



OCR PRIVACY BRIEF

SUMMARY OF THE HIPAA PRIVACY RULE



HIPAA Compliance Assistance

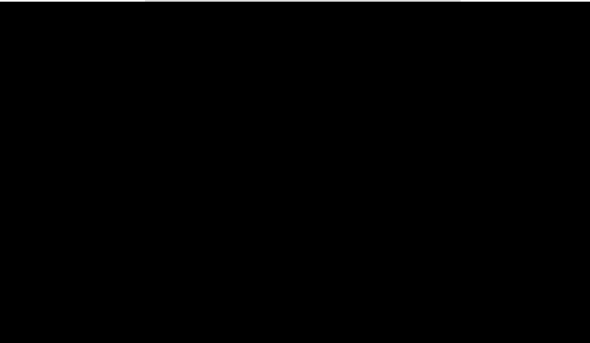
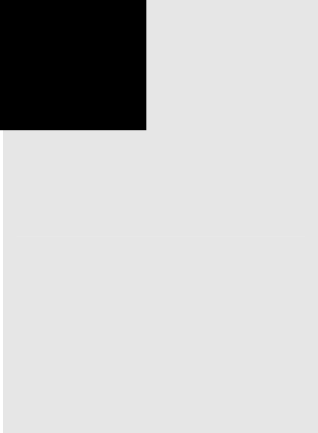
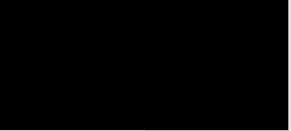
SUMMARY OF THE HIPAA PRIVACY RULE

Contents

Introduction	1
Statutory & Regulatory Background.....	1
Who is Covered by the Privacy Rule	2
Business Associates.....	3
What Information is Protected	3
General Principle for Uses and Disclosures	4
Permitted Uses and Disclosures	4
Authorized Uses and Disclosures.....	9
Limiting Uses and Disclosures to the Minimum Necessary	10
Notice and Other Individual Rights	11
Administrative Requirements.....	14
Organizational Options	15
Other Provisions: Personal Representatives and Minors	16
State Law.....	17
Enforcement and Penalties for Noncompliance	17
Compliance Dates	18
Copies of the Rule & Related Materials.....	18
End Notes	19

SUMMARY OF THE HIPAA PRIVACY RULE

<p>Introduction</p>	<p>The <i>Standards for Privacy of Individually Identifiable Health Information</i> (“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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
<p>Statutory & Regulatory Background</p>	<p>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 <i>Administrative Simplification</i> provisions.</p> <p>HIPAA required the Secretary to issue privacy regulations governing individually identifiable health information, if Congress did not enact privacy legislation within</p>



(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](#).

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

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 individual²¹ and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.

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) specification of health

(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 -0 Td(erg)1u5 (ted,)13.d.5 (e)T (IhTT (

statute, regulation, or court orders).²⁹

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](#).

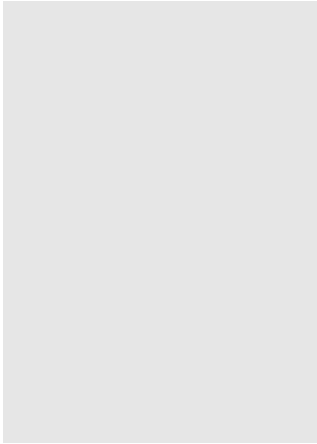
Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.³⁵

Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.³⁶

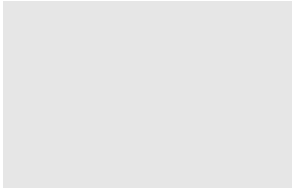
. “Research” is any systematic investigation designed to develop or contribute to generalizable knowledge.³⁷ The Privacy Rule permits a covered entity to use and disclose protected health information for research purposes, without an individual’s authorization, provided the covered entity obtains either: (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](#).

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

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



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](#).

