides more persistent storage (e.g., cloud EHRs) is a business associate.[63]

Breach Notification

The HIPAA breach notification program was established in 2009, pursuant to the HITECH Act.[64] Under the program, covered entities and their business associates must notify all individuals affected by a breach of *unsecured* ePHI without unreasonable delay, but no later than 60 days after the discovery of the breach (see text box). Unsecured ePHI means information that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through encryption.[65] The law exempted encrypted PHI from the definition of a breach in an effort to encourage the practice of encrypting health information.

Covered entities also must notify the HHS Secretary of breaches of unsecured PHI. A "major" breach affecting 500 or more individuals must be reported to the Secretary at the same time the affected individuals are notified. Entities may maintain a log of breaches involving fewer than 500 individuals and submit the log to HHS annually. OCR is required to maintain a website listing all the major breaches (i.e., affecting at least 500 individuals).[66]

The HITECH Act defines a breach as the "unauthorized acquisition, access, use, or disclosure of [PHI] which compromises the security and privacy of such information.... "[67] The definition excludes unintentional access or use of PHI, inadvertent disclosures, and disclosures where the covered entity has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

In its initial rulemaking to implement the breach notification program, HHS stated that the phrase "compromises the security and privacy of PHI" means "poses a significant risk of financial, reputational, or other harm to the individual."[68] Covered entities and business associates faced with an incident involving the unauthorized acquisition, access, use or disclosure of PHI first had

[62] 45 C.F.R. §160.316.

[63] 45 C.F.R. §160.103.

[64] Department of Health and Human Services, Office of the Secretary, "Breach Notification for Unsecured Protected Health Information," Interim final rule with request for comments, 74 *Federal Register* 42740, August 24, 2009. The regulations for the breach notification program are codified at 45 C.F.R. §§164.400 et seq.

[65] 45 C.F.R. §164.402.

[66] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[67] Section 13400 of the HITECH Act; 42 U.S.C. §17921.

[68] 45 C.F.R. 164.402 (2009).

to determine whether it met this harm threshold. If it did, and the incident constituted a breach, then notification was required.

The harm threshold was controversial. Consumer advocacy organizations and others criticized it for being too subjective and for discouraging reporting. They argued for its modification or elimination. HHS responded in the omnibus rule by removing the harm threshold and modifying the risk assessment portion of the breach notification rule to require the use of a more objective assessment. An impermissible use or disclosure of PHI "is presumed to be a breach unless the covered entity or business associate ... demonstrates that there is a low probability that the [PHI] has been compromised based on a risk assessment.... "[69] The modified rule lists the factors that must be included in the risk assessment. Now the default is notification, and the burden is on the covered entity or business associate to perform a risk assessment to determine whether there is a low probability that PHI was compromised. If that determination is made (and documented), then the covered entity or business associate need not provide notification.

The Secretary is required annually to submit a report to Congress on the number and nature of the breaches reported to OCR, and the actions taken in response to such breaches. To date, the Secretary has submitted two reports, each analyzing two years of information. The first report covers 2009-2010, and the second one covers 2011-2012.[70]

Cumulatively, through December 31, 2012, OCR received 710 reports of major breaches affecting a total of approximately 22.5 million individuals. Over the same period, OCR received 77,420 reports of breaches affecting fewer than 500 individuals. In all, these breaches affected approximately 400,000 individuals. Thus, while the major breaches made up about 1% of breach reports, they accounted for more than 98% of all the individuals who were affected by a breach of their PHI.

Of all the categories of causes of breaches, theft accounted for about half of all incidents. OCR identified the following lessons learned from the two breach reports:[71]

- Ensure that an organization's risk analysis and risk management plan is thorough and addresses all potential risks and vulnerabilities to ePHI, regardless of location or media. That includes ePHI on computer hard drives, USB drives, laptops, mobile phones, and other portable devices, as well as ePHI transmitted across networks.
- Ensure that security evaluations are conducted when there are operation changes (e.g., office moves) and technical upgrades for hardware and software so that ePHI remains secure.
- Ensure that ePHI stored on portable electronic devices is properly secured, including through encryption, with clear policies on the use and removal of such devices from a facility.

