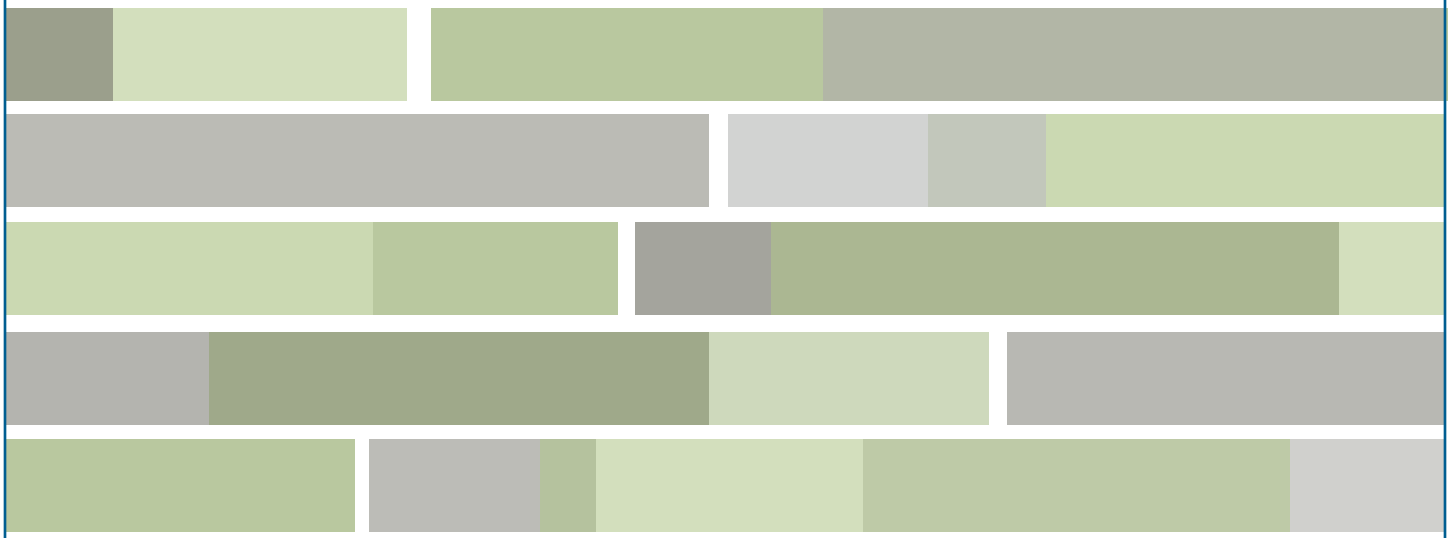
Employee Benefits Series

HIPAA for Health Care Providers



HIPAA for Health Care Providers

The Health Insurance Portability and Accountability Act (HIPAA) requires health care providers to comply with certain rules to ensure the privacy of health information. These rules include the **Privacy**, **Security**, and **Breach Notification Rules**. In addition, health care providers that contract with third parties (which HIPAA calls **"business associates"**) to perform functions involving health information must comply with additional HIPAA rules. Please note that **health care providers that do not comply with HIPAA's rules may face significant penalties**.

IN THIS GUIDE

PRIVACY RULE

The **HIPAA Privacy Rule** establishes a set of national standards to protect the privacy of certain health information that can be linked to a specific person. These standards address the use and disclosure of individuals' health information—called "protected health information," or PHI—by organizations subject to the Privacy Rule, called "covered entities." The Privacy Rule also gives patients certain rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. This subsection will discuss the following topics relevant to the Privacy Rule:

- Covered Entities Under the Privacy Rule
- Protected Health Information (PHI)
- Uses and Disclosures of PHI
- Notice of Privacy Practices Requirements
- Additional Information

Covered Entities Under the Privacy Rule

Among other entities, the HIPAA Privacy Rule specifically applies to health care providers and their "business associates."

Health Care Providers

Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity.

- **"Health care providers":** Health care providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists, and other practitioners) as defined by Medicare, and **any other person or organization that furnishes, bills, or is paid for health care**.
- **"Certain transactions":** These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which the U.S. Department of Health and Human Services (HHS) has established standards.

Note: The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf.

