



## **HIPAA Primer for Nonprofit Social Services Agencies**

September 2009

This publication is available at online at  
[www.probonopartnership.org/publications.htm](http://www.probonopartnership.org/publications.htm)

## TABLE OF CONTENTS

	Page
I. INTRODUCTION.....	1
A. Executive Summary.....	1
B. HIPAA's Scope.....	3
C. If a Social Services Agency is not a HIPAA Covered Entity, What Next? .....	5
D. For Covered Entities, Which Law Applies? HIPAA or State Law? .....	6
E. HIPAA's Privacy and Security Regulations – Which Applies and What are the Differences? .....	7
II. PRIVACY – RESTRICTIONS ON USES AND DISCLOSURES OF PHI .....	7
A. When Can a Covered Entity Use and Disclose PHI? .....	8
III. PRIVACY – INDIVIDUAL RIGHTS.....	14
A. Right to Notice of Privacy Practices .....	14
B. Right of Access to Review/Copy PHI .....	15
C. Right to Request a Restriction on Uses and Disclosures of PHI .....	16
D. Right to Amend PHI.....	18
E. Right to an Accounting of Disclosures of PHI.....	19
IV. PRIVACY – ADMINISTRATIVE REQUIREMENTS .....	21
A. Privacy Officer .....	21
B. Training.....	21
C. Safeguards .....	21
D. Complaints.....	21
E. Sanctions.....	21
F. Mitigation .....	21
G. Refraining from Intimidating or Retaliatory Acts .....	22
H. Policies and Procedures.....	22
I. Documentation .....	22
J. Group Health Plans .....	22
V. OTHER HIPAA OR HITECH REQUIREMENTS .....	23
A. Notifying Individuals Regarding Breaches of Their Unsecured PHI .....	23
B. Prohibition on Sale of PHI .....	25

## TABLE OF CONTENTS

(continued)

	<b>Page</b>
C. Restrictions on Use of PHI for Marketing and Fundraising.....	25
D. Business Associates and the HITECH Act.....	27
VI. SECURITY REQUIREMENTS .....	27
A. Introduction.....	27
B. Administrative Safeguards.....	28
C. Physical Safeguards.....	32
D. Technical Safeguards.....	34
E. Organizational, Policies and Procedures, and Documentation Requirements .....	35
VII. PENALTIES AND ENFORCEMENT .....	36
A. Civil Penalties .....	36
B. Criminal Penalties.....	37
VIII. DEFINITIONS.....	38

## I. Introduction

While providing services to clients, nonprofit social services agencies often obtain identifiable health information. Social services agency (“SSA”) directors, however, often are unclear about whether the HIPAA privacy and security regulations issued under federal Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) apply to their agencies.<sup>1</sup> As indicated below, although HIPAA may not apply directly to certain SSAs, these agencies nonetheless should consider adopting HIPAA-like policies and procedures in order to protect their clients’ sensitive information. SSAs also may need these types of policies and procedures to comply with applicable state laws

This HIPAA Primer for Nonprofit Social Services Agencies is not intended to cover every detail of the HIPAA regulations. Instead, this Primer provides an overview of most of the HIPAA privacy and security requirements. To the extent that an agency determines that it likely is a Covered Entity under HIPAA, we recommend that the agency consult with legal counsel to develop a full HIPAA compliance program.

A number of HIPAA privacy and security requirements were impacted by the HITECH Act section of the American Recovery and Reinvestment Act of 2009 (“ARRA”), the stimulus bill signed by President Obama on February 17, 2009.<sup>2</sup> Although many of the provisions of the HITECH Act have not yet become effective, this Primer from time to time notes how the HITECH Act will affect the relevant HIPAA provisions. See Section V for more information on the HITECH Act.

***Capitalized terms in this Primer are defined in Section VIII, Definitions, at the end of this Primer. All definitions in Section VIII are based on definitions found in the HIPAA regulations.***

### A. Executive Summary

This Primer addresses the following topics:

- HIPAA’s scope: Does it apply to Social Services Agencies (“SSAs”)?
- Uses and disclosures of Protected Health Information (“PHI”), including uses and disclosures for:

---

<sup>1</sup> HIPAA is administered by several federal agencies. The sections of HIPAA that are discussed in this Primer are administered by the U.S. Department of Health and Human Services (“DHHS”). The DHHS has a website dedicated to HIPAA issues at [www.hhs.gov/ocr/privacy/hipaa/understanding/index.html](http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html). The DHHS regulations under HIPAA are set forth in Title 45 of the Code of Federal Regulations (“C.F.R.”). These regulations may be accessed at the website noted immediately above. Please note that administrative regulations are revised from time-to-time and the latest version of the regulations is not always timely updated on a government website.

<sup>2</sup> Pub. L. No. 111-5. ARRA Division A, Title XIII – Health Information Technology, beginning at §13001 is the Health Information Technology for Economic and Clinical Health Act, also known as the “HITECH Act.” The text of the HITECH Act as of February 17, 2009 is available at [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111\\_cong\\_public\\_laws&docid=f:publ005.111.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_public_laws&docid=f:publ005.111.pdf).

- Treatment, Payment, and Health Care Operations;
- Certain situations when there is an opportunity for the Individual to agree or object orally;
- Public health, legal, law enforcement, and certain other activities; and
- Which an authorization is required.
- Individual rights, including the right to:
  - Notice of privacy practices;
  - Access to review/copy PHI;
  - Request a restriction on uses and disclosures of PHI;
  - Amend PHI; and
  - Request an accounting of disclosures of PHI;
- Administrative requirements, such as:
  - Appointing privacy and security officers;
  - Providing HIPAA training to Workforce members;
  - Responding to complaints from Individuals;
  - Sanctioning Workforce members who violate HIPAA policies and procedures;
  - Adopting safeguards to protect the privacy of PHI;
  - Mitigating any harmful effect of a use or disclosure of PHI in violation of HIPAA and HIPAA policies and procedures;
  - Adopting HIPAA policies and procedures; and
  - Documenting certain actions relating to HIPAA compliance and retaining such documentation.
- Maintaining the security of electronic protected health information (“EPHI”), including procedures for reporting security breaches and administrative, physical, and technical safeguards for protecting EPHI.

*Remember, there is no one-size fits all. The HIPAA regulations allow a Covered Entity to develop policies and procedures unique to its size and type of organization.*

## B. HIPAA's Scope

**Covered Entities.** HIPAA does not apply to all healthcare-related agencies that create, use, or disclose identifiable health information. Instead, to be regulated under HIPAA, the agency must be a "Covered Entity". Covered Entities include certain health care providers, health plans, and health care clearinghouses.<sup>3</sup>

**Health Care Providers.** Health care providers include institutional providers such as hospitals, nursing homes, and home health agencies, as well as individual practitioners, including physicians, providers of diagnostic tests, outpatient physical therapy, certified nurse-midwife services, qualified psychologist services, clinical social worker services, and other services.

**What Makes a Health Care Provider a Covered Entity under HIPAA?** Health care providers are not automatically covered under HIPAA. Instead, in order to be covered, they must transmit health information in electronic form using certain electronic standards (required under the HIPAA standard transaction regulations<sup>4</sup>). These standards include billing/claims for health care benefits, encounters, Payments, referrals, eligibility inquiries, and similar financial transactions related to health care benefits.

More specifically, only health care providers *who bill for their services using an electronic transaction* are covered. To help make this determination, the SSA should ask two basic questions:

1. Does the SSA furnish, bill, or receive Payment for health care on a patient encounter or claims basis? If no, it is not a Covered Entity. If yes, go to #2.
2. Does the SSA transmit (send) any transaction related to #1 electronically? If no, the SSA is not a Covered Entity. If yes, then it is a Covered Entity.

Note that if the SSA outsources the electronic processing of healthcare claims and billing transactions to a third party, it is still a Covered Entity.

Here are some examples of who is and who is not a HIPAA Covered Entity:

- SSAs that provide health care services using grant funds and do **not** bill clients' insurers are **not** HIPAA Covered Entities.
- SSAs that bill insurers but do so using only paper claim forms and do not bill insurers using a HIPAA standard electronic transaction also are **not** covered under HIPAA.

---

<sup>3</sup> Health care clearinghouses are entities that process health information received from one entity in a nonstandard format into standard data elements or a standard transaction. 45 C.F.R. § 160.103.

<sup>4</sup> See 45 C.F.R. Part 162, Subparts F through R.

- SSAs that have some grant funding but bill insurers using a standard electronic transaction for some services **are** covered under HIPAA.
- SSAs that communicate via email that may include PHI (e.g., a psychiatrist at an SSA receives requests from patients to prescribe medications) but do not bill insurers using a standard electronic transaction are **not** covered under HIPAA.

**Protected Health Information (“PHI”).** The HIPAA privacy and security regulations described in this Primer apply only to Protected Health Information or PHI. PHI is information which singly or in combination identifies a person and relates to the past, present, or future:

- Physical or mental health or condition of that person;
- Provision of health care to that person; or
- Payment for provision of health care to that person.<sup>5</sup>

**Business Associates.** Under HIPAA, Business Associates assist or provide a service to Covered Entities and use or disclose PHI in the process, and, for that reason, are required to have HIPAA requirements applied to them – but through the terms of their contracts with a Covered Entity. A Business Associate is a person or entity that, on behalf of a Covered Entity, performs, or assists in the performance of, a function or activity involving the use of PHI, including but not limited to claims processing or administration, data analysis, utilization review, quality assurance, billing, or benefit management that involves the use or disclosure of PHI. A person or entity also will be considered a Business Associate if such person or entity provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a Covered Entity, if, in doing so, such person or entity receives PHI.<sup>6</sup>

- If a SSA uses an outside person or entity to perform services like those listed above, then it should have entered into a Business Associate agreement with that person or entity. Please consider contacting legal counsel for assistance in using the proper form of agreement.
- If a SSA provides these types of services to a Covered Entity and has Access to PHI from that entity, then the SSA likely is a Business Associate of that entity. Even if the SSA considered itself a Covered Entity when performing its normal functions, it still is considered a Business Associate when performing services for another Covered Entity.
  - If an agency is a Business Associate, the SSA likely already has entered into a Business Associate agreement with that entity. In any event, as of February 2010, Business Associates will be required to comply with many

---

<sup>5</sup> 45 C.F.R. § 160.103.

