COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual 2024
Health Insurance Portability and Accountability Act of 1996

By Gabriel Imperato,[1] Esq., CHC; Anne Novick Branan,[2] Esq., CHC; Richard Sena[3] ; and Megan Speltz,[4] JD

Fast Facts

Title of law: Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Category: Privacy

Public law: Pub. L. 104–191

Year enacted: 1996

Major amendments: HIPAA Privacy Rule (2003); HIPAA Security Rule (2005); Enforcement Rule (2006); Health Information Technology for Economic and Clinical Health Act (2009); Omnibus Final Rule (2013)

Enforcement agency: U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR)

Link to full text of law: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

Applies to: All health plans, healthcare clearinghouses, healthcare providers, and endorsed sponsors of the Medicare prescription drug discount card, including business associations that supply services and certain functions for covered entities that have access to personal health information.

What Is the Health Insurance Portability and Accountability Act of 1996?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. It consists of a number of rules that lay out different requirements for HIPAA compliance. The Privacy Rule[5] dictates how, when, and under what circumstances personal health information (PHI) can be used and disclosed. The Security Rule[6] sets the minimum standards to safeguard electronic PHI (ePHI). The Breach Notification Rule[7] requires covered entities to provide notification to affected individuals, the Department of Health & Human Services (HHS) Secretary, and the media (under specific circumstances) if there is a breach of unsecured PHI; and business associates must notify covered entities if a breach occurs at or by the associates.[8] The Omnibus Rule made clarifications to the HIPAA Privacy and Security rules and improved the ability of the Office for Civil Rights (OCR) to enforce HIPAA, while also implementing the mandates of the Health Information

Technology for Economic and Clinical Health (HITECH) Act.[9] The Enforcement Rule[10] established how OCR can determine liability and impose civil monetary penalties for HIPAA violations.[11]

HIPAA was enacted to:

- Improve portability and continuity of health insurance coverage
- Combat waste, fraud, and abuse in health insurance and healthcare delivery
- Promote the use of medical savings accounts
- Improve access to long-term care services and coverage to simplify the administration of health insurance[12]

The act consists of five titles. Title I protects health insurance coverage for workers and their families when they change or lose their jobs. Title II, known as the Administrative Simplification provisions, requires the establishment of national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans, and employers. This title is also known as the Privacy rule. Title III sets guidelines for pretax medical spending accounts. Titles IV and V set guidelines for group health plans and company-owned insurance policies.

Violations of HIPAA generally result from the following:

- Lack of adequate risk analyses
- Lack of comprehensive employee training
- Inadequate business associate agreements
- Inappropriate disclosures of PHI
- Ignorance of the minimum necessary rule
- Failure to report breaches within the prescribed time frame

History

HIPAA was enacted by the 104th Congress and signed into law by President Bill Clinton in 1996. When the act was originally passed, it only required the Secretary of HHS to propose standards that would protect individually identifiable health information. The initial proposed "Code Set" standards were not published until 1999, with the first proposals for the Privacy Rule being established in 2000.

Since its original passage, HIPAA legislation has evolved significantly. The language of the act has been modified to address changes in technology, and the scope has shifted to include third-party service providers (business associates) that perform a function on behalf of a HIPAA-covered entity that involves the use or disclosure of PHI. Each of the major rules were passed throughout the early 2000s and build out various requirements of HIPAA compliance.

Related Laws

Preemption of State Law, 45 C.F.R. § 160, Subpart B

HIPAA provides a minimum set of requirements states must follow in protecting individuals' PHI. With respect to these minimums, states cannot pass laws contrary to the HIPAA rules, unless one of the following exceptions apply:

- The law relates to the privacy of PHI and provides greater privacy protection or rights.
- The law provides for the reporting of disease or injury; child abuse; birth or death; or public health surveillance, investigation, or intervention.
- The law requires certain health plan reporting (e.g., financial audits). However, a covered entity is not required to comply with parts of the law that are contrary to HIPAA.[13]

Examples of State Laws Not Preempted by HIPAA

Cal. Health & Safety Code § 123110 (West 2020)

- Healthcare providers must allow patients to inspect their medical records within five business days from the request (as opposed to 30 days under HIPAA).
- A copy of the medical record must be sent to the patient within 15 days from the request.

Fla. Stat. § 501.171 (West 2020)

- Decreases the outer time limit for individual notification of a breach from 60 days to 30 days.