Business Associates

In general, a **business associate** is a person or organization, **other than a member of a covered entity's workforce**, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information (see definition below).

Business associate functions or activities on behalf of a covered entity include:

- Claims processing;
- Data analysis;
- Utilization review; and
- Billing.

Business associate services to a covered entity are limited to:

- Legal;
- Actuarial;
- Accounting;
- Consulting;
- Data aggregation;
- Management;
- Administrative;
- Accreditation; or
- Financial services.

However, persons or organizations are **not** considered business associates if their functions or services **do not involve the use or disclosure of PHI**, and where any access to PHI by such persons would be **incidental**, if at all.

Note: When a covered entity uses a contractor or other non-workforce member to perform business associate services or activities, the Privacy Rule requires that the covered entity include certain protections for individually identifiable health information in a business associate agreement. Click here for sample business associate agreement language from HHS.

Click here to learn more about covered entities under the Privacy Rule.

Protected Health Information (PHI)

The Privacy Rule protects all **individually identifiable health information** held or transmitted by a health care provider or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "**protected health information**," or PHI.

The Privacy Rule defines "individually identifiable health information" as information, including demographic data, that:

- Identifies the individual, or for which there is a reasonable basis to believe it can be used to identify the individual; **and**
- Relates to:
  - The individual's past, present, or future physical or mental health or condition;
  - The provision of health care to the individual; **or**
  - The past, present, or future payment for the provision of health care to the individual.

Individually identifiable health information includes many common identifiers, such as **names, addresses, birth dates, and Social Security Numbers**.

Note: Among other things, the Privacy Rule excludes from protected health information employment records that a health care provider maintains in its capacity as an employer.

Click here to learn more about PHI.

Uses and Disclosures of PHI

A covered entity may not use or disclose protected health information (PHI) unless:

- The Privacy Rule requires the use or disclosure;
- The Privacy Rule permits the use or disclosure; or
- The individual who is the subject of the information (or the individual's personal representative) authorizes the use or disclosure in writing.

In addition, a covered entity must make reasonable efforts and implement policies and procedures to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. This is called the "minimum necessary standard."

Required Disclosures

A covered entity **must** disclose protected health information in **only two situations:**

1. To individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and
2. To HHS when it is undertaking a compliance investigation or review, or an enforcement action.

Permitted Uses and Disclosures

A covered entity is generally permitted to use and disclose protected health information **without an individual's authorization** for the following purposes or situations:

- To the individual who is the subject of the information;
- For treatment, payment, and health care operations (see expanded definition below);
- For uses and disclosures when the person who is the subject of the information has had an opportunity to agree or object (see expanded definition below);
- Incident to an otherwise permitted use and disclosure; and
- For public interest and benefit activities (**including disclosures for workers' compensation purposes**).

Treatment, Payment, and Health Care Operations

A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities. These activities include, among other things:

- The provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation and referral between providers;
- Activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual;
- Case management and care coordination;
- Provider performance evaluation, credentialing, and accreditation; and
- Business planning, development, management, and administration.

Uses and Disclosures with the Opportunity to Agree or Object

Informal permission may be obtained by asking the individual outright, or by **circumstances that clearly give the individual the opportunity to agree, acquiesce, or object**. Where the individual

is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.

For example, informal permission may be relied upon for the following common purposes:

- To list the individual's name, general condition, religious affiliation, and location in the provider's facility directory;
- To disclose to the individual's family, relatives, or friends, or to other persons whom the individual identifies, protected health information directly relevant to that person's involvement in the individual's care or payment for care; and
- Notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care of the individual's location, general condition, or death.

Additional rules apply to permitted uses and disclosures. For more information, click here.

Authorized Uses and Disclosures

A covered entity must obtain the individual's **written authorization** for any use or disclosure of protected health information that is not required or permitted by the Privacy Rule.

A written authorization **must** contain these "core elements":

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
3. 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.
4. 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.
5. 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.

6. 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.

In addition to the core elements, the Privacy Rule **also requires** that the written authorization contain statements adequate to place the individual on notice of all of the following:

1. The individual's right to revoke the authorization in writing, **and either**:
   - The exceptions to the right to revoke and a description of how the individual may revoke the authorization; **or**
   - A reference to the covered entity's notice.
2. The ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization, by stating **either**:
   - The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization; **or**
   - The consequences to the individual of a refusal to sign the authorization when the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.
3. The potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer be protected.