<sup>6</sup> 45 C.F.R. § 160.103.

of the HIPAA standards described below. The regulations for Business Associates are expected to be revised and in effect by February 10, 2010.

**Employer Group Health Plans.** HIPAA does not apply to employers, even though they may have medical information relating to items such as sick notes, workplace health testing, disabilities, and life insurance. However, to the extent that an employer sponsors a group health plan, HIPAA applies only to such plan. If an employer, on behalf of its group health plan, amends its group health plan documents and complies with other requirements, the employer may use and disclose PHI relating to its group health plan to administer the group health plan, including determining what benefits to offer, including wellness programs. When doing so, the employer must comply with its plan document amendments, including provisions specifying that the employer must safeguard the PHI and may not use it for employment-related determinations. A more detailed discussion of how HIPAA regulates employer group health plans is beyond the scope of this primer.<sup>7</sup>

### **C. If a Social Services Agency is not a HIPAA Covered Entity, What Next?**

Even if HIPAA does not apply to a particular SSA, the SSA still needs to safeguard any identifiable health information it has. First, the agency (or the health care practitioners on its staff) may be required to do so by state law. For example, HIV/AIDS and substance abuse laws require strict privacy of individual information. SSAs may also have the social security number of its clients on file and certain privacy laws apply to that information.<sup>8</sup>

Second, to the extent an SSA has a privacy policy on its website explaining how the agency uses and protects identifiable health information, the Federal Trade Commission requires the SSA to comply with such policy.<sup>9</sup> Third, if an SSA does not safeguard such information, it will lose the trust of its clients and risk adverse public relations.

If they haven't done so already, SSA directors should consider adopting privacy and security policies and practices for safeguarding identifiable health information or enhancing existing policies and procedures. Given that the HIPAA standards have been effective for a number of years, these standards now can be considered a model for protecting identifiable health information. Please keep in mind, however, that the HIPAA standards do not preempt (i.e., supersede) state law that is more stringent.

---

<sup>7</sup> See 45 C.F.R. §§ 164.504(f), .530(k).

<sup>8</sup> See Primer on Selected Federal, Connecticut, New Jersey and New York Privacy, Identity Theft and Information Security Laws Relevant to Charitable and Other Nonprofit Organizations, available at [www.probonopartnership.org/publications.htm](http://www.probonopartnership.org/publications.htm).

<sup>9</sup> See, for example, *In The Matter of Eli Lilly and Company*, at [www.ftc.gov/os/caselist/0123214/0123214.shtm](http://www.ftc.gov/os/caselist/0123214/0123214.shtm). The legal proceeding against Eli Lilly was brought under Section 5(a) of the Federal Trade Commission Act.

## D. For Covered Entities, Which Law Applies? HIPAA or State Law?<sup>10</sup>

**HIPAA Establishes A “Floor.”** The HIPAA privacy standards provide a minimum “floor” of national privacy standards designed to protect against inappropriate use and disclosure of PHI. States may provide additional protections above this floor.

The HIPAA standards generally preempt contrary state laws, unless an exception applies. Some exceptions include state laws requiring reporting of a disease or injury, child abuse, birth, or death, or for the conduct of public health. These state laws remain in place – HIPAA does not preempt them.

**More Stringent.** If a state law regulates the privacy or security of health information and is “more stringent” than the HIPAA privacy and security regulations, the state law will not be preempted – meaning that the SSA will need to comply with the state law. A state law relating to privacy or security will be considered “more stringent” than the HIPAA privacy and security standards if the state law meets at least one of the following six criteria:

- The state law prohibits or restricts uses and disclosures of PHI that would otherwise be permitted by the HIPAA standards;
- The state law permits Individuals greater rights of access to or amendment of PHI;
- The state law permits greater disclosure/notice of information to an Individual who is the subject of PHI about use, disclosure, rights, and remedies relating to such PHI, including disclosures relating to data security breaches;
- With respect to an authorization/release of records form, the state law narrows the scope or duration, increase the privacy protections afforded, or reduces the coercive effect of the circumstances surrounding the authorization, as applicable;
- With respect to record keeping or requirements relating to accounting of disclosures, the state law requires retention or reporting of more detailed information or for a longer duration; or
- With respect to any other matter, the state law provides greater privacy or security protections for the person who is the subject of the PHI.<sup>11</sup>

---

<sup>10</sup> Some health care providers may be subject to both HIPAA and the federal confidentiality of substance abuse patient records statute (42 U.S.C. 290dd-2 and its implementing regulation, 42 C.F.R. Part 2). As noted in the preamble to the final HIPAA privacy regulations, in most cases there is no conflict between the rules. The HIPAA rules permit a health care provider to disclose PHI in a number of situations, but do not require such disclosure. Therefore, if a disclosure is permitted under HIPAA, but prohibited under the federal substance abuse patient record rules, the provider would comply with the federal substance abuse requirements. See 65 Fed. Reg. at 82482–83 (December 28, 2000).

<sup>11</sup> 45 C.F.R. § 160.202.

**What Remains?** These rules generally mean that state laws providing increased protection for certain types of records (for example, those relating to HIV/AIDS, genetic information, and behavioral/mental health information) generally are not preempted by the HIPAA standards and Covered Entities must comply with them, as applicable. In addition, to the extent state laws require reporting or permits greater patient access to their PHI, these laws also will not be preempted and therefore must be followed.

In any event, please consider contacting legal counsel for assistance in determining whether a specific state privacy or security-related law would be preempted or considered “more stringent.”

### **E. HIPAA’s Privacy and Security Regulations – Which Applies and What are the Differences?**

The HIPAA *privacy regulations* apply to all types of PHI: oral, paper, and electronic. The privacy regulations apply to all Covered Entities and generally address who has Access to PHI, for what purpose, how uses and disclosures of PHI are to be managed, what records must be developed, and who must be trained, among other things.

By contrast, the HIPAA *security regulations* apply only to electronic PHI. The security regulations apply to all Covered Entities and address administrative, physical, and technical measures (for example, user IDs, passwords, locked cabinets, and information security policies and procedures) to keep electronic PHI safe from intrusions on its Integrity, confidentiality, and accessibility.

The privacy regulations are discussed below in Sections II – IV. The security regulations are discussed below in Section VI.

## **II. Privacy – Restrictions on Uses and Disclosures of PHI**

The HIPAA privacy regulations restrict how Covered Entities may use and disclose PHI. In particular, Covered Entities may not use or disclose PHI except as permitted or required under the regulations.<sup>12</sup> Generally, Covered Entities may use and disclose PHI for Treatment, Payment, and Health Care Operations, as those terms are defined in the regulations.<sup>13</sup> Certain other uses and disclosures of PHI require a signed authorization from the Individual whose PHI is involved, while others require Covered Entities to follow specific requirements (for example disclosures relating to litigation, research, and law enforcement). All PHI, including oral, paper, and electronic PHI, is subject to the HIPAA privacy standards.

---

<sup>12</sup> 45 C.F.R. § 164.502(a).

<sup>13</sup> 45 C.F.R. §§ 164.502, .501(definitions).

## A. When Can a Covered Entity Use and Disclose PHI?<sup>14</sup>

The HIPAA regulations address in great detail permitted uses and disclosures of PHI. A complete discussion of all such permitted uses and disclosures (or restrictions on uses and disclosures) is beyond the scope of this Primer. We encourage Covered Entities to consult with legal counsel regarding these details of the privacy regulations. Generally, Covered Entities are permitted to use and disclose PHI for several purposes or situations, including for Treatment, Payment, and Health Care Operations.

- **Treatment, Payment, and Health Care Operations.** In particular, PHI may be used and disclosed for the:
  - Covered Entity's own Treatment, Payment, and Health Care Operations activities;
  - Treatment activities of any health care provider having a relationship with the Individual;
  - Payment activities of another Covered Entity or health care provider having a relationship with the Individual; and
  - Health Care Operations of another Covered Entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities (if both entities have a relationship with the Individual).<sup>15</sup>
  
- **Opportunity to Agree or Object.** PHI may be used and disclosed under certain limited circumstances when the Individual has been given the opportunity to agree or object to the use and disclosure.<sup>16</sup> The following circumstances fall under this category:
  - **Facility Directories:** Covered Entities may rely on an Individual's oral permission to list in its facility directory his or her name, general condition, religious affiliation, and location in the provider's facility. If the Individual does not object, the Covered Entity may then disclose the Individual's condition and location in the facility to anyone asking for the Individual by name, and also may disclose the Individual's religious affiliation to clergy.
  - **Disclosures to Person's Involved in an Individual's Care:** Covered Entities may rely on an Individual's informal permission to disclose PHI to persons whom the Individual identifies as being involved with his/her care or Payment for care. Similarly, Covered Entities may rely on an Individual's informal permission to use or disclose PHI for the purpose of notifying family members and others regarding Individual's location, general condition, or

---

<sup>14</sup> 45 C.F.R. § 164.502(a).

<sup>15</sup> 45 C.F.R. § 164.506(c).

<sup>16</sup> 45 C.F.R. § 164.510.

death. One example of a disclosure to a person involved in a patient's care would be a pharmacist dispensing a filled prescription to a person acting on behalf of the patient.

- **Emergency Situations.** When the Individual is incapacitated or in an emergency situation, Covered Entities generally may use and disclose PHI if, in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the Individual.
- **Public Health, Legal, Law Enforcement, and Certain Other Activities.** Covered Entities are permitted, although not required, to use and disclose PHI, without an Individual's authorization/permission, for a number of purposes. The HIPAA privacy regulations include very specific procedures relating to each type of use or disclosure mentioned below, and Covered Entities should review the regulations before disclosing PHI for these types of activities.<sup>17</sup>

Specifically, Covered Entities may use and disclose PHI for the activities described below, as long as all the requirements listed in the regulations are met:

- If use or disclosure is required by law (for example, state laws requiring reporting of gunshot wounds, communicable diseases, and child and elder abuse);
- For public health activities to:
  - ✓ a public health authority authorized to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability;
  - ✓ a public health authority authorized to receive reports of child abuse and neglect;
  - ✓ a person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity and has responsibility for quality, safety, or effectiveness of such product or activity;
  - ✓ a person who may have been exposed to a communicable disease or who may be at risk of contracting or spreading a disease or condition (if notification is authorized by law)
  - ✓ employers, regarding employees, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with certain laws.
- To a health oversight agency for oversight activities authorized by law;

---

<sup>17</sup>

45 C.F.R. § 164.512.

- In the course of a judicial or administrative proceeding if certain conditions are met;
  - For a law enforcement purpose to a law enforcement official if certain conditions are met;
  - To funeral directors and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law;
  - To facilitate the donation and transplantation of cadaveric organs, eyes, and tissue;
  - For Research provided that the Covered Entity obtains certain approval, documents, or representations;
  - When disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public;
  - For certain essential government functions (for example, assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, protecting the President); and
  - To comply with workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.<sup>18</sup>
- **Disclosing an Individual's Own PHI to the Individual.** An authorization is not required when an Individual requests to review/copy his or her own PHI. See Section III.B below.
  - **Personal Representatives.** Except under limited circumstances, a Covered Entity must treat a personal representative as the Individual for purpose of the privacy regulations. For example, if state law permits a parent or guardian to act on behalf of a minor Individual, the Covered Entity must treat such person as the personal representative with respect to PHI relevant to that minor Individual, including for purposes of signing authorizations and exercising the rights described in Section III.<sup>19</sup>
  - **Uses and Disclosures for Which an Authorization is Required.** A Covered Entity must obtain the Individual's written authorization for any use or disclosure of PHI that is not otherwise permitted under HIPAA, that is, not for Treatment,

---

<sup>18</sup> 45 C.F.R. § 164.512.