[69] Ibid., as amended by the HIPAA omnibus rule.

[70] Department of Health and Human Services, Office for Civil Rights, *Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2009 and 2010*, August 15, 2011; Department of Health and Human Services, Office for Civil Rights, *Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2011 and 2012*, May 20, 2014. Both reports and accompanying submission letters are available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreptmain.html.

[71] Ibid., pp. 26-27 (2011-2012 report).

- Implement clear policies and procedures for the proper disposal of PHI in all forms.
- Ensure physical safeguards are in place to limit access to facilities and workstations that maintain PHI.
- Ensure that employees are fully trained on the organization's privacy and security policies and procedures.

Enforcement and Compliance Audits

The HITECH Act's provisions to expand and strengthen HIPAA enforcement were in part a response to the approach taken initially by OCR to work with entities in violation of the HIPAA standards and encourage voluntary compliance through corrective action.[72] Privacy advocates criticized the agency for not being more aggressive in its enforcement activities and for not penalizing noncompliant organizations. At the time of the HITECH Act enactment, OCR had not levied a single civil penalty against a covered entity, though cases had been referred to DOJ for criminal prosecution.

The HITECH Act clarified that the criminal penalties for wrongful disclosure apply to individuals who without authorization use or disclose such information maintained by a covered entity, whether they are employees or not. This provision was prompted by a Memorandum Opinion issued by the DOJ Office of Legal Counsel in June 2005 clarifying the scope of HIPAA criminal enforcement.[73] The opinion was interpreted by some to mean that employees of covered entities could not be held liable for a HIPAA criminal violation; only covered entities could be prosecuted directly.

Table 2 summarizes the four tiers of CMPs that replaced the original HIPAA penalty of $100 per violation up to an annual maximum of $25,000 for multiple violations of the same requirement. The lowest tier applies to entities that "did not know, and by exercising reasonable diligence would not have known" of the violation.[74] The second tier applies to violations due to reasonable cause and is likely to cover many common violations by otherwise generally compliant covered entities; for example, those that occur due to human error, despite workforce training and appropriate policies and procedures. Reasonable cause covers violations in which the entity "knew, or by exercising reasonable diligence would have known" of the violation, "but did not act with willful neglect."[75]

The final two tiers, both dealing with violations due to willful neglect, are distinguished based on whether the entity took corrective action within 30 days. Willful neglect means "conscious, intentional failure or reckless indifference to the obligation to comply."[76]

[72] 45 C.F.R. §160.304.

[73] Department of Justice, Office of Legal Counsel, "Memorandum Opinion for The General Counsel Department of Health and Human Services and the Senior Counsel to the Deputy Attorney General on the Scope of Criminal Enforcement Under 42 U.S.C. §1320d-6," June 1, 2005.

[74] 45 C.F.R. §160.404(b)(2)(i).

[75] 45 C.F.R. §160.401.

[76] Ibid.

OCR must investigate whenever there is evidence of a possible violation due to willful neglect.[77] However, the omnibus rule states that, absent indications of willful neglect, OCR will continue to seek compliance through informal, voluntary action if appropriate.[78]

Table 2. HIPAA Civil Monetary Penalties

As Amended by the HITECH Act

Violation Category	Per Violation	Annual Maximum
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect—Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect—Not Corrected	≥$50,000	$1,500,000

Source: Section 1176 of the Social Security Act; 42 U.S.C. §1320d–5.

The HITECH Act requires the Secretary to conduct periodic audits to ensure that covered entities and business associates comply with the Privacy and Security Rules.[79] Unlike complaint investigations or compliance reviews, which are initiated in response to specific events or incidents, audits are based on a set of objective selection criteria.

OCR developed and conducted a pilot audit program that targeted 115 covered entities representing a broad range of sizes and complexities. The audits were conducted according to a protocol that identified the processes, controls, and policies of covered entities in three areas: privacy, security, and breach notification. OCR engaged PricewaterhouseCoopers (PwC) to evaluate the pilot audit program and is using PwC's findings to finalize plans for a permanent audit program. OCR has requested additional funding to establish the audit program,[80] which it believes will generate tools for covered entities to self-evaluate and help spread a culture of compliance within the health care sector as entities become aware of the program and its expectations.