Note: A covered entity generally **may not** condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization.

Click here for more information on authorized uses and disclosures.

Minimum Necessary Standard

A covered entity must make reasonable efforts and implement policies and procedures to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. This is called the "**minimum necessary standard**."

When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose.

The minimum necessary standard is **not imposed** in any of the following circumstances:

- Disclosure to or a request by a health care provider for treatment;
- Disclosure to an individual who is the subject of the information, or the individual's personal representative;
- Use or disclosure made pursuant to an authorization;
- Disclosure to HHS for complaint investigation, compliance review, or enforcement; or
- Disclosures required by regulation or law.

For additional guidance on the minimum necessary standard, click here.

Notice of Privacy Practices Requirements

Covered entities generally must provide patients a **Notice of Privacy Practices**. The Privacy Rule requires that the notice contain certain elements and be distributed at certain times.

Content Requirements

Covered entities are required to provide a notice in plain language that describes:

- How the covered entity may use and disclose protected health information about an individual;
- The individual's rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the covered entity;
- The covered entity's legal duties with respect to the information, including a statement that the covered entity is required by law to maintain the privacy of protected health information;
- Whom individuals can contact for further information about the covered entity's privacy policies; and
- The notice's effective date.

Model versions of the Notice of Privacy Practices are available here.

Distribution Requirements

A health care provider must generally distribute its notice **no later than the date of first service delivery** and make a good faith effort to **obtain the individual's written acknowledgment of receipt** of the notice. If an acknowledgment cannot be obtained, the provider must document his or her efforts to obtain the acknowledgment and the reason it was not obtained.

In **emergency treatment situations**, the health care provider must provide the notice as soon as reasonably practicable after the emergency situation has ended. In these situations, health care

providers are not required to make a good faith effort to obtain a written acknowledgment from individuals.

In addition, all health care providers must make the notice available to any person who asks for it and prominently post and make available its notice on any web site it maintains that provides information about its customer services or benefits.

Click here for more on the Notice of Privacy Practices requirements.

SECURITY RULE

The **HIPAA Security Rule** establishes national standards for protecting certain health information held or transferred in **electronic form**. Among other requirements, the Security Rule most notably requires covered entities to put in place specified **administrative, technical, and physical safeguards** to secure individuals' electronic protected health information, or e-PHI. This subsection of the Guide will address the following topics relevant to the Security Rule:

- Covered Entities Under the Security Rule
- Covered Information Under the Security Rule
- Security Rule Requirements

Covered Entities Under the Security Rule

Among other entities, the HIPAA Security Rule specifically applies to **health care providers**, regardless of size, who electronically transmit health information in connection with **certain transactions**.

- "**Health care providers**" include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists, and other practitioners) as defined by Medicare, and **any other person or organization that furnishes, bills, or is paid for health care**.
- "**Certain transactions**" include **claims, benefit eligibility inquiries, referral authorization requests, or other transactions** for which the U.S. Department of Health and Human Services (HHS) has established standards.

Note: The Security Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf.

Click here for more information on covered entities under the Security Rule.

Covered Information Under the Security Rule

The Security Rule protects **"electronic protected health information,"** or e-PHI, which is all individually identifiable health information a health care provider creates, receives, maintains, or transmits in electronic form. **The Security Rule does not apply to PHI transmitted orally or in writing.**

HIPAA defines "individually identifiable health information" as information, including demographic data, that:

- Identifies the individual, or for which there is a reasonable basis to believe it can be used to identify the individual; **and**
- Relates to:
  - The individual's past, present, or future physical or mental health or condition;
  - The provision of health care to the individual; **or**
  - The past, present, or future payment for the provision of health care to the individual.

Individually identifiable health information includes many common identifiers such as **names, addresses, birth dates, and Social Security Numbers**.

Click here to learn more about covered information under the Security Rule.