<sup>19</sup> 45 C.F.R. § 164.502(g). A Covered Entity may elect not to treat a person as the personal representative of an Individual if the Covered Entity has a reasonable belief that the Individual has been or may be subjected to domestic violence, abuse, or neglect by such person; treating such person as the personal representative could endanger the Individual; and the Covered Entity, in the exercise of professional judgment, decides that it is not in the best interest of the Individual to treat the person as the Individual's personal representative.

Payment, or Health Care Operations or not for one of the permitted uses or disclosures listed above.

- **What Items Must be Included in an Authorization?** Authorizations must be in writing, use plain language, and contain specific information regarding:
  - ✓ the information to be disclosed or used;
  - ✓ the person(s) disclosing the information;
  - ✓ the person(s) receiving the information;
  - ✓ the purpose of the disclosure;
  - ✓ an expiration date or event;
  - ✓ the right to revoke the authorization in writing; and
  - ✓ certain other information and statements.<sup>20</sup>

Covered Entities are encouraged to develop their own authorization form and seek the advice of legal counsel as needed.

- **Specific Uses and Disclosures that Require Authorization.**<sup>21</sup>

- **Psychotherapy Notes.** Using and disclosing Psychotherapy Notes always requires an authorization, except for certain limited situations. These exceptions include the following: A Covered Entity may use or disclose the Psychotherapy Notes:
  - ✓ for treating patients;
  - ✓ for its own training and to defend itself in legal proceedings brought by the Individual;
  - ✓ for the Department of Health and Human Services to investigate or determine the Covered Entity's compliance with HIPAA;
  - ✓ to avert a serious and imminent threat to public health or safety;
  - ✓ to a health oversight agency for lawful oversight of the originator of the Psychotherapy Notes;

---

<sup>20</sup> 45 C.F.R. § 164.508.

<sup>21</sup> 45 C.F.R. § 164.508. The other statements include informing the Individual that the information released may no longer be protected by the HIPAA privacy regulations. 45 C.F.R. § 164.508.

- ✓ for the lawful activities of a coroner or medical examiner; and
  - ✓ as required by applicable federal or state law.
- **Marketing.**<sup>22</sup> An authorization is required for most “marketing” activities, except that an authorization is not required for face-to-face marketing communications between a Covered Entity and an Individual, and for a Covered Entity’s provision of promotional gifts of nominal value. No authorization is needed to make a communication that falls within one of the exceptions to the marketing definition. Marketing is discussed in more detail in Section V.C below.
- **The Minimum Necessary Standard.** HIPAA requires Covered Entities to adhere to the “Minimum Necessary” standard for uses and disclosures.<sup>23</sup> Under this standard, Covered Entities, may only use, disclose, and request the minimum amount of identifiable health information necessary for the task at hand. Covered Entities are required to develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary amount.
  - **Business Associate Use and Disclosure of PHI.** Business Associates may only use and disclose PHI on behalf of the Covered Entity and may not use PHI for their own purposes, except that Business Associates are permitted to use PHI for administration, for management, and to carry out their own legal responsibilities. HIPAA requires the Covered Entity to enter into a contract with the Business Associate which must include certain protections for the information.<sup>24</sup> Covered Entities are encouraged to develop their own template for a Business Associate Agreement and seek advice from legal counsel as appropriate.

Under the HITECH Act, as of February 2010, Business Associates will be required to comply with most of the HIPAA privacy and security requirements.<sup>25</sup>

- **De-identification of PHI.** If PHI is de-identified in accordance with one of the two de-identification methods listed in the HIPAA privacy regulation, then the de-identified information may be used or disclosed for any purpose and no longer is considered PHI.<sup>26</sup> Therefore, if possible, it is always to a Covered Entity's advantage to either de-identify PHI or not retain PHI for an Individual. This may not be possible when records retention rules or policies require the original PHI to be retained.

---

<sup>22</sup> 45 C.F.R. §§ 164.508, .501 (definitions).

<sup>23</sup> 45 C.F.R. §§ 164.502(b), 164.514(d).

<sup>24</sup> 45 C.F.R. § 164.504(e). See Section V.D below.

<sup>25</sup> See Section V.D below.

<sup>26</sup> 45 C.F.R. § 164.514.

In addition, Covered Entities may disclose PHI to a Business Associate so that the Business Associate may de-identify the information in accordance with the two methods.<sup>27</sup>

The two de-identification methods are:

- A determination by a qualified statistician: The statistician must have “appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable.” This person must apply such principles and methods and determine that “the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an Individual who is a subject of the information.”
- “The safe harbor”: the removal of 18 specified identifiers of the Individual and of the Individual’s relatives, household members, and employers is required, and is adequate only if the Covered Entity has no actual knowledge that the remaining information could be used to identify the Individual. Some of these identifiers include:
  - ✓ Names, street addresses, birthdates, social security numbers;
  - ✓ Geographic subdivisions smaller than a State;
  - ✓ Dates of service, telephone numbers, fax numbers;
  - ✓ Email addresses;
  - ✓ Medical record numbers, account numbers; and
  - ✓ Any other unique identifying number, characteristic, or code.<sup>28</sup>
- **Limited Data Set.** A “limited data set” is PHI from which certain specified direct identifiers of Individuals have been removed. A limited data set is generally used and disclosed only for Research purposes or for public health or Health Care Operations. A Covered Entity that discloses a limited data set for these purposes must obtain “satisfactory assurance,” in the form of a data use agreement that meets the requirements in the HIPAA regulations, including that the recipient of the limited data set will only use or disclose the PHI for limited purposes. A limited data set may include the following identifiers (while fully de-identified data may not include these identifiers):
  - ✓ Five digit zip codes (and any other geographic subdivision, such as a state, county, city, precinct, except street address);

---

<sup>27</sup> 45 C.F.R. § 164.502(d)(1).

<sup>28</sup> 45 C.F.R. § 164.514.

- ✓ Dates of birth and death; and
- ✓ Dates of admission or discharge.<sup>29</sup>

### **III. Privacy – Individual Rights**

Under the HIPAA privacy regulations, Individuals have a number of rights relating to their PHI maintained by a Covered Entity (including their Business Associates). Covered Entities are required to respond to Individuals' requests relating to these rights. The regulations specify in extensive detail how Covered Entities must handle requests from Individuals to exercise these rights. Business Associates must assist Covered Entities in responding to such requests if they have the PHI that is responsive to such requests. The following discussion summarizes each of these rights.

#### **A. Right to Notice of Privacy Practices**

Individuals have the right to adequate notice of the uses and disclosures of PHI made by the Covered Entity, and of their rights and the Covered Entity's duties with respect to their PHI.<sup>30</sup>

**What Should the Notice Say?** The "Notice of Privacy Practices" must be written in plain language and contain specified elements, including but not limited to a header, descriptions of uses and disclosures of PHI, a statement of Individuals' rights regarding their PHI, cover entities' duties regarding PHI, and other elements required by law.<sup>31</sup> The notice must be updated if there is a material change to the Covered Entity's policies and procedures or, for example, when there is a change in law or regulation that affects a provision in the notice.

**When to Provide Notice?** A Covered Entity must provide the notice to Individuals on request. Covered health providers with direct Treatment relationship with Individuals must:

- In a non-emergency Treatment situation, provide the notice no later than the date of the first service delivery to the Individuals. Covered Entities must make a good faith effort to obtain a written acknowledgment of receipt of the notice and, if not obtained, document such good faith efforts and the reason why the acknowledgement was not obtained.
- In an emergency Treatment situation, provide the notice as soon as reasonably practicable after the emergency Treatment situation.

---

<sup>29</sup> 45 C.F.R. § 164.514(e).

<sup>30</sup> Business Associates are not required to develop and distribute their own "Notices of Privacy Practices."

<sup>31</sup> 45 C.F.R. § 164.520.

- Have the notice available at the physical service delivery site, for instance, posting the notice on wall.

**Electronic Notice.** A Covered Entity that maintains a web site must prominently post its notice on its web site. A Covered Entity may provide notice to Individuals by e-mail if the Individual agrees to electronic receipt of the notice.<sup>32</sup>

## **B. Right of Access to Review/Copy PHI**

Individuals have the right to inspect and obtain copies of their PHI.<sup>33</sup> However, the right of access does not apply to PHI:

- that is not maintained by a Covered Entity or Business Associate in a Designated Record Set;
- that is compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;
- that was obtained under a promise of confidentiality;
- that is Psychotherapy Notes; or
- that is excepted from access by more stringent state (e.g., HIV) or federal laws.

**Can a Covered Entity Require Individuals to Make a Written Request for Copies of Their Records?** Yes, as long as the Covered Entity informs Individuals of such requirements.

### **How Quickly Must a Covered Entity Respond to Such Requests?**

- A Covered Entity must inform the Individual that his/her request has been accepted or denied no later than 30 days after receiving the request, or 60 days if the requested information is not on-site.
- A Covered Entity may extend the deadline (once) by no more than 30 days by providing the requesting Individual with a written statement explaining the reasons for the delay.<sup>34</sup>

**How Must a Covered Entity Provide the PHI/Records Requested?** A Covered Entity must provide the PHI requested in the form or format it was requested, or other form or format agreed to by the Covered Entity and the Individual. If the Individual agrees, the Covered Entity may provide the Individual with an explanation or summary of the requested information.

