DO YOU KNOW WHEN A HIPAA BUSINESS ASSOCIATE AGREEMENT IS REQUIRED?

Randi Kopf, RN, MS, JD
Kopf HealthLaw, LLC
Rockville, Maryland
www.kopfhealthlaw.com
301-251-2788

Rose M. Matricciani, RN, JD
Whiteford, Taylor & Preston LLP
Baltimore, Maryland
rmatricciani@wtplaw.com
410-347-9476

Skip Navigation

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

Business Associate Contracts

SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS
(Published January 25, 2013)

Introduction

A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

A written contract between a covered entity and a business associate must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information; (4) require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information; (5) require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings; (6) to the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation; (7) require the business associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule; (8) at termination of the contract, if feasible, require the business associate to return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity; (9) require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and (10) authorize termination of the contract by the covered entity if the business associate violates a material term of the contract. Contracts between business associates and business associates that are subcontractors are subject to these same requirements.

This document includes sample business associate agreement provisions to help covered entities and business associates more easily comply with the business associate contract requirements. While these sample provisions are written for the purposes of the contract between a covered entity and its business associate, the language may be adapted for purposes of the contract between a business associate and subcontractor.

This is only sample language and use of these sample provisions is not required for compliance with the HIPAA Rules. The language may be changed to more accurately reflect business arrangements between a covered entity and business associate or business associate and subcontractor. In addition, these or similar provisions may be incorporated into an agreement for the provision of services between a covered entity and business associate or business associate and subcontractor, or they may be incorporated into a separate business associate agreement. These provisions address only concepts and requirements set forth in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, and alone may not be sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that may be required or typically included in a valid contract. Reliance on this sample may not be sufficient for compliance with State law, and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Sample Business Associate Agreement Provisions

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.

Definitions

Catch-all definition:

Guidance Materials for Covered Entities

- Summary of the Privacy Rule
- Guidance on Significant Aspects of the Privacy Rule
- Fast Facts for Covered Entities
- Provider Guide: Communicating With a Patient's Family, Friends, or Other Persons Identified by the Patient
- Guidance on the Application of FERPA and HIPAA to Student Health Records
- Sample Business Associate Contract
- Misleading Marketing Claims
- Sign Up for the OCR Privacy Listserv

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the [Choose either "covered entity" or "individual or the individual's designee"] as necessary to satisfy covered entity's obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual's request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual's request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either "covered entity" or "individual"] as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

(h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as "as necessary to perform the services set forth in Service Agreement."]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

(b) Business associate may use or disclose protected health information as required by law.

(c) Business associate agrees to make uses and disclosures and requests for protected health information

[Option 1] consistent with covered entity's minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add ", except for the specific uses and disclosures set forth below."]

(e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.

(b) [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.

(c) [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

Permissible Requests by Covered Entity

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within the time specified by covered entity]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) Obligations of Business Associate Upon Termination.

[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;
4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and
5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

Back to Top

United States Department of Health & Human Services

OCR PRIVACY BRIEF

SUMMARY OF THE HIPAA PRIVACY RULE

OCR
OFFICE FOR CIVIL RIGHTS

HIPAA Compliance Assistance

SUMMARY OF
THE HIPAA PRIVACY RULE

Contents

SUMMARY OF
THE HIPAA PRIVACY RULE

Introduction

The *Standards for Privacy of Individually Identifiable Health Information* ("Privacy Rule") establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[1] The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

This is a summary of key elements of the Privacy Rule and not a complete or comprehensive guide to compliance. Entities regulated by the Rule are obligated to comply with all of its applicable requirements and should not rely on this summary as a source of legal information or advice. To make it easier for entities to review the complete requirements of the Rule, provisions of the Rule referenced in this summary are cited in notes at the end of this document. To view the entire Rule, and for other additional helpful information about how it applies, see the OCR website: http://www.hhs.gov/ocr/hipaa. In the event of a conflict between this summary and the Rule, the Rule governs.

Links to the OCR Guidance Document are provided throughout this paper. Provisions of the Rule referenced in this summary are cited in endnotes at the end of this document. To review the entire Rule itself, and for other additional helpful information about how it applies, see the OCR website: http://www.hhs.gov/ocr/hipaa.

Statutory & Regulatory Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information. Collectively these are known as the *Administrative Simplification* provisions.