The HITECH Act requires the Secretary annually to submit a report to Congress that summarizes the number and types of complaints received; the compliance reviews and enforcement actions taken; the number of audits performed and their findings; and the Secretary's plan for improving HIPAA compliance and enforcement for the following year. The Secretary has submitted two such reports to date, each covering the same two-year period as the two breach notification reports submitted to Congress, which were described earlier.[81]

[77] Section 1176(c) of the Social Security Act, as added by Section 13410(a) of the HITECH Act; 42 U.S.C. §1320d–5(c).

[78] 78 *Federal Register* 5566, 5578-557945; C.F.R. §160.312.

[79] Section 13421 of the HITECH Act; 42 U.S.C. §17940.

[80] OCR included an additional $2 million in its FY2016 budget request for a permanent HIPAA audit program.

[81] Department of Health and Human Services, Office for Civil Rights, *Annual Report to Congress on HIPAA Privacy Rule and Security Rule Compliance For Calendar Years 2009 and 2010*, August 11, 2011; Department of Health and Human Services, Office for Civil Rights, *Annual Report to Congress on HIPAA Privacy Rule and Security Rule Compliance For Calendar Years 2011 and 2012*, May 20, 2014. Both reports and accompanying submission letters are available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/compliancereptmain.html.

Research

In 2009, the Institute of Medicine (IOM) released a report on the Privacy Rule's impact on research.[82] The IOM concluded that the rule does not adequately protect the privacy of health information used for research. It also concluded that the rule, as currently implemented, impedes the conduct of important new research. The report found that there is considerable variation in how organizations that collect and use health data are interpreting and following the rule. It discussed the challenges in reconciling the Privacy Rule with other federal regulations—primarily the Common Rule[83]—that govern human subject research. The report also examined inconsistencies between the Privacy Rule and the Common Rule, neither of which applies uniformly to all health research.

For example, the Privacy Rule generally prohibited combining an authorization with any other legal permission to create a "compound" authorization, unless it was for the same study. Thus, a Privacy Rule authorization for a specific research study could be combined with Common Rule informed consent to participate in the research. But any separate research activity, such as collecting specimens or data for a central research database or repository, would require its own authorization. Unlike Common Rule informed consent, Privacy Rule authorizations also had to be study-specific; authorizations for future research were prohibited.

The omnibus rule addressed some of these inconsistencies. The Privacy Rule now permits compound authorizations for any type of research activity (with limited exceptions)[84] and allows authorizations for future research, provided the description of the future research uses is sufficiently clear that it would be "reasonable for an individual to expect that his or her protected health information could be used or disclosed for such future research."[85]

[82] Institute of Medicine, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, Washington, DC, February 2009, http://www.nap.edu/openbook.php?record_id=12458.

[83] The Common Rule refers to the core set of federal regulations for protecting human subjects in federally funded research. Under the Common Rule, research protocols must be approved by an Institutional Review Board (IRB) to ensure that the rights and welfare of the research subjects are protected. The Common Rule lists several criteria for IRB approval, including the requirement that researchers obtain the informed consent of their research subjects. An IRB may waive the informed consent requirement based on certain specified criteria. 45 C.F.R. Part 46, Subpart A.

[84] 45 C.F.R. §164.508(b)(3).

[85] 78 *Federal Register* 5566, 5612.

Appendix. HIPAA Administrative Simplification

Table A-1. Health Information Standards and Related Requirements

Standards	Location in Title 45 C.F.R.
General Administrative Requirements	Part 160, Subpart A
Preemption of State Law	Part 160, Subpart B
Compliance, Investigations, Civil Monetary Penalties, Procedures for Hearings	Part 160, Subparts C-E
Unique Health Identifiers (Health Care Providers, Health Plans, Employers)	Part 162, Subparts A, D-F
Electronic Transactions and Code Sets	Part 162, Subparts A, I-S
Security of Protected Electronic Health Information	Part 164, Subparts A, C
Notification of Breach of Unsecured Protected Health Information	Part 164, Subpart D
Privacy of Protected Health Information	Part 164, Subparts A, E

Author Contact Information

C. Stephen Redhead
Specialist in Health Policy
credhead@crs.loc.gov, 7-2261