Security Rule Requirements

The Security Rule **requires** health care providers to maintain reasonable and appropriate **administrative, technical, and physical safeguards** for protecting electronic protected health information (e-PHI). Specifically, health care providers **must**:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain, or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

The Security Rule does not dictate which security measures a health care provider must use. Instead, the rule requires the health care provider to **consider**:

- Its size, complexity, and capabilities;
- Its technical, hardware, and software infrastructure;
- The costs of security measures; and
- The likelihood and possible impact of potential risks to e-PHI.

In addition, health care providers are also **required** to **document**, **review**, and, as needed, **modify** their security measures.

Administrative Safeguards

The Security Rule requires covered entities to put in place the following administrative safeguards:

- **Security Management Process**: Health care providers must identify and analyze potential risks to e-PHI, and must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level. As part of the security management process, a health care provider must regularly perform an ongoing risk analysis that involves:
  - Evaluating the likelihood and impact of potential risks to e-PHI;
  - Implementing appropriate security measures to address the risks identified in the risk analysis;
  - Documenting the chosen security measures and, where required, the rationale for adopting those measures; and
  - Maintaining continuous, reasonable, and appropriate security protections.
- **Security Personnel:** A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.
- **Information Access Management:** A covered entity must implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access).
- **Workforce Training and Management:** A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.
- **Evaluation**: A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

Technical Safeguards

The Security Rule requires covered entities to put in place the following technical safeguards:

- **Access Control**: A covered entity must implement technical policies and procedures that allow only authorized persons to access e-PHI.
- **Audit Controls**: A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

- **Integrity Controls**: A covered entity must implement policies and procedures, including electronic measures, to ensure that e-PHI is not improperly altered or destroyed.
- **Transmission Security**: A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

Physical Safeguards

The Security Rule requires covered entities to put in place the following physical safeguards:

- **Facility Access and Control:** A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.
- **Workstation and Device Security**: A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of e-PHI.

Documentation Requirements

The Security Rule requires covered entities to put in place policies and procedures to assure compliance, as follows:

- A covered entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities or assessments.
- A covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of e-PHI.

Click here for more information on the Security Rule's requirements.

BREACH NOTIFICATION RULE

The HIPAA Breach Notification Rule requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information (PHI). This subsection of the Guide addresses the following topics concerning the Breach Notification Rule:

- What is a "Breach"?
- Breach Notification Requirements
- Administrative Requirements

What is a "Breach"?

HIPAA defines a **"breach"** as, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI.

An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised, based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

There are **three exceptions** to the HIPAA definition of breach:

1. The **unintentional** acquisition, access, or use of PHI made in good faith and within the scope of authority.
2. The **inadvertent** disclosure of PHI by a person authorized to access PHI to another person authorized to access PHI at the same covered entity or business associate.
3. If the covered entity or business associate has a **good faith belief** that the unauthorized person to whom the disclosure was made would not have been able to retain the information.

Breach Notification Requirements

Following a breach of unsecured PHI, covered entities must provide notification of the breach to **affected individuals**, **HHS**, and, in certain circumstances, to **the media**.

Notice to Affected Individuals

Covered entities must notify affected individuals of the breach by first-class mail or by email, if the affected individual has agreed to receive such notices electronically. These individual notifications must be provided without unreasonable delay and in no case later than **60 days** following the discovery of a breach and must include, to the extent possible:

- A brief description of the breach;
- A description of the types of information that were involved in the breach;
- The steps affected individuals should take to protect themselves from potential harm;
- A brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches; and
- Contact information for the covered entity (or business associate, as applicable).

If the covered entity has insufficient or out-of-date contact information for **10 or more individuals**, the covered entity must post the notice on the home page of its website for at least 90 days **or** provide the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least 90 days, where individuals can learn if their information was involved in the breach.

If the covered entity has insufficient or out-of-date contact information for **fewer than 10 individuals**, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

Notice to HHS

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the U.S. Department of Health and Human Services (HHS) of breaches of unsecured PHI by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects **500 or more individuals**, covered entities must notify HHS without unreasonable delay—and in no case later than **60 days**—following the breach. Covered entities may notify HHS annually of breaches involving **fewer than 500 individuals**, no later than **60 days after the end of the calendar year** in which the breaches are discovered.