HIPAA required the Secretary to issue privacy regulations governing individually identifiable health information, if Congress did not enact privacy legislation within

	three years of the passage of HIPAA. Because Congress did not enact privacy legislation, HHS developed a proposed rule and released it for public comment on November 3, 1999. The Department received over 52,000 public comments. The final regulation, the Privacy Rule, was published December 28, 2000.[2] In March 2002, the Department proposed and released for public comment modifications to the Privacy Rule. The Department received over 11,000 comments. The final modifications were published in final form on August 14, 2002.[3] A text combining the final regulation and the modifications can be found at 45 CFR Part 160 and Part 164, Subparts A and E on the OCR website: http://www.hhs.gov/ocr/hipaa.
Who is Covered by the Privacy Rule	The Privacy Rule, as well as all the Administrative Simplification rules, apply to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities"). For help in determining whether you are covered, use the decision tool at: http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp. **Health Plans.** Individual and group plans that provide or pay the cost of medical care are covered entities.[4] Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations ("HMOs"), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. There are exceptions—a group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity. Two types of government-funded programs are not health plans: (1) those whose principal purpose is not providing or paying the cost of health care, such as the food stamps program; and (2) those programs whose principal activity is directly providing health care, such as a community health center,[5] or the making of grants to fund the direct provision of health care. Certain types of insurance entities are also not health plans, including entities providing only workers' compensation, automobile insurance, and property and casualty insurance. **Health Care Providers.** Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule.[6] Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must be in connection with a standard transaction. 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. 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.

	Health Care Clearinghouses. *Health care clearinghouses* are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa.[7] In most instances, health care clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or health care provider as a business associate. In such instances, only certain provisions of the Privacy Rule are applicable to the health care clearinghouse's uses and disclosures of protected health information.[8] Health care clearinghouses include billing services, repricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions.
Business Associates	**Business Associate Defined.** 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. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing.[9] 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 protected health information, and where any access to protected health information by such persons would be incidental, if at all. A covered entity can be the business associate of another covered entity. **Business Associate Contract.** When a covered entity uses a contractor or other non-workforce member to perform *"business associate"* services or activities, the Rule requires that the covered entity include certain protections for the information in a business associate agreement (in certain circumstances governmental entities may use alternative means to achieve the same protections). In the business associate contract, a covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates.[10] Moreover, a covered entity may not contractually authorize its business associate to make any use or disclosure of protected health information that would violate the Rule. Covered entities that have an existing written contract or agreement with business associates prior to October 15, 2002, which is not renewed or modified prior to April 14, 2003, are permitted to continue to operate under that contract until they renew the contract or April 14, 2004, whichever is first.[11] Sample business associate contract language is available on the OCR website at: http://www.hhs.gov/ocr/hipaa/contractprov.html. Also see OCR "Business Associate" Guidance.
What Information is Protected	**Protected Health Information.** The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information *"protected health information (PHI)."*[12]

	"Individually identifiable health information" is information, including demographic data, that 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, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.[13] Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g. **De-Identified Health Information.** There are no restrictions on the use or disclosure of de-identified health information.[14] De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: 1) a formal determination by a qualified statistician; or 2) the removal of 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.[15]
General Principle for Uses and Disclosures	**Basic Principle.** A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.[16] **Required Disclosures.** A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.[17] See OCR "Government Access" Guidance.
Permitted Uses and Disclosures	**Permitted Uses and Disclosures.** A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and

(6) Limited Data Set for the purposes of research, public health or health care operations.[18] Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

(1) To the Individual. A covered entity may disclose protected health information to the individual who is the subject of the information.

(2) Treatment, Payment, Health Care Operations. A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities.[19] A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship. See OCR "Treatment, Payment, Health Care Operations" Guidance.

> ***Treatment*** is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.[20]
>
> ***Payment*** encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual[21] and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.
>
> ***Health care operations*** are any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.[22]

Most uses and disclosures of psychotherapy notes for treatment, payment, and health care operations purposes require an authorization as described below.[23]

Obtaining "consent" (written permission from individuals to use and disclose their protected health information for treatment, payment, and health care operations) is optional under the Privacy Rule for all covered entities.[24] The content of a consent form, and the process for obtaining consent, are at the discretion of the covered entity electing to seek consent.