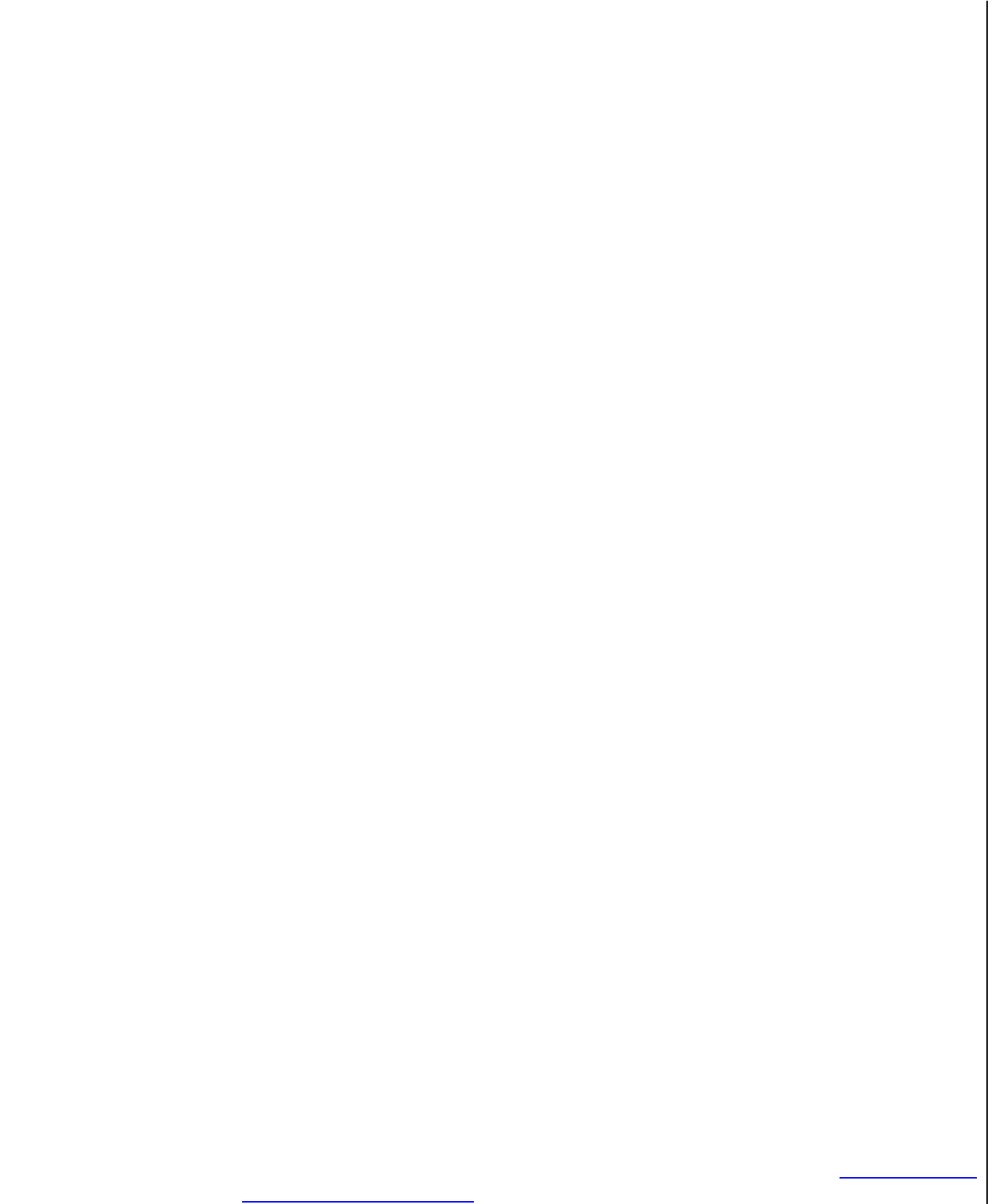


Covered entities, whether

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 a9.2 1c3cr3-10.1 (ve)ato

**Administrative
Requirements**





State Law	<p>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.</p> <p>Exception Determination. In addition, preemption of a contrary State law will not</p>
Enforcement and Penalties for Noncompliance	

~~15165.80 5165.504(32~~

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.