N.Y. Pub. Health § 18 (McKinney 2020)

- Healthcare providers must allow patients to inspect their medical records within 10 business days from the request (as opposed to 30 days under HIPAA).
- A copy of the medical record must be sent to the patient within a reasonable time of the request.

Health Insurance Portability and Accountability Act Compliance Risks

Risk Area: Lack of Adequate Risk Analysis, Policies and Procedures, and Employee Training

> a. A covered entity or business associate must, in accordance with § 164.306:
>
> 1.
>
> i. Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.
>
> ii. Implementation specifications:
>
> A. Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or

business associate.

B. Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

C. Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

3.

i. Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

ii. Implementation specifications:

A. Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

B. Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

C. Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)

(B) of this section.

4.

i. Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

ii. Implementation specifications:

A. Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

B. Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

C. Access establishment and modification (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

5.

i. Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).

ii. Implementation specifications. Implement:

A. Security reminders (Addressable). Periodic security updates.

B. Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

C. Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

D. Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.

6.

i. Standard: Security incident procedures. Implement policies and procedures to address security incidents.

ii. Implementation specification: Response and reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

7.

i. Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

ii. Implementation specifications:

A. Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

B. Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

C. Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

D. Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

E. Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

8. Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.[14]

Context: Central to HIPAA compliance is the preemption of inappropriate access to PHI. HIPAA requires that healthcare organizations conduct a risk analysis, implement policies to curb risk, and implement disciplinary measures against employees who fail to adhere to those policies. Training is also an essential part of HIPAA's breach preemption rules. Healthcare organizations must implement policies that make employees aware of the need to maintain security and what to do in the event a security incident occurs. Additionally, healthcare organizations must be prepared in the event that data centers containing PHI are compromised by properly backing up and protecting data. Lastly, keeping PHI secure is an ongoing process for healthcare organizations, and they must conduct routine evaluations to comply with HIPAA and changes in the organizational and security environment.

Risk Area: Inadequate Business Associate Agreements

> b.
>
> 1. Business associate contracts and other arrangements. A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.
> 2. A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.
> 3. Implementation specifications: Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).[15]

> a.
>
> 1. Standard: Business associate contracts or other arrangements. The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.
> 2. Implementation specifications (Required) -
>
> i. Business associate contracts. The contract must provide that the business associate will -
>
> A. Comply with the applicable requirements of this subpart;

B. In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and

C. Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.

ii. Other arrangements. The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).

iii. Business associate contracts with subcontractors. The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.[16]

Context: HIPAA generally applies to two types of entities: (1) covered entities and (2) business associates.[17] Covered entities include healthcare providers, healthcare clearinghouses, and health plans. Business associates include organizations or persons, and their subcontractors, that transmit PHI to or from covered entities. Because PHI often needs to be transmitted, covered entities contract with business associates to provide these services, and both entities are bound by HIPAA's various rules. In order for these contracts to comply with HIPAA, they must include "satisfactory assurances" that the business associate will protect the PHI. These assurances extend to subcontractors of the business associates, and they include a requirement to report "security incidents" to the covered entity if they arise.

Risk Area: Unauthorized Disclosure

a. Standard: Authorizations for uses and disclosures -

1. Authorization required: General rule. Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

2. Authorization required: Psychotherapy notes. Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

i. To carry out the following treatment, payment, or health care

operations:

A. Use by the originator of the psychotherapy notes for treatment;

B. Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

C. Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and

ii. A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

3. Authorization required: Marketing.

i. Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:

A. A face-to-face communication made by a covered entity to an individual; or

B. A promotional gift of nominal value provided by the covered entity.

ii. If the marketing involves financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved.

4. Authorization required: Sale of protected health information.

i. Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart. (ii) Such authorization must state that the disclosure will result in remuneration to the covered entity.

b. Implementation specifications: General requirements -

1. Valid authorizations.

    i. A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (a)(4)(ii), (c)(1), and (c)(2) of this section, as applicable.

    ii. A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.

2. Defective authorizations. An authorization is not valid, if the document submitted has any of the following defects:

    i. The expiration date has passed or the expiration event is known by the covered entity to have occurred;

    ii. The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable;

    iii. The authorization is known by the covered entity to have been revoked;

    iv. The authorization violates paragraph (b)(3) or (4) of this section, if applicable;

    v. Any material information in the authorization is known by the covered entity to be false.