(3) Uses and Disclosures with 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.

Facility Directories. It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information. A covered health care provider may rely on an individual's informal permission to list in its facility directory the individual's name, general condition, religious affiliation, and location in the provider's facility.[25] The provider may then disclose the individual's condition and location in the facility to anyone asking for the individual by name, and also may disclose religious affiliation to clergy. Members of the clergy are not required to ask for the individual by name when inquiring about patient religious affiliation.

For Notification and Other Purposes. A covered entity also may rely on an individual's informal permission 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. [26] This provision, for example, allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, a covered entity may rely on an individual's informal permission to use or disclose protected health information for the purpose of 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. In addition, protected health information may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts.

(4) Incidental Use and Disclosure. The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the "minimum necessary," as required by the Privacy Rule.[27] See OCR "Incidental Uses and Disclosures" Guidance.

(5) Public Interest and Benefit Activities. The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes.[28] These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information.

Required by Law. Covered entities may use and disclose protected health information without individual authorization as *required by law* (including by

statute, regulation, or court orders).[29]

Public Health Activities. Covered entities may disclose protected health information to: (1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect; (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance; (3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers, 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 the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law.[30] See OCR "Public Health" Guidance; CDC Public Health and HIPAA Guidance.

Victims of Abuse, Neglect or Domestic Violence. In certain circumstances, covered entities may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.[31]

Health Oversight Activities. Covered entities may disclose protected health information to health oversight agencies (as defined in the Rule) for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.[32]

Judicial and Administrative Proceedings. Covered entities may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.[33]

Law Enforcement Purposes. Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.[34]

Decedents. Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.[35]

Cadaveric Organ, Eye, or Tissue Donation. Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.[36]

Research. "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge.[37] The Privacy Rule permits a covered entity to use and disclose protected health information for research purposes, without an individual's authorization, provided the covered entity obtains either: (1) documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board; (2) representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or (3) representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought.[38] A covered entity also may use or disclose, without an individuals' authorization, a limited data set of protected health information for research purposes (see discussion below).[39] See OCR "Research" Guidance; NIH Protecting PHI in Research.

Serious Threat to Health or Safety. Covered entities may disclose protected health information that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.[40]

Essential Government Functions. An authorization is not required to use or disclose protected health information for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.[41]

	Workers' Compensation. Covered entities may disclose protected health information as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.[42] See OCR "Workers' Compensation" Guidance. **(6) Limited Data Set.** A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.[43] A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.
Authorized Uses and Disclosures	**Authorization.** A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule.[44] A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.[45] An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. Examples of disclosures that would require an individual's authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes. All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data. The Privacy Rule contains transition provisions applicable to authorizations and other express legal permissions obtained prior to April 14, 2003.[46] **Psychotherapy Notes[47].** A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions[48]: • The covered entity who originated the notes may use them for treatment. • A covered entity may use or disclose, without an individual's authorization, the psychotherapy notes, for its own training, and to defend itself in legal proceedings brought by the individual, for HHS to investigate or determine the covered entity's compliance with the Privacy Rules, 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, for the lawful activities of a coroner or medical examiner or as required by law. **Marketing.** Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service.[49] The Privacy Rule carves out the following health-related activities from this definition of marketing: • Communications to describe health-related products or services, or payment

	for them, provided by or included in a benefit plan of the covered entity making the communication; • Communications about participating providers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefits plan; • Communications for treatment of the individual; and • Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual. Marketing also is an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information, in exchange for direct or indirect remuneration, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services. A covered entity must obtain an authorization to use or disclose protected health information for marketing, except 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, however, to make a communication that falls within one of the exceptions to the marketing definition. An authorization for marketing that involves the covered entity's receipt of direct or indirect remuneration from a third party must reveal that fact. See OCR "Marketing" Guidance.
Limiting Uses and Disclosures to the Minimum Necessary	**Minimum Necessary.** A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts 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.[50] A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. 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. See OCR "Minimum Necessary" Guidance. The minimum necessary requirement is not imposed in any of the following circumstances: (a) disclosure to or a request by a health care provider for treatment; (b) disclosure to an individual who is the subject of the information, or the individual's personal representative; (c) use or disclosure made pursuant to an authorization; (d) disclosure to HHS for complaint investigation, compliance review or enforcement; (e) use or disclosure that is required by law; or (f) use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules. **Access and Uses.** For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of