---

<sup>32</sup> 45 C.F.R. § 164.520.

<sup>33</sup> 45 C.F.R. § 164.524.

<sup>34</sup> 45 C.F.R. § 164.524.

- Under the HITECH Act, when requested by the Individual, a Covered Entity that uses Electronic Health Records (as defined under this Act), must produce a copy of the person's PHI in electronic format. Also, if the Individual so chooses, the Covered Entity must transmit the copy directly to an entity or person designated by the Individual, provided that the request is clear, conspicuous, and specific. A Covered Entity may charge a fee for providing electronic access to the information, but the fee may not be greater than the Entity's labor costs in responding to the request.<sup>35</sup>

**May a Covered Entity Charge the Individual for the Copies and/or Providing the Information?** Yes. A Covered Entity may charge a reasonable, cost-based fee, including only the cost of copying, postage, and preparing an explanation or summary.

**May a Covered Entity Deny an Individual's Request for Copies/Access?** Yes, in limited circumstances. A Covered Entity may deny an Individual copies/access on certain grounds, including that the PHI is Psychotherapy Notes, is compiled in anticipation of a legal proceeding, or was obtained from someone else under a promise of confidentiality, or that a licensed health care professional has determined such request is reasonably likely to endanger the Individual or other persons.<sup>36</sup>

**May an Individual Seek a Review of the Denial?** Sometimes. Whether an Individual can seek a review of the denial of an access request hinges on the grounds on which a Covered Entity denied the request. Certain grounds for denial are reviewable and others are not.

**What if the Covered Entity Denies the Request?** To the extent possible, the Covered Entity must give the Individual access/copies of any other PHI requested, inform the Individual of the his or her review rights, and describe how the Individual may complain about or appeal (if applicable) the denial.<sup>37</sup> If the Covered Entity does not maintain the information requested, but knows where the information is maintained, for instance, at the location of another healthcare provider, the Covered Entity must inform the Individual where to direct the request for access.<sup>38</sup>

### **C. Right to Request a Restriction on Uses and Disclosures of PHI**

Individuals have the right to ask a Covered Entity to restrict certain uses or disclosures of their PHI.

---

<sup>35</sup> HITECH Act, Section 13405(e).

<sup>36</sup> 45 C.F.R. § 164.524.

<sup>37</sup> To the extent a denial is reviewable and an Individual requests a review of the denial of access, the Covered Entity must designate a licensed health care professional who was not directly involved in the denial to review the decision to deny access. 45 C.F.R. § 164.524(a)(4).

<sup>38</sup> 45 C.F.R. § 164.524.

**Must a Covered Entity Agree to a Restriction?** No. A Covered Entity is not required to agree to a restriction.<sup>39</sup>

- Exception: Under the HITECH Act, however, a health care provider must agree when an Individual asks the provider not to use or disclose his/her PHI to a health plan for purposes of Payment or Health Care Operations (the disclosure is not for the purpose of carrying out Treatment) and the PHI pertains solely to a health care service for which the provider has been paid out of pocket in full.<sup>40</sup>

**What if a Covered Entity Agrees to a Request for a Restriction?** A Covered Entity that agrees to a restriction may not use or disclose PHI in violation of such restriction, except when such information is needed to provide emergency Treatment to such Individual.<sup>41</sup>

**How Can a Covered Entity Terminate a Restriction?** The Covered Entity may terminate its agreement to a restriction, if:

- the Individual agrees to or requests the termination in writing; and
- the Covered Entity informs the Individual that it is terminating the restriction, except that such termination will be effective only with respect to information not yet created or received.<sup>42</sup>

**Can Individuals Request Confidential Communication?** Yes. Individuals can request to receive communication of PHI from Covered Entities in a confidential manner, for instance, receiving communications of PHI by alternative means or at alternative locations (other than their homes).

**Must a Covered Entity Provide Confidential Communication Upon Request?** Yes. A Covered Entity must accommodate reasonable requests from Individuals.

**Can a Covered Entity Set Up Conditions on Providing Confidential Communication?** Yes. A Covered Entity can establish conditions on which it will provide confidential communication. But the Covered Entity cannot require an explanation from an Individual about why the person needs confidential communication.<sup>43</sup>

---

<sup>39</sup> 45 C.F.R. § 164.522(a).

<sup>40</sup> HITECH Act, Section 13405(a).

<sup>41</sup> To the extent a disclosure is required by law (for example, reporting of certain diseases), a Covered Entity could not agree to an Individual's request not to make such a disclosure without violating the applicable law.

<sup>42</sup> 45 C.F.R. § 164.522(a)(2).

<sup>43</sup> 45 C.F.R. § 164.522(b)(2).

## D. Right to Amend PHI

Individuals have the right to ask Covered Entities to amend their PHI.<sup>44</sup>

**Can a Covered Entity Require Individuals to Request Amendments in Writing and to Provide a Reason?** Yes, as long as the Covered Entity informs Individuals in advance.

### **How Quickly Must a Covered Entity Respond to Such Requests?**

- A Covered Entity must respond to an Individual's requests for an amendment no later than 60 days after receipt of the request.
- A Covered Entity may extend the deadline (once) by no more than 30 days by providing the Individual with a written statement explaining the reasons for the delay.

**May a Covered Entity Deny a Request for an Amendment of PHI?** Yes, if the Covered Entity determines that the PHI:

- Was accurate and complete;
- Was not created by the Covered Entity, unless the Individual provides a reasonable basis to believe that the originator of PHI is no longer available to respond to the requested amendment; or
- Was not part of a Designated Record Set (which means that the PHI generally was not used by the Covered Entity for Treatment determinations).<sup>45</sup>

**What if a Covered Entity Accepts a Request for an Amendment?** The Covered Entity must make appropriate amendments to the PHI as required by the regulation, inform the Individual, and inform others, including persons who have received the Individual's PHI from them previously.

### **What if a Covered Entity Denies a Request for an Amendment?**

- The Covered Entity must provide the requesting Individual with a timely, written denial, using plain language and containing specified elements required by the regulation.
- The Covered Entity must permit the requesting Individual to submit a written statement of disagreement.
- The Covered Entity may prepare written rebuttal to the statement of disagreement.

---

<sup>44</sup> 45 C.F.R. § 164.526.

<sup>45</sup> 45 C.F.R. § 164.526.

- If an Individual submits a statement of disagreement, the Cover Entity must append/link the statement of disagreement and the rebuttal (if any) to the record so that future disclosures include these materials.<sup>46</sup>

**What if the Covered Entity is Informed by Another Covered Entity of an Amendment?** If a Covered Entity receives an amendment from another provider, the Covered Entity must amend the Individual's PHI so that it includes the amendment. To the extent a Business Associate has access to the relevant PHI, the Covered Entity must notify the Business Associate of the amendment.<sup>47</sup>

## **E. Right to an Accounting of Disclosures of PHI**

Individuals have the right to receive accountings (lists) of disclosures of PHI made by Covered Entities in the six years prior to the date of request.<sup>48</sup>

**Can a Covered Entity Require Individuals to Make a Written Request for an Accounting?** Yes, as long as the Covered Entity informs Individuals of such requirements in advance.

**Are There any Exceptions?** Yes. A Covered Entity is **not** required to account for disclosures of PHI to carry out Treatment, Payment, and Health Care Operations, disclosures pursuant to an authorization, or under certain other circumstances.<sup>49</sup> This means that prior to the effective date of the relevant section of the HITECH Act, Covered Entities only have to track and account for certain types of disclosures, including disclosures pursuant to court orders and disclosures relating to public health.

- **Note:** As a result of the HITECH Act, as of either January 1, 2011 or 2014 (the earlier date applies if the Covered Entity used an electronic health record prior to January 1, 2009), if a Covered Entity has an "electronic health record" (as defined in the HITECH Act), the Covered Entity must track and, if a Individual requests an accounting, account for disclosures made for the purposes of Treatment, Payment, and Health Care Operations (as well as other types of disclosures not excepted).<sup>50</sup> This expanded right to an accounting applies to disclosures made during three years prior to the date on which the accounting is requested, rather than the six years permitted under the original HIPAA privacy regulations. With respect to disclosures made by Business Associates on behalf of Covered Entities, the HITECH Act permits Covered Entities either to provide the requesting Individual with an accounting of disclosures of PHI made by the

---

<sup>46</sup> 45 C.F.R. § 164.526.

<sup>47</sup> 45 C.F.R. § 164.526(c)(3).

<sup>48</sup> 45 C.F.R. § 164.528.

<sup>49</sup> 45 C.F.R. § 164.528.

<sup>50</sup> "Electronic health record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. HITECH Act, Section 13400(5).

Covered Entity's Business Associates, or to provide a list and contact information for all relevant Business Associates. The Individual would then be able to contact the Business Associates for an accounting.<sup>51</sup> This expanded right to an accounting likely will be very burdensome for healthcare providers.

**What Must be Included in an Accounting of Disclosures?** The accounting must include:

- Disclosures of PHI that occurred during the six years prior to the date of the request, including the disclosures to or by Business Associates;
- Disclosures of PHI that occurred during the three years prior to the date of the request, including the disclosures to or by Business Associates, in the case of a Covered Entity with an electronic health record; and
- The date of the disclosures, the name of the entities or persons who received the information, a brief description of the information and a statement of the purpose of disclosures, and other information required by the regulation.<sup>52</sup>

**How Quickly Must a Covered Entity Respond to Such Requests?**

- A Covered Entity must respond to Individual's request no later than 60 days after receiving it.
- A Covered Entity may extend the deadline (once) by no more than 30 days by providing the Individual with a written statement explaining the reasons for the delay.

**Can a Covered Entity Impose a Fee for Providing an Accounting?**

- A Covered Entity must provide the first accounting to any Individual in any 12-month period without charge; and
- The Covered Entity may impose a reasonable, cost-based fee for each subsequent request by the same Individual within the same 12-month period, provided that the Covered Entity informs the Individual in advance of the fee, and provides the Individual with an opportunity to withdraw or modify the request.

---

<sup>51</sup> HITECH Act, Section 13405(c).

<sup>52</sup> 45 C.F.R. § 164.528(b)(2).

