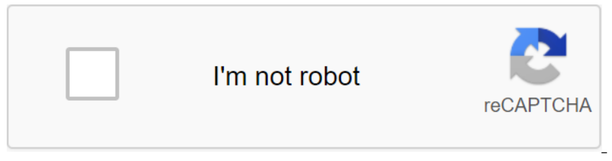
Hipaa notice of privacy practices form pdf



Continue

For the purposes of HIPAA Research is defined as: any systematic study (including research, testing and evaluation) that has as its primary purpose development or contribution to generalized knowledge. Identify De-Identified Data Definition Limited DataSet Show Me More... I want to... Enter eIRBGet Training This is a summary of key elements of the Privacy Regulation, including who is covered, what information is protected, and how protected health information can be used and disclosed. Because this is a review of the Privacy Code, it does not address all the details of each provision. Summary of the PDF Privacy Rules Introduction Standards for individually identifiable medical information (Privacy Rule) establishes, for the first time, a set of national standards to protect certain medical information. The U.S. Department of Health and Human Services (HHS) issued a Privacy Rule to comply with the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA1 Privacy Regulations relate to the use and disclosure of individual medical information, Protected medical information by organizations subject to the Privacy Rule, called covered organizations, as well as privacy standards for individuals to understand and monitor how their health information is used. Compliance with the Privacy Rule for voluntary compliance activities and penalties for civil funds. The primary purpose of the Privacy Rule is to ensure that individuals' medical information is properly protected while ensuring that the medical information is available to provide and promote high-quality care and to protect the health and well-being of the public. The rule balances, allowing for the important use of information while protecting the privacy of people who seek medical care and healing. Given that the health market is diverse, the rule is designed to be flexible and comprehensive to cover the different uses and disclosures that need to be addressed. This is a summary of the key elements of the Privacy Rule, not a complete or comprehensive compliance guide. Organizations governed by the Rule are required to comply with all its applicable requirements and should not rely on this summary as a source of legal information or advice. To make it easier for organizations to revise all the requirements of the Rule, the provisions of the Rule mentioned in this summary are included in the final notes. Visit our Privacy Rule section to view all the Rules as well learn more about how the Rule is applied. In the event of a conflict between this summary and the Rule, the Rule is regulated. The Public Law Act 104-191 on Public Insurance and Accountability was passed on 21 August 1996. Sections 261 to 264 HIPAA require HHS Secretary for Publicizing Standards for Electronic Exchange, Privacy and Security of Medical Information. Taken together, they are known as administrative simplification provisions. HIPAA requires the secretary to issue privacy rules governing individually identifiable health information if Congress has not passed privacy legislation within three years of hipAA's passage. Because Congress did not pass the Privacy Act, HHS drafted the proposed rule and released it for public comment on November 3, 1999. The department has received more than 52,000 comments from the public. The final ruling, the Privacy Rule, was issued on December 28, 2000.2 In March 2002, the Department proposed and issued for public discussion of changes to the Privacy Rules. The department received more than 11,000 comments. The final changes were published in its final form on 14 August 2002.3 Text, combining final regulation and changes can be found on 45 CFR Part 160 and Part 164, subcharging A and E. Who is covered by the Privacy Rule, as well as all administrative simplification rules, apply to health plans, medical focal points, and any health care provider that transmits medical information electronically in connection with operations for which the HHS secretary has adopted standards under HIPAA (covered persons). Use the CMS solution tool to help you determine if you're covered. Health plans. Individual and group plans that provide or pay the cost of care are covered by entities.4 Health plans include health, dental, vision, and prescription drug insurers, health care organizations (HMOs), Medicare, Medicaid, Medicare and Medicare supplement insurers, and long-term care insurers (excluding home nursing homes fixed-cost compensation policies). Health plans also include group health plans, employer-funded health plans, government and church health plans, and health plans for several employers. There are exceptions - a group health insurance plan with less than 50 participants, which is run solely by the employer who created and supports the plan, is not covered by the organization. Two types of government-funded programmes are not health plans: (1) those whose primary purpose is not to provide or pay for health care costs, such as the food stamp programme; and (2) those programmes whose main activities are direct health care, such as community-related 5 or grants to fund direct health care. Some types of insurance organizations are also not health insurance plans, including organizations that provide only workers' compensation, car insurance, and property and accident insurance. If the insurance company has a separate line of business, one of which is a health insurance plan, HIPAA rules apply to the organization regarding the line of business health insurance. Providers. Every health care provider, regardless of size, who electronically transmits medical information connection to certain transactions is a covered entity. These transactions include claims, benefit requests, referral authorization requests or other transactions for which HHS has set standards under the HIPAA Transaction Rule.6 The use of electronic technologies such as e-mail does not mean that the health care provider is a covered organization; The transfer must be in connection with a standard transaction. The privacy rule applies