Notice to the Media

Covered entities that experience a breach affecting **more than 500 residents** of a state or jurisdiction are required to provide notice to prominent media outlets serving the state or jurisdiction. Covered entities will likely provide this notification in the form of a press release to

appropriate media outlets serving the affected area. This media notification must be provided without unreasonable delay and in no case later than **60 days** following the discovery of a breach, and must include the same information required for the notice to affected individuals (see above).

Note: If a breach of unsecured PHI occurs at or by a **business associate**, the business associate must provide notice to the covered entity without unreasonable delay and **no later than 60 days** from the discovery of the breach.

Administrative Requirements

Covered entities and business associates should **maintain documentation** that all required notifications of the use or disclosure of unsecured PHI were made, or alternatively, documentation to demonstrate that notification was not required.

Covered entities are also required to comply with certain administrative requirements with respect to breach notification. For example, covered entities **must** have in place written policies and procedures regarding breach notification, train employees on these policies and procedures, and develop and apply appropriate sanctions against workforce members who do not comply with them.

Click here for more information on the Breach Notification Rule.

BUSINESS ASSOCIATES

By law, the HIPAA Privacy Rule applies only to covered entities – health plans, health care clearinghouses, and certain health care providers. However, most health care providers and health plans do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. The Privacy Rule allows covered providers and health plans to disclose protected health information to these "business associates" if the providers or plans obtain satisfactory assurances that the business associate will:

- Use the information only for the purposes for which it was engaged by the covered entity;
- Safeguard the information from misuse; and
- Help the covered entity comply with some of the covered entity's duties under the Privacy Rule.

Covered entities may disclose protected health information to an entity in its role as a business associate only to help the covered entity carry out its health care functions – not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate.

How the Rule Works

General Rule

The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

What Is a "Business Associate"?

A "business associate" is generally a person or entity that performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of protected health information. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

The following persons and entities are also considered "business associates" under the final omnibus rule:

- Subcontractors that create, receive, maintain, or transmit protected health information on behalf of another business associate;
- Health Information Exchange Organizations, E-prescribing Gateways, or other persons that provide data transmission services with respect to protected health information to a covered entity and that require access on a routine basis to such protected health information;
- Persons who offer a personal health record to one or more individuals on behalf of a covered entity.

The Privacy Rule lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

Business associate functions and activities include: claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; billing; benefit management; practice management; repricing; and patient safety activities. Business associate services are: legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial.

Examples of Business Associates

- A third-party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- A consultant that performs utilization reviews for a hospital.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan's pharmacist network.
- A shredding company hired by a third-party administrator to handle document and media shredding to securely dispose of paper and electronic protected health information.

Business Associate Contracts

A covered entity's contract or other written arrangement with its business associate must contain certain elements specified by law. For the convenience of health plans and other covered entities, the U.S. Department of Health and Human Services has created a Sample Business Associate Agreement. Among other requirements, the contract must:

- Describe the permitted and required uses of protected health information by the business associate;
- Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and
- Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

Obligation to Cure Breaches of a Business Associate

Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR). A federal rule makes business associates of covered entities **directly liable** for violations of the Privacy Rule for impermissible uses and disclosures pursuant to their business associate contracts.

HIPAA PENALTIES

Individual violations of the HIPAA rules (including the Privacy, Security, and Breach Notification Rules) can lead to civil penalties of **approximately $55,000 each**, while the most severe violations are subject to seven-figure fines, and criminal prosecution.

The following civil penalty amounts apply to civil penalties assessed for violations of the HIPAA rules that occurred after **November 2, 2015**:

- For a covered entity that **did not know** of the violation, and by exercising reasonable diligence would not have known of the violation, the minimum penalty is **$112** per violation;
- For violations **due to reasonable cause and not willful neglect**, the minimum penalty is **$1,118** per violation;
- For violations due to **willful neglect and corrected during the 30-day period** beginning on the first date the covered entity or business associate knew, or, by exercising reasonable diligence, would have known that the violation occurred, the minimum penalty is **$11,182** per violation; and
- For violations due to **willful neglect and not corrected during the 30-day period** beginning on the first date the covered entity or business associate knew, or by exercising reasonable diligence, would have known that the violation occurred, the minimum penalty is **$55,910** per violation.

Click here for more information.

Provided by:

HR360, Inc.
50 Washington Street, Suite 411
Norwalk, CT 06854

Phone: (203) 977-8100
www.hr360.com