## **IV. Privacy – Administrative Requirements**<sup>53</sup>

### **A. Privacy Officer**

Each Covered Entity must designate a privacy officer responsible for the development and implementation of the Covered Entity's policies and procedures. A Covered Entity also must designate a contact person or office that will be responsible for receiving complaints and providing further information about matters covered by the "Notice of Privacy Practices". Usually, the privacy officer assumes the role of the contact person.

### **B. Training**

A Covered Entity is required to train all members of its Workforce (who are involved with PHI) regarding its HIPAA policies and procedures.<sup>54</sup> Training should be provided to new members of the Workforce and periodically thereafter to all employees whose job functions mean they do or may have Access to PHI. Training should also be provided to employees when their jobs change or after there is any material change in an agency's policies and procedures for HIPAA compliance.

### **C. Safeguards**

A Covered Entity must implement reasonable safeguards to protect PHI from any use or disclosure that would violate the HIPAA requirements. See Sections V and VI below.

### **D. Complaints**

A Covered Entity must provide a process for Individuals to complain about the Covered Entity's privacy policies and procedures. Individuals also have the right to complain to the United States Department of Health and Human Services. As of June 2009, approximately 45,000 privacy-related complaints had been submitted to this Department.

### **E. Sanctions**

A Covered Entity must have and apply appropriate sanctions against employees who fail to comply with the Covered Entity's privacy policies and procedures.

### **F. Mitigation**

A Covered Entity must mitigate, to the extent practicable, any harmful effect that is known to the Covered Entity of a use or disclosure of PHI in violation of the Covered Entity's privacy policies and procedures, or the HIPAA privacy regulations. For example, if a fax containing PHI has been sent to the wrong number, the Covered Entity would contact the person who received it and ask them to destroy it. The fax cover sheet also would include instructions if the person who received it is not the intended recipient.

---

<sup>53</sup> 45 C.F.R. § 164.530.

<sup>54</sup> "Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity, is under the direct control of such entity, whether or not they are paid by the Covered Entity. 45 C.F.R. § 160.103.

## **G. Refraining from Intimidating or Retaliatory Acts**

A Covered Entity may not intimidate or take other retaliatory actions against any Individual for exercising his or her privacy rights, including filing a complaint.

## **H. Policies and Procedures**

A Covered Entity must implement policies and procedures for implementing the privacy requirements. The policies and procedures should generally address the administrative requirements in this Section IV as well as the key requirements of both the HIPAA privacy and the security regulations. Various documents, such as the “Authorization Form” and the “Notice of Privacy Practices”, should also be kept with the policies and procedures. A Covered Entity must change its policies and procedures as necessary to comply with changes in the law.

## **I. Documentation**

A Covered Entity must:

- Maintain the PHI-related policies and procedures (including documentation of all security safeguards) in written or electronic forms and make them accessible to all Workforce members who are working with or may work with PHI.
- Maintain HIPAA-related communications in written or electronic forms if retention is required under the regulations, including all authorization forms, copies of its “Notice of Privacy Practices,” Individuals’ requests for access, restrictions, amendments, and accountings of disclosures, and the Covered Entity’s responses to these requests, including any denials.
- Maintain an action, activity, or designation required (by the regulations) to be documented in written or electronic form, such as designation of privacy officers, training logs, sanctions imposed on Workforce members who violate the policies or HIPAA regulations, complaints (including documentation on how complaints have been resolved), and Business Associate agreements.
- Retain all this documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.

## **J. Group Health Plans**

The privacy regulations contain additional requirements applicable only to group health plans; these requirements are not addressed in this Primer.<sup>55</sup>

---

<sup>55</sup> 45 C.F.R. §§ 164.504(f), 164.530(k).

## V. Other HIPAA or HITECH Requirements

### A. **Notifying Individuals Regarding Breaches of Their Unsecured PHI**

**Breach.** As defined under the HITECH Act, with certain exceptions, “breach” means the acquisition, Access, use, or disclosure of oral, paper, or electronic PHI in a manner not permitted under the privacy regulations which compromises the security or privacy of such information<sup>56</sup> “Compromises the security and privacy” of PHI means “poses a significant risk of financial, reputational, or other harm to the individual.”<sup>57</sup> This means that not all impermissible uses or disclosures of PHI need to be reported. Instead, Covered Entities and Business Associates must perform a risk assessment to determine whether there is a significant risk of harm to the Individual as a result of the impermissible use or disclosure.

**Notification.** As of September 23, 2009, Covered Entities are required to report to Individuals any breaches of unsecured PHI (as defined under the HITECH Act and regulations issued under it).<sup>58</sup> Covered Entities are required to report breaches to Individuals without unreasonable delay after discovery of the breach.<sup>59</sup> Except under very limited circumstances, notifications must be made no later than sixty calendar days after discovery of the breach.<sup>60</sup> The notice must be:

- In writing to the last known address of the Individual via first class mail (or via e-mail if specified by the Individual);
- By substitute notice where the contact information is insufficient or out-of-date (for example, the notice is returned as undeliverable), including, where there are ten or more Individuals with insufficient information, conspicuous posting on the home page of the website of the Covered Entity or in major print or broadcast media for a period determined by the Secretary of the Department of Health and Human Services (“DHHS”);

---

<sup>56</sup> 45 C.F.R. § 164.402; HITECH Act, Section 13400(1).

<sup>57</sup> 74 Fed. Reg. 42740, 67 (August 24, 2009) (citing 45 C.F.R. § 164.402). A use or disclosure of PHI that does not include the identifiers required to be deleted for a “limited data set” in 45 C.F.R. § 164.514(e)(2) that also does not include dates of birth and zip codes does not compromise the security or privacy of the PHI. 74 Fed. Reg. 42740, 67.

<sup>58</sup> HITECH Act, Section 13402(a). Compliance is required by September 23, 2009, but DHHS noted that the Office of Civil Rights (“OCR”) will use its enforcement discretion, and not impose sanctions for failing to provide notice for breaches that are discovered 180 days from August 24. 74 Fed. Reg. 42740, 56-7. During the initial time period – after the rule has taken effect but before DHHS imposes sanctions – DHHS expects covered entities to comply with the regulations and will work with covered entities, through technical assistance and voluntary corrective action, to achieve compliance. 74 Fed. Reg. 42740.

<sup>59</sup> HITECH Act, Section 13402(c); 45 C.F.R. § 164.404(a).

<sup>60</sup> HITECH Act, Section 13402(d); 45 C.F.R. § 164.404(b).

- By telephone or other method where there is a possibility of imminent misuse;
- To prominent print or broadcast media outlets in states or geographic areas where the Individuals affected by the breach likely reside if the breach is reasonably believed to affect more than 500 residents of that state or geographic area;
- To the Secretary of DHHS (1) immediately for breaches involving more than 500 Individuals and (2) annually for all other breaches; and
- By the Secretary of DHHS posting on the DHHS website of a list that identifies each Covered Entity involved in a breach in which the unsecured PHI of more than 500 Individuals is acquired or disclosed.<sup>61</sup>

The HITECH Act and the implementing regulations also specify what information must be included in breach notifications, including but not limited to a brief description of what happened, including the date of the breach and the date of the discovery, the types of unsecured PHI that was involved in the breach (for example, social security numbers, addresses), steps Individuals should take to protect themselves from potential harm resulting from the breach, and a brief description of what the Covered Entity is doing to investigate the breach, mitigate losses, and protect against any further breaches.<sup>62</sup>

**Unsecured PHI.** As defined in Guidance issued by the DHHS, “unsecured” PHI means PHI in any form that is not secured by using one of two methods for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals: Encryption and destruction.

“Encryption” means that the “[e]lectronic PHI has been encrypted as specified in the HIPAA security regulations by ‘the use of an algorithmic process to transform data in to a form in which there is a low probability of assigning meaning without use of a confidential process or key’ and such confidential process or key that might enable decryption has not been breached.”<sup>63</sup> The DHHS Guidance mentions two sources describing Encryption processes that will be deemed satisfactory.

“Destruction” means that the “media on which the PHI is stored or recorded has been destroyed in one of the following ways:

- Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise reconstructed; or

---

<sup>61</sup> HITECH Act, Section 13402(e); 45 C.F.R. § 164.404(c).

<sup>62</sup> HITECH Act, Section 13402(f); 45 C.F.R. § 164.404(c).

<sup>63</sup> Department of Health and Human Services, Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of [the HITECH Act] of the ARRA; Request for Information, 74 Fed. Reg. 19006 (April 27, 2009)[hereinafter “DHHS Guidance”]. This Guidance was clarified and reissued in conjunction with the publication of the DHHS Breach Notification Interim Final Rule, 74 Fed. Reg. at 42740, 42–43 (August 24, 2009).

- Electronic Media have been cleared, purged, or destroyed consistent with National Institute of Standards and Technology (“NIST”) Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.”<sup>64</sup>

To the extent PHI has been secured (encrypted or destroyed) as described in the DHHS Guidance, Covered Entities would not have to notify Individuals of any breach of such information.

**Business Associates.** In the event of a breach, Business Associates must provide notice to the Covered Entity, including the identification of each Individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during the breach.<sup>65</sup> The Covered Entity is responsible for notifying Individuals regarding breaches of their unsecured PHI.

## B. Prohibition on Sale of PHI

With certain exceptions, the HITECH Act prohibits Covered Entities and Business Associates from receiving direct and indirect remuneration in exchange for PHI of an Individual without obtaining authorization from the Individual, including a specification whether the PHI may be further exchanged for remuneration by the purchaser receiving the PHI.<sup>66</sup>

## C. Restrictions on Use of PHI for Marketing and Fundraising

**Marketing.** Under the HIPAA privacy regulations, any communication that encourages the recipient to purchase or use a product or service is considered “marketing” and requires an authorization from the Individual, unless it is:

- Made for Treatment of the Individual;
- Made for case management or care coordination for the Individual, or to direct or recommend alternative Treatments, therapies, healthcare providers, or settings of care to the Individual;
- In the form of a face-to-face communication made by a Covered Entity to an Individual; or
- In the form of a promotional gift of nominal value provided by the Covered Entity.<sup>67</sup>

---

<sup>64</sup> DHHS Guidance, 74 Fed. Reg. 19006.

<sup>65</sup> HITECH Act, Section 13402(b).

<sup>66</sup> HITECH Act, Section 13405(d).