	protected health information to which access is needed, and any conditions under which they need the information to do their jobs. **Disclosures and Requests for Disclosures.** Covered entities must establish and implement policies and procedures (which may be standard protocols) for *routine, recurring disclosures, or requests for disclosures,* that limits the protected health information disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For non-routine, non-recurring disclosures, or requests for disclosures that it makes, covered entities must develop criteria designed to limit disclosures to the information reasonably necessary to accomplish the purpose of the disclosure and review each of these requests individually in accordance with the established criteria. **Reasonable Reliance.** If another covered entity makes a request for protected health information, a covered entity may rely, if reasonable under the circumstances, on the request as complying with this minimum necessary standard. Similarly, a covered entity may rely upon requests as being the minimum necessary protected health information from: (a) a public official, (b) a professional (such as an attorney or accountant) who is the covered entity's business associate, seeking the information to provide services to or for the covered entity; or (c) a researcher who provides the documentation or representation required by the Privacy Rule for research.
Notice and Other Individual Rights	**Privacy Practices Notice.** Each covered entity, with certain exceptions, must provide a notice of its privacy practices.[51] The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices. The Rule also contains specific distribution requirements for direct treatment providers, all other health care providers, and health plans. See OCR "Notice" Guidance. • **Notice Distribution.** A covered health care provider with a *direct treatment relationship* with individuals must deliver a privacy practices notice to patients starting April 14, 2003 as follows: o Not later than the first service encounter by personal delivery (for patient visits), by automatic and contemporaneous electronic response (for electronic service delivery), and by prompt mailing (for telephonic service delivery); o By posting the notice at each service delivery site in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice; and o In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates.

Covered entities, whether *direct treatment providers* or *indirect treatment providers* (such as laboratories) or *health plans* must supply notice to anyone on request.[52] A covered entity must also make its notice electronically available on any web site it maintains for customer service or benefits information.

The covered entities in an *organized health care arrangement* may use a joint privacy practices notice, as long as each agrees to abide by the notice content with respect to the protected health information created or received in connection with participation in the arrangement.[53] Distribution of a joint notice by any covered entity participating in the organized health care arrangement at the first point that an OHCA member has an obligation to provide notice satisfies the distribution obligation of the other participants in the organized health care arrangement.

A health plan must distribute its privacy practices notice to each of its enrollees by its Privacy Rule compliance date. Thereafter, the health plan must give its notice to each new enrollee at enrollment, and send a reminder to every enrollee at least once every three years that the notice is available upon request. A health plan satisfies its distribution obligation by furnishing the notice to the "named insured," that is, the subscriber for coverage that also applies to spouses and dependents.

- **Acknowledgement of Notice Receipt.** A covered health care provider with a direct treatment relationship with individuals must make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice.[54] The Privacy Rule does not prescribe any particular content for the acknowledgement. The provider must document the reason for any failure to obtain the patient's written acknowledgement. The provider is relieved of the need to request acknowledgement in an emergency treatment situation.

Access. Except in certain circumstances, individuals have the right to review and obtain a copy of their protected health information in a covered entity's *designated record set*.[55] The "designated record set" is that group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.[56] The Rule excepts from the right of access the following protected health information: psychotherapy notes, information compiled for legal proceedings, laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information held by certain research laboratories. For information included within the right of access, covered entities may deny an individual access in certain specified situations, such as when a health care professional believes access could cause harm to the individual or another. In such situations, the individual must be given the right to have such denials reviewed by a licensed health care professional for a second opinion.[57] Covered entities may impose reasonable, cost-based fees for the cost of copying and postage.

Amendment. The Rule gives individuals the right to have covered entities amend their protected health information in a designated record set when that information is