3. Compound authorizations. An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

    i. An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the

unconditioned authorization.

ii. An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

iii. An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under paragraph (b)(4) of this section does not apply to a compound authorization created in accordance with paragraph (b)(3)(i) of this section.

4. Prohibition on conditioning of authorizations. A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

   i. A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;

   ii. A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

      A. The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

      B. The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and

   iii. A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.

5. Revocation of authorizations. An individual may revoke an authorization provided under this section at any time, provided that

the revocation is in writing, except to the extent that:

i. The covered entity has taken action in reliance thereon; or

ii. If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

6. Documentation. A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).

c. Implementation specifications: Core elements and requirements -

1. Core elements. A valid authorization under this section must contain at least the following elements:

i. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

ii. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

iii. The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

iv. A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

v. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.

vi. Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

2. Required statements. In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

i. The individual's right to revoke the authorization in writing, and either:

A. The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

B. To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.

ii. The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

A. The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or

B. The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.

iii. The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.

3. Plain language requirement. The authorization must be written in plain language.

4. Copy to the individual. If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.[18]

Context: The default rule under HIPAA is that healthcare providers may not use or disclose a patient's PHI without authorization. This rule also governs what makes an effective authorization, which includes a description of the information, names of those authorized to transmit and those authorized to receive the information, a purpose for the authorization, a date or event of expiration, and the individual's signature. Authorizations must also include certain adequate notices to the authorizing individual, and a signed copy must be supplied to the individual.

Risk Area: Minimum Necessary Disclosure Rule

b. Standard: Minimum necessary -

1. Minimum necessary applies. When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

2. Minimum necessary does not apply. This requirement does not apply to:

    i. Disclosures to or requests by a health care provider for treatment;

    ii. Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;

    iii. Uses or disclosures made pursuant to an authorization under § 164.508;

    iv. Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;

    v. Uses or disclosures that are required by law, as described by § 164.512(a); and

    vi. Uses or disclosures that are required for compliance with applicable requirements of this subchapter.[19]

Context: An important subpart of section 164.502 is subsection (b), which is known as the Minimum Necessary Rule. When authorized, a healthcare provider or its business associate may disclose PHI, but only to the extent necessary. The rule does have exceptions for disclosures or requests by a healthcare provider for treatment, disclosures to patients of their own PHI, certain authorized disclosures, compliance investigations, and disclosures required by law (e.g., court orders or subpoenas) or for compliance.

Risk Area: PHI Security Requirements

a. General requirements. Covered entities and business associates must do the following:

    1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

    2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

    3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

4. Ensure compliance with this subpart by its workforce.

b. Flexibility of approach.

    1. Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

    2. In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

        i. The size, complexity, and capabilities of the covered entity or business associate.

        ii. The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

        iii. The costs of security measures.

        iv. The probability and criticality of potential risks to electronic protected health information.

c. Standards. A covered entity or business associate must comply with the applicable standards as provided in this section and in §§ 164.308, 164.310, 164.312, 164.314 and 164.316 with respect to all electronic protected health information.

d. Implementation specifications. In this subpart:

    1. Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.

    2. When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.

    3. When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must –

        i. Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic

protected health information; and

ii. As applicable to the covered entity or business associate -

A. Implement the implementation specification if reasonable and appropriate; or

B. If implementing the implementation specification is not reasonable and appropriate -

1. Document why it would not be reasonable and appropriate to implement the implementation specification; and

2. Implement an equivalent alternative measure if reasonable and appropriate.

e. Maintenance. A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with § 164.316(b)(2)(iii).[20]

Context: Covered entities and business associates are required to implement security measures to protect PHI. These measures must ensure employees are adequately trained in PHI security and must protect against reasonably anticipated threats, unauthorized uses, and unauthorized disclosures. Although HIPAA does not prescribe specific measures and implementation of PHI security, covered entities and business associates must consider their size and security capabilities, infrastructure, cost, and potential risks of their chosen security method.