<sup>67</sup> 45 C.F.R. § 164.501. The following also are exceptions to the marketing definition: Communications to describe a product or service that is provided by or included in a plan of benefits of the Covered Entity making the communication, including communications about the

If a marketing communication involves direct or indirect remuneration to the Covered Entity from a third party, the authorization must state that such remuneration is involved.

“Marketing” also includes (and an authorization therefore is required) an arrangement between a Covered Entity and any other entity whereby the Covered Entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or services.<sup>68</sup>

As a result of the HITECH Act, as of February 17, 2010, additional restrictions will be imposed on a Covered Entity that receives compensation for a communications. In particular, a Covered Entity will not be permitted to receive direct or indirect payment in exchange for making such communications, unless

- Such payment is for a communication regarding a drug currently prescribed for the recipient of the communication, and such payment is reasonable (to be interpreted in DHHS regulations);
- The communication is made by the Covered Entity, and the Covered Entity obtains a valid authorization from the Individual; or
- The communication is made by a Business Associate of a Covered Entity, on behalf of such Covered Entity, and such communication is consistent with the applicable Business Associate agreement.<sup>69</sup>

**Fundraising.** Under the current HIPAA regulations, a Covered Entity may use only certain information for the purpose of raising funds for its own benefit, without a written, HIPAA-compliant authorization from the Individual. In particular, the Covered Entity may use only demographic information relating to an Individual, as well as the dates that health care was provided to the Individual, for this purpose. This means that a hospital could use this type of information to send fundraising materials to all patients treated at a particular time or to a category of patients (for example, female patients). But if the Hospital is building a new cardiac wing, it may not solicit funds from patients who received cardiac treatment without first obtaining a written authorization from each such patient.

Also, any written fundraising communication (using only demographic and date of care information) must include an opportunity for the recipient to opt out or elect not to receive any further fundraising communications.<sup>70</sup> Under the HITECH Act, as of February 17, 2010, if a person opts out, it must be treated as a revocation of a prior HIPAA authorization form (used when a use or disclosure is not permitted without explicit

---

entities participating in a healthcare provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits. 45 C.F.R. § 164.501.

<sup>68</sup> 45 C.F.R. § 164.501.

<sup>69</sup> HITECH Act, Section 13406(a).

<sup>70</sup> 45 C.F.R. § 164.514(f).

Individual consent) signed by the person.<sup>71</sup> All authorization forms and opt-out elections must be retained by Covered Entities for at least six years. This increases the importance of tracking opt-outs from fundraising communications.

#### **D. Business Associates and the HITECH Act**

**Application of HIPAA Regulations to Business Associates.** Currently, the HIPAA regulations do not apply directly to Business Associates. Instead, Covered Entities are required to obtain “satisfactory assurances” that the Business Associate will appropriately safeguard PHI. These “assurances” must be documented in the form of a Business Associate agreement between the Covered Entity and each of its Business Associates. The HIPAA privacy and security regulations each list numerous provisions that must be included in Business Associate agreements. To the extent Business Associates release PHI to their own vendors, they must have “downstream” agreements with these vendors, obligating them to comply with the same requirements in the Business Associate’s agreement with the Covered Entity.<sup>72</sup>

However, as a result of the HITECH Act, as of February 17, 2010, many of the HIPAA privacy and security requirements will apply directly to Business Associates, including provisions relating to application of the civil and criminal penalties described in Section VII below. This means that if a Business Associate breaches a provision of its Business Associate agreement with a Covered Entity, it also may have violated the HIPAA requirements and will be subject to penalties. To the extent an SSA is a Business Associate to a Covered Entity (and not a Covered Entity itself), the SSA will need to develop a HIPAA compliance program.<sup>73</sup>

Covered Entities are encouraged to develop their own template for a Business Associate Agreement and seek advice from legal counsel as appropriate.

## **VI. Security Regulations**

### **A. Introduction**

The HIPAA security regulations specify a series of administrative, physical, and technical standards to be used by Covered Entities to protect the confidentiality, accessibility, and Integrity of their **electronic** PHI, referred to as “E PHI” in this Section VI.<sup>74</sup> The standards are highly technical, and Covered Entities generally work with their information technology staff or consultants to develop a HIPAA security regulation compliance program.

The standards are divided into either “required” or “addressable” Implementation Specifications -- instructions on how to implement each standard. If an Implementation

---

<sup>71</sup> HITECH Act, Sections 13401 and 13404.

<sup>72</sup> 45 C.F.R. §§ 164.502(e) and 164.504(e).

<sup>73</sup> HITECH Act, Section 13406(b).

<sup>74</sup> 45 C.F.R. §§ 164.302 - .318.

Specification is labeled “addressable,” then the Covered Entity must analyze whether it is a reasonable and appropriate safeguard for the entity’s EPHI. In particular, the Covered Entity must assess whether the specification likely would protect the Covered Entity’s EPHI from reasonably anticipated threats and hazards. If the Covered Entity chooses not to implement an addressable specification based on this type of assessment, it must document its reasoning for not implementing it, and, if reasonable and appropriate, implement an equivalent alternative measure.

If an Implementation Specification is labeled “required,” the Covered Entity must implement it.

Each of the three categories of safeguards – administrative, physical and technical – is discussed separately below. We do not discuss every safeguard, but instead describe a number of safeguards in each of the three categories. The Implementation Specifications are indented.<sup>75</sup> In some cases, requirements under the HIPAA security regulations should already be addressed by policies and procedures developed under the HIPAA privacy regulations – adjustments would need to be made based on the extent of EPHI and the scope of the Covered Entities’ IT or computer systems.

Remember, there is no one-size fits all. The HIPAA regulations allow a Covered Entity to develop policies and procedures unique to its size and type of organization.

## **B. Administrative Safeguards<sup>76</sup>**

Administrative Safeguards are actions, policies, and procedures that manage the selection, development, implementation, and maintenance of security measures to protect EPHI and manage the conduct of a Covered Entity’s Workforce in relation to the protection of that information. This category of safeguards contains over half of the HIPAA security requirements.

**Security Management Process:** Covered Entities must implement policies and procedures to prevent, detect, contain, and correct security violations. The risk analysis and risk management Implementation Specifications discussed below are extremely important because they form the foundation for a HIPAA security compliance program.

### **Risk Analysis (Required)**

Covered Entities must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, Integrity, and availability of EPHI held by the Covered Entity. The overall objective of a HIPAA risk analysis is to document the potential risks and vulnerabilities to the confidentiality, Integrity, or availability of EPHI and determine the appropriate safeguards to bring the level of risk to an acceptable and manageable level, as determined by the Covered Entity taking into account the types of EPHI held by the Covered Entity and the identified risks and vulnerabilities to the EPHI.

---

<sup>75</sup> Some of the safeguards do not have separate implementation specifications because instructions are not needed for those safeguards.

<sup>76</sup> 45 C.F.R. § 164.308.

The security regulations do not require that any particular method be used for conducting a risk analysis. Nonetheless, most risk analyses contain the following steps:

**EXAMPLE RISK ANALYSIS STEPS:<sup>77</sup>**

1. Identify the scope of the analysis;
2. Gather data;
3. Identify and document potential threats and vulnerabilities;
4. Assess current security measures;
5. Determine the likelihood of threat occurrence (high, medium, and low);
6. Determine the potential impact of threat occurrence (high, medium, and low);
7. Determine the level of risk (high, medium, and low); and
8. Identify security measures to lower the risks and their impact; and
9. Finalize documentation of the risk analysis.

A risk analysis must take into account all of a Covered Entity's EPHI, regardless of its source or location (e.g., in the possession of a Business Associate). Covered Entities must identify where the EPHI is stored, received, maintained, and transmitted. Possible methods for gathering relevant data include reviewing all systems and applications, reviewing past or existing projects (including previous risk analyses), interviewing relevant IT and professional staff, and reviewing documentation, including existing security policies and procedures. Covered Entities then must identify all potential threats and vulnerabilities, and then determine which threats and vulnerabilities can be reasonably anticipated. For most entities, human threats will be of greatest concern.

After all reasonably anticipated threats and vulnerabilities are identified, Covered Entities must review and document their existing security measures. Security measures can be both technical and nontechnical. Technical measures are part of information systems hardware and software. Examples of technical measures include Access controls and identification, authentication, and Encryption methods. Non-technical measures are management and operational controls, such as policies, procedures, or standards, and physical and environmental security measures.

Once Covered Entities have determined all reasonably anticipated threats and vulnerabilities and have assessed their current security measures, they will have the information needed to determine the likelihood that a threat will trigger or

---

<sup>77</sup> Example provided by: National Institute of Standards and Technology, *Risk Management Guide for Information Systems Technology*, at pages 8-26 (July 2002), available at <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.

exploit a specific vulnerability and the resulting impact on the Covered Entity. Covered Entities should consider each potential threat and vulnerability combination and rate them by the probability that the combination will actually occur. Some common risks include unauthorized Access to EPHI, temporary or permanent loss of EPHI, and loss of physical assets. The impact of each potential outcome should be measured to assist the entity in prioritizing risk mitigation activities.

Next, Covered Entities must determine the level of risk to EPHI. The level of risk is determined by analyzing the values assigned to the likelihood of threat occurrence and the resulting impact of threat occurrence. The risk level determination may be performed by assigning a risk level based on the average of the assigned likelihood and impact levels. For each risk, entities should identify the type of response needed to reasonably and appropriately reduce the risk to acceptable levels, and a general timeline for implementing the response.

Finally, once the specific actions necessary to manage risks are determined, Covered Entities are required to document the risk analysis.

#### **Risk Management (Required)**

Covered Entities must implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate manner. This often involves strengthening existing security measures and implementing new ones. Risk management naturally follows risk analysis, and is the process of implementing the specific actions identified in the risk analysis as necessary for security regulation compliance. Both risk analysis and risk management are on-going processes, and must be adaptable to changing environmental or operational conditions.

#### **Sanction Policy (Required)**

Covered Entities must apply appropriate sanctions against Workforce members who fail to comply with security policies and procedures. A sanction policy should include a range of disciplinary actions based on the severity of the violation. A Covered Entity should have already developed this under the HIPAA privacy regulations.

#### **Information System Activity Review (Required)**

Covered Entities must implement procedures to regularly review records of information system activity, such as audit logs, Access reports, and Security Incident tracking reports. The purpose of this specification is to enable entities to determine if any EPHI has been used or disclosed in an unauthorized manner.