	inaccurate or incomplete.[58] If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment.[59] If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. The Rule specifies processes for requesting and responding to a request for amendment. A covered entity must amend protected health information in its designated record set upon receipt of notice to amend from another covered entity. **Disclosure Accounting.** Individuals have a right to an accounting of the disclosures of their protected health information by a covered entity or the covered entity's business associates.[60] The maximum disclosure accounting period is the six years immediately preceding the accounting request, except a covered entity is not obligated to account for any disclosure made before its Privacy Rule compliance date. The Privacy Rule does not require accounting for disclosures: (a) for treatment, payment, or health care operations; (b) to the individual or the individual's personal representative; (c) for notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories; (d) pursuant to an authorization; (e) of a limited data set; (f) for national security or intelligence purposes; (g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or (h) incident to otherwise permitted or required uses or disclosures. Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities. **Restriction Request.** Individuals have the right to request that a covered entity restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death.[61] A covered entity is under no obligation to agree to requests for restrictions. A covered entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.[62] **Confidential Communications Requirements.** Health plans and covered health care providers must permit individuals to request an alternative means or location for receiving communications of protected health information by means other than those that the covered entity typically employs.[63] For example, an individual may request that the provider communicate with the individual through a designated address or phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card. Health plans must accommodate reasonable requests if the individual indicates that the disclosure of all or part of the protected health information could endanger the individual. The health plan may not question the individual's statement of endangerment. Any covered entity may condition compliance with a confidential communication request on the individual specifying an alternative address or method of contact and explaining how any payment will be handled.

Administrative Requirements	HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources. **Privacy Policies and Procedures.** A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.[64] **Privacy Personnel.** A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.[65] **Workforce Training and Management.** Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity).[66] A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions.[67] A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.[68] **Mitigation.** A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.[69] **Data Safeguards.** A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure.[70] For example, such safeguards might include shredding documents containing protected health information before discarding them, securing medical records with lock and key or pass code, and limiting access to keys or pass codes. See OCR "Incidental Uses and Disclosures" Guidance. **Complaints.** A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule.[71] The covered entity must explain those procedures in its privacy practices notice.[72] Among other things, the covered entity must identify to whom individuals can submit complaints to at the covered entity and advise that complaints also can be submitted to the Secretary of HHS. **Retaliation and Waiver.** A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule.[73] A covered entity may not

	require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.[74] **Documentation and Record Retention.** A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.[75] **Fully-Insured Group Health Plan Exception.** The only administrative obligations with which a fully-insured group health plan that has no more than enrollment data and summary health information is required to comply are the (1) ban on retaliatory acts and waiver of individual rights, and (2) documentation requirements with respect to plan documents if such documents are amended to provide for the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO that services the group health plan.[76]
Organizational Options	The Rule contains provisions that address a variety of organizational issues that may affect the operation of the privacy protections. **Hybrid Entity.** The Privacy Rule permits a covered entity that is a single legal entity and that conducts both covered and non-covered functions to elect to be a "hybrid entity."[77] (The activities that make a person or organization a covered entity are its "covered functions."[78]) To be a hybrid entity, the covered entity must designate in writing its operations that perform covered functions as one or more "health care components." After making this designation, most of the requirements of the Privacy Rule will apply only to the health care components. A covered entity that does not make this designation is subject in its entirety to the Privacy Rule. **Affiliated Covered Entity.** Legally separate covered entities that are affiliated by common ownership or control may designate themselves (including their health care components) as a single covered entity for Privacy Rule compliance.[79] The designation must be in writing. An affiliated covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions. **Organized Health Care Arrangement.** The Privacy Rule identifies relationships in which participating covered entities share protected health information to manage and benefit their common enterprise as "organized health care arrangements."[80] Covered entities in an organized health care arrangement can share protected health information with each other for the arrangement's joint health care operations.[81] **Covered Entities With Multiple Covered Functions.** A covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions.[82] The covered entity may not use or disclose the protected health information of an individual who receives services from one covered function (e.g., health care provider) for another covered function (e.g., health plan) if the individual is not involved with the other function.