Risk Area: Required Notification of Breach

a. Standard -

1. General rule. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

2. Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with

the federal common law of agency).

b. Implementation specification: Timeliness of notification. Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

c. Implementation specifications: Content of notification -

    1. Elements. The notification required by paragraph (a) of this section shall include, to the extent possible:

        A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

        B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

        C. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

        D. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

        E. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

    2. Plain language requirement. The notification required by paragraph (a) of this section shall be written in plain language.

d. Implementation specifications: Methods of individual notification. The notification required by paragraph (a) of this section shall be provided in the following form:

    1. Written notice.

        i. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

        ii. If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the

individual (as specified under § 164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

2. Substitute notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).

    i. In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

    ii. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

        A. Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

        B. Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

3. Additional notice in urgent situations. In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.[21]

a. Standard. For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in § 164.404(a)(2), notify prominent media outlets serving the State or jurisdiction.

b. Implementation specification: Timeliness of notification. Except as provided in § 164.412, a covered entity shall provide the notification

required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

c. Implementation specifications: Content of notification. The notification required by paragraph (a) of this section shall meet the requirements of § 164.404(c).[22]

a. Standard. A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary.

b. Implementation specifications: Breaches involving 500 or more individuals. For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in § 164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by § 164.404(a) and in the manner specified on the HHS Web site.

c. Implementation specifications: Breaches involving less than 500 individuals. For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS website.[23]

Context: In the event of a breach, covered entities are required to notify individuals within 60 days of discovering the breach. A breach is considered to be known when any employee or agent of the covered entity discovers the breach or should have discovered the breach had the entity conducted "reasonable diligence." Once discovered, the covered entity must contact the individual via first-class mail and disclose what happened, what information was compromised, and self-protecting steps the individual can take. The rule also requires covered entities to disclose to the affected individual what the entity is doing to investigate the breach, mitigate harm, and protect against further breaches. For breaches affecting more than 500 people, the covered entity must contact prominent media outlets where the affected individuals are located.

Risk Area: Civil Money Penalties

a. The amount of a civil money penalty will be determined in accordance with paragraph (b) of this section, and §§ 160.406, 160.408, and 160.412. These amounts were adjusted in accordance with the Federal Civil Monetary Penalty Inflation Adjustment Act of 1990, (Pub. L. 101-140), as amended by the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, (section 701 of Pub. L. 114-74), and appear at 45 CFR part 102 . These amounts will be updated annually and published at 45 CFR part 102 .

b. The amount of a civil money penalty that may be imposed is subject to the following limitations:

1. For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty -
    i. In the amount of more than $100 for each violation; or
    ii. In excess of $25,000 for identical violations during a calendar year (January 1 through the following December 31);
2. For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty -
    i. For a violation in which it is established that the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision,
        A. In the amount of less than $100 or more than $50,000 for each violation; or
        B. In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31);
    ii. For a violation in which it is established that the violation was due to reasonable cause and not to willful neglect,
        A. In the amount of less than $1,000 or more than $50,000 for each violation; or
        B. In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31);
    iii. For a violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,
        A. In the amount of less than $10,000 or more than $50,000 for each violation; or
        B. In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31);
    iv. For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,

A. In the amount of less than $50,000 for each violation; or

B. In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31).

3. If a requirement or prohibition in one administrative simplification provision is repeated in a more general form in another administrative simplification provision in the same subpart, a civil money penalty may be imposed for a violation of only one of these administrative simplification provisions.[24]

Context: Civil penalties for HIPAA violations depend on both when the violations occurred and the nature of the violation. Violations prior to February 18, 2009, are limited to civil penalties of no more than $100 per violation and no more than $25,000 for the calendar year. Violations on or after February 18, 2009, may range from no less than $100 to no less than $10,000 per violation depending on the nature of the violation. However, the calendar year limit is uniformly set at $1,500,000. The amounts are subject to yearly adjustments in accordance with inflation, and adjusted civil penalty amounts may be found at 45 C.F.R. § 102.3 .

Risk Area: Criminal Penalties

a. Offense:

A person who knowingly and in violation of this part—

1. uses or causes to be used a unique health identifier;

2. obtains individually identifiable health information relating to an individual; or

3. discloses individually identifiable health information to another person,

shall be punished as provided in subsection (b). For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1320d–9(b)(3) of this title) and the individual obtained or disclosed such information without authorization.

b. Penalties:

A person described in subsection (a) shall—

1. be fined not more than $50,000, imprisoned not more than 1 year, or both;

2. if the offense is committed under false pretenses, be fined not more

than $100,000, imprisoned not more than 5 years, or both; and

3. if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.[25]

Context: Criminal liability under HIPAA is appropriate for individuals without authorization who knowingly use, cause to be used, obtain, or disclose individually identifiable health information maintained by a covered entity. Criminal penalties depend on the nature of the offense and the intent of the violator. Maximum limits for the most egregious violations range up to a $250,000 fine and 10 years in prison.