**Assigned Security Responsibility:** Covered Entities must identify a security official/officer who is responsible for the development and implementation of the policies and procedures required by the security regulations.

**Workforce Security:** Covered Entities must implement policies and procedures to ensure that all members of its Workforce have appropriate Access to EPHI, and to prevent unauthorized Workforce members from obtaining Access. For each Workforce member who needs Access to EPHI to carry out their duties, the entity must identify the

EPHI that is needed, when it is needed, the identity of the employee, and the computer systems and applications that provide Access to the information.

**Workforce Clearance Procedure (Addressable)**

When reasonable and appropriate, Covered Entities must implement procedures to determine whether the Access of a Workforce member to EPHI is appropriate. The clearance process must establish the procedures to verify that a Workforce member does in fact have the appropriate Access for their job function.

**Information Access Management:** Covered Entities must implement policies and procedures for authorizing Access to EPHI. The purpose of this standard is to minimize the risk of inappropriate disclosure, alteration, or destruction of EPHI.

**Access Authorization (Addressable)**

When reasonable and appropriate, Covered Entities must implement policies and procedures for granting Access to EPHI through Access to a Workstation, transaction, program, process, or other mechanism. In general, Covered Entities must identify who has authority to grant Access privileges and the process for granting Access.

**Security Awareness and Training:** Covered Entities must implement a security awareness and training program for all Workforce members. Training should be provided to new members of the Workforce and periodically thereafter to all employees whose job functions mean they do or may have Access to PHI. In addition, periodic retraining should be given whenever environmental or operational changes affect the security of EPHI (such as new or updated policies, new or upgraded software and hardware, or new security technology).

**Security Reminders (Addressable)**

When reasonable and appropriate, Covered Entities must implement periodic security updates. Security reminders may take many forms, including emails regarding new viruses, spyware, worms, and other Malicious Software.

**Protection from Malicious Software (Addressable)**

When reasonable and appropriate, Covered Entities must implement procedures for guarding against, detecting, and reporting Malicious Software.

**Log-in Monitoring (Addressable)**

When reasonable and appropriate, Covered Entities must implement procedures for monitoring log-in attempts and reporting discrepancies. Many information systems can be set to identify multiple unsuccessful attempts to log-in or record log-in attempts in an audit trail.

**Password Management (Addressable)**

When reasonable and appropriate, Covered Entities must implement procedures for creating, changing, and safeguarding passwords. Entities should also ensure that their Workforce members are trained on how to safeguard their passwords, and should establish guidelines for creating passwords and changing them during periodic password change cycles.

**Security Incident Procedures:** Covered Entities must implement policies and procedures to address Security Incidents. Security Incident procedures must address how to identify Security Incidents, including to whom such incidents must be reported.

**Response and Reporting (Required)**

Covered Entities must identify and respond to suspected or known Security Incidents, mitigate (to the extent practicable) the harmful effects of Security Incidents that are known to the entity, and document Security Incidents and their outcomes. Possible Security Incidents an entity may encounter include:

- Stolen or inappropriately obtained passwords used to Access EPHI.
- Virus attacks that interfere with the operations of information systems with EPHI.
- Physical break-ins leading to the theft of Electronic Media with EPHI.
- Stolen or lost laptops, memory sticks, and other portable Electronic Media.

**Contingency Plan:** Covered Entities must establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain EPHI. The goal of such policies and procedures is to ensure that organizations will have their EPHI available whenever it is needed.

**Data Backup Plan (Required)**

Covered Entities must establish and implement procedures to create and maintain retrievable exact copies of EPHI. Many entities have backup procedures as a part of their current business practices.

**Disaster Recovery Plan (Required)**

Covered Entities must establish and implement as needed procedures to restore any loss of data. The plan should address what data is to be restored. A copy of the plan should be readily accessible at more than one location.

**Periodic Review of Security Measures:** Covered Entities must perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the security regulations and, subsequently, in response to environmental or operational changes affecting the security of EPHI.

**Business Associate Contracts:** Covered Entities are required to document the satisfactory assurances required through written contract with the Business Associate that meet the applicable Organizational Requirements (see Section V.D above).

### **C. Physical Safeguards<sup>78</sup>**

Physical Safeguards are physical measures, policies, and procedures that protect Covered Entities' electronic information systems and related buildings and equipment from natural and environmental hazards, as well as from unauthorized intrusions.

---

<sup>78</sup> 45 C.F.R. § 164.310.

**Facility Access Controls:** Covered Entities must implement policies and procedures to limit physical Access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized Access is allowed.

**Contingency Operations (Addressable)**

When reasonable and appropriate, Covered Entities must establish and implement procedures that allow facility Access in support of restoration of lost data under the required disaster recovery plan in the event of an emergency.

**Facility Security Plan (Addressable)**

When reasonable and appropriate, Covered Entities must implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical Access, tampering, and theft. Facility security plans must document the use of physical Access controls that ensure that only authorized individuals have Access to the facility. Some common physical Access controls include:

- Locked doors, signs warning of restricted areas, surveillance cameras, and alarms.
- Property controls such as property control tags or engravings on equipment.
- Personnel controls such as ID badges, visitor badges, and security escorts.

**Workstation Use and Security:** Covered Entities must implement policies and procedures that specify the proper function to be performed, the manner in which these function are to be performed, and the physical attributes of the surroundings of a specific Workstation or class of Workstations that can Access EPHI. These safeguards must also extend to off-site Workstations that can Access EPHI (including employees working from home or satellite offices). Common practices to safeguard Workstation use include logging off before leaving a Workstation for an extended period of time, and using and continually updating antivirus software.

**Device and Electronic Media Controls:** Covered Entities must implement policies and procedures that govern the receipt and removal of hardware and Electronic Media containing EPHI into and out of a facility, as well as within the facility.

**Disposal (Required)**

Covered Entities must implement policies and procedures to address the final disposition of EPHI, and/or the hardware or Electronic Media on which it is stored. Disposed Electronic Media must be unusable or inaccessible.

**Electronic Media Re-Use (Required)**

Covered Entities must implement procedures for the removal of EPHI from Electronic Media before the media is made available for re-use. Instead of disposing of Electronic Media, entities may choose to re-use it when appropriate in order to save costs. This standard applies to internal re-use (such as re-deployment of PCs or sharing of floppy disks) as well as external re-use (such as the donation of Electronic Media to charities or local schools).

**Data Backup and Storage (Addressable)**

When reasonable and appropriate, Covered Entities must create retrievable exact copies of EPHI before the movement of equipment.

**D. Technical Safeguards<sup>79</sup>**

Technical Safeguards are defined as the technology and the policies and procedures for its use that protect EPHI and control Access to it.

**Access Control:** Covered Entities must implement technical policies and procedures for electronic information systems that maintain EPHI to allow Access only to those persons or software programs that have been granted Access rights.

**Unique User Identification (Required)**

Covered Entities must assign a unique name and/or number for identifying and tracking user identities.

**Emergency Access Procedure (Required)**

Covered Entities must establish and implement as needed procedures for obtaining necessary EPHI during an emergency.

**Automatic Logoff (Addressable)**

When appropriate and reasonable, Covered Entities must implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

**Encryption and Decryption (Addressable)**

When appropriate and reasonable, Covered Entities must implement a mechanism to encrypt and decrypt EPHI. Encryption is a method of converting an original message of regular text into encoded text by means of an algorithm, resulting in a low probability that anyone other than the receiving party would be able to decrypt the text and convert it into plain text.

**Audit Controls:** Covered Entities must implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.

**Integrity:** Covered Entities must implement policies and procedures to protect EPHI from improper alteration or destruction.

**Person or Entity Authentication:** Covered Entities must implement procedures to verify that a person or entity seeking Access to EPHI is the one claimed. There are a few basic ways to provide proof of identity for authentication, including using a password, PIN, or biometric such as a fingerprint.

**Transmission Security:** Covered Entities must implement technical security measures to guard against unauthorized Access to EPHI that is being transmitted over an electronic communications network. Covered Entities should review their current methods for transmitting EPHI (such as through email, the Internet, or a private or point-

---

<sup>79</sup> 45 C.F.R. § 164.312.

to-point network), identify the available and appropriate means to protect EPHI as it is transmitted, select appropriate solutions, and document their decisions.

**Integrity Controls (Addressable)**

When appropriate and reasonable, Covered Entities must implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until it is disposed. A primary method of protecting the Integrity of transmitted EPHI is through the use of network communications protocols, which ensure that the data sent matches the data that is received.

**Encryption (Addressable)**

When appropriate and reasonable, Covered Entities must implement a mechanism to encrypt EPHI being transmitted. There are various types of Encryption technology available to Covered Entities, and no single interoperable Encryption solution for communicating over open networks currently exists. As part of its Guidance issued in April 2009, the Department of Health and Human Services listed two Encryption processes that will satisfy the Guidance.<sup>80</sup>

**E. Organizational, Policies and Procedures, and Documentation Requirements<sup>81</sup>**

**Business Associate Agreements:** As is the case with the HIPAA privacy regulations, Covered Entities must have agreements with Business Associates that will have Access to the Covered Entity's EPHI. The Business Associate must include specified provisions under which the Business Associate agrees to safeguard EPHI in its possession.

**Policies and Procedures:** Covered Entities must implement reasonable and appropriate policies and procedures to comply with the security regulations.

**Documentation:** Covered Entities must maintain the policies and procedures implemented to comply with the security regulations in written form and maintain a written record of any action, activity, or assessment which is required by the security regulations to be documented. The documentation must be retained for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

**Availability (Required)**

Covered Entities must make the documentation available (through hard copies or intranet websites) to those persons responsible for implementing the procedures to which the documentation pertains.

**Updates (Required)**

Covered Entities must review documentation periodically, and update it as needed, in response to environmental or operational changes affecting the security of the EPHI. Covered Entities also must manage their documentation so that it reflects the current status of the security plans and procedures implemented to comply with the security regulations.

---

<sup>80</sup> See the DHHS Guidance document discussed above at footnote 63.

<sup>81</sup> 45 C.F.R. §§ 164.314, .316.

## VII. Penalties and Enforcement

Violations of the HIPAA rules can give rise to both civil and criminal penalties. Each type of penalty is discussed below.