	Group Health Plan disclosures to Plan Sponsors. A group health plan and the health insurer or HMO offered by the plan may disclose the following protected health information to the "plan sponsor"—the employer, union, or other employee organization that sponsors and maintains the group health plan[83]: • Enrollment or disenrollment information with respect to the group health plan or a health insurer or HMO offered by the plan. • If requested by the plan sponsor, summary health information for the plan sponsor to use to obtain premium bids for providing health insurance coverage through the group health plan, or to modify, amend, or terminate the group health plan. "Summary health information" is information that summarizes claims history, claims expenses, or types of claims experience of the individuals for whom the plan sponsor has provided health benefits through the group health plan, and that is stripped of all individual identifiers other than five digit zip code (though it need not qualify as de-identified protected health information). • Protected health information of the group health plan's enrollees for the plan sponsor to perform plan administration functions. The plan must receive certification from the plan sponsor that the group health plan document has been amended to impose restrictions on the plan sponsor's use and disclosure of the protected health information. These restrictions must include the representation that the plan sponsor will not use or disclose the protected health information for any employment-related action or decision or in connection with any other benefit plan.
Other Provisions: Personal Representatives and Minors	**Personal Representatives.** The Privacy Rule requires a covered entity to treat a *"personal representative"* the same as the individual, with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Rule.[84] A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate. The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual. **Special case: Minors.** In most cases, parents are the personal representatives for their minor children. Therefore, in most cases, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children. In certain exceptional cases, the parent is not considered the personal representative. In these situations, the Privacy Rule defers to State and other law to determine the rights of parents to access and control the protected health information of their minor children. If State and other law is silent concerning parental access to the minor's protected health information, a covered entity has discretion to provide or deny a parent access to the minor's health information, provided the decision is made by a licensed health care professional in the exercise of professional judgment. See OCR "Personal Representatives" Guidance.

State Law	**Preemption.** In general, State laws that are contrary to the Privacy Rule are preempted by the federal requirements, which means that the federal requirements will apply.[85] "Contrary" means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.[86] The Privacy Rule provides exceptions to the general rule of federal preemption for contrary State laws that (1) relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such information, (2) provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or (3) require certain health plan reporting, such as for management or financial audits. **Exception Determination.** In addition, preemption of a contrary State law will not occur if HHS determines, in response to a request from a State or other entity or person, that the State law: • Is necessary to prevent fraud and abuse related to the provision of or payment for health care, • Is necessary to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation, • Is necessary for State reporting on health care delivery or costs, • Is necessary for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or • Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.
Enforcement and Penalties for Noncompliance	**Compliance.** Consistent with the principles for achieving compliance provided in the Rule, HHS will seek the cooperation of covered entities and may provide technical assistance to help them comply voluntarily with the Rule.[87] The Rule provides processes for persons to file complaints with HHS, describes the responsibilities of covered entities to provide records and compliance reports and to cooperate with, and permit access to information for, investigations and compliance reviews. **Civil Money Penalties.** HHS may impose civil money penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement.[88] That penalty may not exceed $25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year. HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.

	Criminal Penalties. A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of $50,000 and up to one-year imprisonment.[89] The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal sanctions will be enforced by the Department of Justice.
Compliance Dates	**Compliance Schedule.** All covered entities, except "small health plans," must be compliant with the Privacy Rule by April 14, 2003.[90] Small health plans, however, have until April 14, 2004 to comply. **Small Health Plans.** A health plan with annual receipts of not more than $5 million is a small health plan.[91] Health plans that file certain federal tax returns and report receipts on those returns should use the guidance provided by the Small Business Administration at 13 Code of Federal Regulations (CFR) 121.104 to calculate annual receipts. Health plans that do not report receipts to the Internal Revenue Service (IRS), for example, group health plans regulated by the Employee Retirement Income Security Act 1974 (ERISA) that are exempt from filing income tax returns, should use proxy measures to determine their annual receipts.[92] See What constitutes a small health plan?
Copies of the Rule & Related Materials	The entire Privacy Rule, as well as guidance and additional materials, may be found on our website, http://www.hhs.gov/ocr/hipaa.

End Notes

[1] Pub. L. 104-191.

[2] 65 FR 82462.

[3] 67 FR 53182.

[4] 45 C.F.R. §§ 160.102, 160.103.

[5] Even if an entity, such as a community health center, does not meet the definition of a health plan, it may, nonetheless, meet the definition of a health care provider, and, if it transmits health information in electronic form in connection with the transactions for which the Secretary of HHS has adopted standards under HIPAA, may still be a covered entity.

[6] 45 C.F.R. §§ 160.102, 160.103; *see* Social Security Act § 1172(a)(3), 42 U.S.C. § 1320d-1(a)(3). The transaction standards are established by the HIPAA Transactions Rule at 45 C.F.R. Part 162.

[7] 45 C.F.R. § 160.103.

[8] 45 C.F.R. § 164.500(b).

[9] 45 C.F.R. § 160.103.

[10] 45 C.F.R. §§ 164.502(e), 164.504(e).

[11] 45 C.F.R. § 164.532

[12] 45 C.F.R. § 160.103.

[13] 45 C.F.R. § 160.103

[14] 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).

[15] The following identifiers of the individual or of relatives, employers, or household members of the individual must be removed to achieve the "safe harbor" method of de-identification: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of Census (1) the geographic units formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000; (C) All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses: (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and ® any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met. In addition to the removal of the above-stated identifiers, the covered entity may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual who is subject of the information. 45 C.F.R. § 164.514(b).

[16] 45 C.F.R. § 164.502(a).

[17] 45 C.F.R. § 164.502(a)(2).

[18] 45 C.F.R. § 164.502(a)(1).

[19] 45 C.F.R. § 164.506(c).

[20] 45 C.F.R. § 164.501.

[21] 45 C.F.R. § 164.501.

[22] 45 C.F.R. § 164.501.

[23] 45 C.F.R. § 164.508(a)(2)

[24] 45 C.F.R. § 164.506(b).

[25] 45 C.F.R. § 164.510(a).

[26] 45 C.F.R. § 164.510(b).

[27] 45 C.F.R. §§ 164.502(a)(1)(iii).

[28] *See* 45 C.F.R. § 164.512.

[29] 45 C.F.R. § 164.512(a).

[30] 45 C.F.R. § 164.512(b).

[31] 45 C.F.R. § 164.512(a), (c).

[32] 45 C.F.R. § 164.512(d).

[33] 45 C.F.R. § 164.512(e).

[34] 45 C.F.R. § 164.512(f).

[35] 45 C.F.R. § 164.512(g).

[36] 45 C.F.R. § 164.512(h).

[37] The Privacy Rule defines research as, "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." 45 C.F.R. § 164.501.

[38] 45 C.F.R. § 164.512(i).

[39] 45 CFR § 164.514(e).

[40] 45 C.F.R. § 164.512(j).

[41] 45 C.F.R. § 164.512(k).

[42] 45 C.F.R. § 164.512(l).

[43] 45 C.F.R. § 164.514(e). A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses: (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; (xvi) Full face photographic images and any comparable images. 45 C.F.R. § 164.514(e)(2).

[44] 45 C.F.R. § 164.508.

[45] A covered entity may condition the provision of health care solely to generate protected health information for disclosure to a third party on the individual giving authorization to disclose the

information to the third party. For example, a covered entity physician may condition the provision of a physical examination to be paid for by a life insurance issuer on an individual's authorization to disclose the results of that examination to the life insurance issuer. A health plan may condition enrollment or benefits eligibility on the individual giving authorization, requested before the individual's enrollment, to obtain protected health information (other than psychotherapy notes) to determine the individual's eligibility or enrollment or for underwriting or risk rating. A covered health care provider may condition treatment related to research (e.g., clinical trials) on the individual giving authorization to use or disclose the individual's protected health information for the research. 45 C.F.R. 508(b)(4).

[46] 45 CFR § 164.532.

[47] "Psychotherapy notes" means 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 of the individual's medical record. Psychotherapy notes excludes 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. 45 C.F.R. § 164.501.

[48] 45 C.F.R. § 164.508(a)(2).

[49] 45 C.F.R. §§ 164.501 and 164.508(a)(3).

[50] 45 C.F.R. §§ 164.502(b) and 164.514 (d).

[51] 45 C.F.R. §§ 164.520(a) and (b). A group health plan, or a health insurer or HMO with respect to the group health plan, that intends to disclose protected health information (including enrollment data or summary health information) to the plan sponsor, must state that fact in the notice. Special statements are also required in the notice if a covered entity intends to contact individuals about health-related benefits or services, treatment alternatives, or appointment reminders, or for the covered entity's own fundraising.

[52] 45 C.F.R. § 164.520(c).

[53] 45 C.F.R. § 164.520(d).

[54] 45 C.F.R. § 164.520(c).

[55] 45 C.F.R. § 164.524.

[56] 45 C.F.R. § 164.501.