### A. Civil Penalties

**Amounts.** Prior to the HITECH Act, the HIPAA statute provided for civil money penalties only for knowing violations. As amended by the HITECH Act, civil money penalties may be assessed for violations caused by willful neglect. Under the HITECH Act, the civil money penalties are now tiered, depending on the nature of the violation:

Tier	Nature of Violation	Range of Penalties	Maximum Penalty
1	Violation unknown or by exercising reasonable diligence would not have known	From \$100 to \$25,000 per each violation for all such violations in a calendar year	\$1.5 million for all violations of this type
2	Violation due to reasonable cause and not willful neglect	From \$1,000 to \$100,000 per each violation for all such violations in a calendar year	\$1.5 million for all violations of this type
3	Violation due to willful neglect, if corrected within thirty days from knowledge of violation	From \$10,000 to \$250,000 per each violation for all such violations in a calendar year	\$1.5 million for all violations of this type
4	Violation due to willful neglect not corrected	From \$50,000 to \$1.5 million per each violation for all such violations in a calendar year	\$1.5 million for all violations of this type

<sup>82</sup>

**Distribution of Civil Penalties Collected.** Any penalties and settlement collections for HIPAA violations must be transferred to DHHS to be used for purposes of HIPAA privacy and security enforcement. In addition, after regulations and reports are finalized as

<sup>82</sup> Penalties Chart, American Health Lawyers Association, Member Briefing, Health Information and Technology Practice Group, HIT in a HITECH World: An Analysis of the HITECH Act, at pages 52-53, citing HITECH Act, Section 13410(d). *Note:* The statutory wording regarding the new tiers is confusing and it is possible that the chart will change if this issue is clarified.

required by the HITECH ACT, a portion of civil money penalties will be paid to Individuals harmed by the acts that constitute HIPAA offenses.<sup>83</sup>

**Audits.** The HITECH Act requires the Secretary of Health and Human Services to conduct periodic audits of Covered Entities and Business Associates to ensure compliance with the HIPAA privacy and security regulations. The Secretary must report annually to certain Congressional Committees regarding the number of audits and, in a summary manner, the audit findings.<sup>84</sup>

**Enforcement Through State Attorneys General.** The HITECH Act greatly enhances enforcement of HIPAA by permitting state attorneys general to commence civil actions on behalf of state residents regarding HIPAA violations occurring after February 17, 2009. This right is in addition to any other powers that the attorney general may have under state law. A state bringing such an action must notify the Secretary of DHHS prior to bringing the action or as soon as feasible after bringing the action. The purpose of the such actions by state attorneys general must be to enjoin further HIPAA violations; or obtain damages on behalf of the state's residents. Damages may be awarded up to \$200.00 per violation with a maximum of \$25,000 for all violations of the identical requirement in a calendar year. An award also may include costs and reasonable attorney fees to the state.<sup>85</sup>

**Corrective Action Plans.** The HITECH Act also confirmed that DHHS has the authority to enter into corrective action plans, without imposing penalties, where a violator did not know or with reasonable diligence would not have known that a violation occurred.<sup>86</sup>

## B. Criminal Penalties

**Penalties.** Criminal penalties for violating HIPAA range from fines of up to \$50,000 and imprisonment for up to one year for a simple violation; to fines of up to \$100,000 and imprisonment for up to five years for an offense committed under false pretenses; and to a fine of up to \$250,000 and imprisonment for up to ten years for an offense committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, gain, or malicious harm.<sup>87</sup>

**Application of Criminal Penalties.** Before the HITECH Act, there was some confusion regarding whether the penalties could be applied only to Covered Entities. The HITECH Act clarified that persons other than Covered Entities may be prosecuted for a HIPAA violation, particularly individuals who, without authorization, obtain or disclose such

---

<sup>83</sup> HITECH Act, Section 13410(c)(2), (3).

<sup>84</sup> HITECH Act, Section 12424(a).

<sup>85</sup> HITECH Act, Section 13410(e).

<sup>86</sup> HITECH Act, Section 13410(f).

<sup>87</sup> 42 U.S.C. § 1320d-6.

information maintained by a Covered Entity, whether or not they are employees of a Covered Entity.<sup>88</sup>

## **VIII. Definitions**

**Access:** The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.<sup>89</sup>

**Administrative Safeguards:** Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect Electronic Protected Health Information and to manage the conduct of the Covered Entity's Workforce in relation to the protection of that information.<sup>90</sup>

**Business Associate:** A person or entity that, on behalf of a Covered Entity, performs, or assists in the performance of, a function or activity involving the use of PHI, including but not limited to claims processing or administration, data analysis, utilization review, quality assurance, billing, or benefit management that involves the use or disclosure of PHI. A person or entity also will be considered a Business Associate if such person or entity provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a Covered Entity, if, in doing so, such person or entity receives PHI.<sup>91</sup>

**Covered Entity:** A health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA standard electronic transaction, such as a claim or eligibility inquiry.<sup>92</sup>

**Designated Record Set:** A group of records maintained by or for the Covered Entity that is (i) the medical records and billing records about Individuals maintained by or for a covered health care provider; (ii) the enrollment, Payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the Covered Entity to make decisions about Individuals.<sup>93</sup>

**Electronic Media:** (1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as a magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines,

---

<sup>88</sup> HITECH Act, Section 13409.

<sup>89</sup> 45 C.F.R. § 164.304.

<sup>90</sup> 45 C.F.R. § 164.304.

<sup>91</sup> 45 C.F.R. § 160.103.

<sup>92</sup> 45 C.F.R. § 160.103.

<sup>93</sup> 45 C.F.R. § 164.501.

dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.<sup>94</sup>

**Electronic Protected Health Information:** PHI that is transmitted by Electronic Media; or maintained in Electronic Media.<sup>95</sup>

**Encryption:** A method of converting an original message of regular text into encoded text by means of an algorithm, resulting in a low probability that anyone other than the receiving party would be able to decrypt the text and convert it into plain text.<sup>96</sup>

**Health Care Operations:** Any of the following activities of the Covered Entity to the extent that the activities are related to covered functions:

- (1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about Treatment alternatives; and related functions that do not include Treatment;
- (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, evaluating health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, and accreditation, certification, licensing, or credentialing activities;
- (3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 45 C.F.R. § 164.514(g) are met, if applicable;
- (4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

---

<sup>94</sup> 45 C.F.R. § 160.103.

<sup>95</sup> 45 C.F.R. § 160.103.

<sup>96</sup> 45 C.F.R. § 164.304.

- (5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, and development or improvement of methods of Payment or coverage policies; and
- (6) Business management and general administrative activities of the entity, including, but not limited to:
  - (i) Management activities relating to implementation of and compliance with the HIPAA regulations;
  - (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that Protected Health Information is not disclosed to such policy holder, plan sponsor, or customer;
  - (iii) Resolution of internal grievances;
  - (iv) The sale, transfer, merger, or consolidation of all or part of the Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity, and due diligence related to such activity; and
  - (v) Consistent with the applicable requirements of 45 C.F.R. § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the Covered Entity.<sup>97</sup>

**Implementation Specification:** Specific requirements or instructions for implementing a Standard.<sup>98</sup>

**Individual:** The person who is the subject of Protected Health Information.<sup>99</sup>

**Integrity:** The property that data or information have not been altered or destroyed in an unauthorized manner.<sup>100</sup>

**Malicious Software:** Any program that harms information systems, such as viruses, spyware, and worms.<sup>101</sup>

---

<sup>97</sup> 45 C.F.R. § 164.501.

<sup>98</sup> 45 C.F.R. § 160.103.

<sup>99</sup> 45 C.F.R. § 160.103.

<sup>100</sup> 45 C.F.R. § 164.304.

<sup>101</sup> 45 C.F.R. § 164.304.

**Payment:**

- (1) The activities undertaken by:
  - (i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
  - (ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and
- (2) The activities in paragraph (1) of this definition relate to the Individual to whom health care is provided and include, but are not limited to:
  - (i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
  - (ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;
  - (iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
  - (iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
  - (v) Utilization review activities, including precertification and preauthorization of services, and concurrent and retrospective review of services; and
  - (vi) Disclosure to consumer reporting agencies of any of the following Protected Health Information relating to collection of premiums or reimbursement:
    - (A) Name and address;
    - (B) Date of birth;
    - (C) Social security number;
    - (D) Payment history;
    - (E) Account number; and
    - (F) Name and address of the health care provider and/or health plan.<sup>102</sup>

**Physical Safeguards:** Physical measures, policies, and procedures to protect a Covered Entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.<sup>103</sup>

---

<sup>102</sup> 45 C.F.R. § 164.501.

<sup>103</sup> 45 C.F.R. § 164.304.

**Protected Health Information:** Information that identifies an Individual, is created or received by a Covered Entity, and relates to: the past, present, or future physical or mental health or condition of that Individual; provision of health care to that Individual; or Payment for provision of health care to that Individual.

**Psychotherapy Notes:** Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy Notes do not include medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of Treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the Treatment plan, symptoms, prognosis, and progress to date.<sup>104</sup>

**Research:** A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.<sup>105</sup>

**Security Incident:** The attempted or successful unauthorized Access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.<sup>106</sup>

**Treatment:** The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.<sup>107</sup>

**Technical Safeguards:** The technology and the policy and procedures for its use that protect Electronic Protected Health Information and control Access to it.<sup>108</sup>

**Workforce:** Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity, is under the direct control of such entity, whether or not they are paid by the Covered Entity.<sup>109</sup>

---

<sup>104</sup> 45 C.F.R. § 164.501.

<sup>105</sup> 45 C.F.R. § 164.501.

<sup>106</sup> 45 C.F.R. § 164.304.

<sup>107</sup> 45 C.F.R. § 164.501.

<sup>108</sup> 45 C.F.R. § 164.304.

<sup>109</sup> 45 C.F.R. § 160.103.

**Workstation:** An electronic computing device (for example, a laptop or desktop computer) or any other device that performs similar functions, and Electronic Media stored in its immediate environment.<sup>110</sup>

---

IRS Circular 230 Disclosure: To ensure compliance with requirements imposed by the IRS, we inform you that any tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or any other U.S. federal tax law or (ii) promoting, marketing, or recommending to another party any transaction or matter addressed herein.

This document is provided as a general informational service to volunteers, clients, and friends of the *Pro Bono Partnership*. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does distribution of this document create an attorney-client relationship.

Copyright 2009 Dechert LLP. All rights reserved. No further use, copying, dissemination, distribution, or publication is permitted without the express written permission of Dechert LLP.

September 2009

---

<sup>110</sup> 45 C.F.R. § 164.304.