[57] A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed by a licensed health care professional (who is designated by the covered entity and who did not participate in the original decision to deny), when a licensed health care professional has determined, in the exercise of professional judgment, that: (a) the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; (b) the protected health information makes reference to another person (unless such other person is a health care provider) and the access requested is reasonably likely to cause substantial harm to such other person; or (c) the request for access is made by the individual's personal representative and the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

A covered entity may deny access to individuals, without providing the individual an opportunity for review, in the following protected situations: (a) the protected health information falls under an exception to the right of access; (b) an inmate request for protected health information under certain circumstances; (c) information that a provider creates or obtains in the course of research that includes treatment for which the individual has agreed not to have access as part of consenting

to participate in the research (as long as access to the information is restored upon completion of the research); (d) for records subject to the Privacy Act, information to which access may be denied under the Privacy Act, 5 U.S.C. § 552a; and (e) information obtained under a promise of confidentiality from a source other than a health care provider, if granting access would likely reveal the source. 45 C.F.R. § 164.524.

[58] 45 C.F.R. § 164.526.

[59] Covered entities may deny an individual's request for amendment only under specified circumstances. A covered entity may deny the request if it: (a) may exclude the information from access by the individual; (b) did not create the information (unless the individual provides a reasonable basis to believe the originator is no longer available); (c) determines that the information is accurate and complete; or (d) does not hold the information in its designated record set. 164.526(a)(2).

[60] 45 C.F.R. § 164.528.

[61] 45 C.F.R. § 164.522(a).

[62] 45 C.F.R. § 164.522(a). In addition, a restriction agreed to by a covered entity is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.

[63] 45 C.F.R. § 164.522(b).

[64] 45 C.F.R. § 164.530(i).

[65] 45 C.F.R. § 164.530(a).

[66] 45 C.F.R. §160.103.

[67] 45 C.F.R. § 164.530(b).

[68] 45 C.F.R. § 164.530(e).

[69] 45 C.F.R. § 164.530(f).

[70] 45 C.F.R. § 164.530(c).

[71] 45 C.F.R. § 164.530(d).

[72] 45 C.F.R. § 164.520(b)(1)(vi).

[73] 45 C.F.R. § 164.530(g).

[74] 45 C.F.R. § 164.530(h).

[75] 45 C.F.R. § 164.530(j).

[76] 45 C.F.R. § 164.530(k).

[77] 45 C.F.R. §§ 164.103, 164.105.

[78] 45 C.F.R. § 164.103.

[79] 45 C.F.R. §164.105. Common ownership exists if an entity possesses an ownership or equity interest of five percent or more in another entity; common control exists if an entity has the direct or indirect power significantly to influence or direct the actions or policies of another entity. 45 C.F.R. §§ 164.103.

[80] The Privacy Rule at 45 C.F.R. § 160.103 identifies five types of organized health care arrangements:

- A clinically-integrated setting where individuals typically receive health care from more than one provider.
- An organized system of health care in which the participating covered entities hold themselves out to the public as part of a joint arrangement and jointly engage in

utilization review, quality assessment and improvement activities, or risk-sharing payment activities.

- A group health plan and the health insurer or HMO that insures the plan's benefits, with respect to protected health information created or received by the insurer or HMO that relates to individuals who are or have been participants or beneficiaries of the group health plan.
- All group health plans maintained by the same plan sponsor.
- All group health plans maintained by the same plan sponsor and all health insurers and HMOs that insure the plans' benefits, with respect to protected health information created or received by the insurers or HMOs that relates to individuals who are or have been participants or beneficiaries in the group health plans.

[81] 45 C.F.R. § 164.506(c)(5).

[82] 45 C.F.R. § 164.504(g).

[83] 45 C.F.R. § 164.504(f).

[84] 45 C.F.R. § 164.502(g).

[85] 45 C.F.R. §160.203.

[86] 45 C.F.R. § 160.202.

[87] 45 C.F.R.§ 160.304

[88] Pub. L. 104-191; 42 U.S.C. §1320d-5.

[89] Pub. L. 104-191; 42 U.S.C. §1320d-6.

[90] 45 C.F.R. § 164.534.

[91] 45 C.F.R. § 160.103.

[92] Fully insured health plans should use the amount of total premiums that they paid for health insurance benefits during the plan's last full fiscal year. Self-insured plans, both funded and unfunded, should use the total amount paid for health care claims by the employer, plan sponsor or benefit fund, as applicable to their circumstances, on behalf of the plan during the plan's last full fiscal year. Those plans that provide health benefits through a mix of purchased insurance and self-insurance should combine proxy measures to determine their total annual receipts.