to the health care provider, whether he transmits these transactions electronically directly or uses the payment service or other third party to do so on his behalf. Health care providers include all service providers (e.g. institutional providers such as hospitals) and providers of health or medical services (e.g. unspecified providers such as doctors, dentists and other practitioners) as defined by Medicare, and any other person or organization that provides, bills or is paid for medical care. Health care centers are organizations that process non-standard information they receive from another organization, in a standard (i.e. standard format or data content), or vice versa.7 In most cases, medical focal points will receive individually identifiable medical information only when they provide these medical treatment services or a health care provider as a business partner. In such cases, only certain provisions of the Privacy Regulation apply to the use and disclosure of protected medical information.8 Medical clearing centers include billing services, reputational companies, public health management information systems, and value-added networks and switches if these organizations serve as a focal point. The business partner of the partners has been identified. Typically, a business partner is a person or organization other than a member of the workforce of a covered organization that performs certain functions or activities on behalf of or provides certain services to a covered organization that includes the use or disclosure of individually identifiable medical information. The functions or activities of business partners on behalf of the affected organization include claims processing, data analysis, usage review and billing.9 Business Partner Services for the person covered are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services. However, individuals or organizations are not considered business partners unless their functions or services are related to the use or disclosure of protected medical information and when any access is made to protected medical information will take place in any case. The organization covered may be a business partner of another affected organization. Business partner's contract. When a covered organization uses a contractor or other non-working member to perform the services or activities of a business partner, the rule requires that the organization covered includes certain information protection measures in a business partner's agreement (under certain circumstances government agencies may use alternative means to achieve the same protection). In a business partner contract, the organization covered must impose certain written guarantees on individually identified medical information used or disclosed by its business partners.10 In addition, the organization covered cannot under contract authorize its business partner to use or disclose protected medical information that would violate the Rule. Covered organizations that had a valid written contract or agreement with business partners until 15 October 2002, which was not extended or amended until 14 April 2003, were allowed to continue under the contract until they extended the contract or on 14 April 2004, depending on whether it was the first.11 See. additional advice on business partners and the language of an exemplary business partner. What information is protected by protected medical information. The Privacy Rule protects all individually identifiable medical information that an organization or its business partner has or transmits, in any form or media, whether electronic, paper or oral. The Privacy Rule calls this information protected medical information (PHI). 12 Individually identifiable medical information is information, including demographic data, which relates to: past, present or future physical or mental health or human condition, medical care to an individual, or past, present or future payment for medical care to an individual, and which identifies a person or for whom there is reasonable reason to believe that it can be used to identify an individual.13 Individually identifiable health information includes a lot of common data. for example, name, address, date of birth, Social Security number). The Privacy Rule excludes from protected medical information the employment records that the organization maintains as an employer and education and some other records subject to or defined in the Family Education and Privacy Rights Act, 20 U.S.C. No.1232g. De-Identified Health Information. There is no restriction on the use or disclosure of deidentified medical information.14 Deidentified health information does not identify or provide reasonable grounds for identifying a person. There are two ways to de-determinify information; Or: (1) the official definition of qualified statisticians; or (2) it is required that the IDs of a person and relatives, family members and employers and adequate only if the person covered does not have the actual knowledge that the remaining information can be used to identify the person.15 The General Principle of Use and Disclosure of the Basic Principle. The main purpose of the Privacy Rule is to identify and limit the circumstances in which information can be used or disclosed by the affected organizations. The organization covered may not use or disclose protected medical information, except for either: (1), as the Privacy Rule allows or requires; or (2) as the person who is the subject of the information (or the person's personal representative) authorizes in writing.16 Required disclosure. The organization covered must disclose protected medical information only in two situations: (a) individuals (or their personal representatives) in particular when they request access to the medical information protected by it or the accounting of its protected medical information; and (b) HHS when it conducts an investigation of compliance or review or enforcement action.17 See additional recommendations on government access. Permitted use and disclosure of permitted uses and disclosures. A person who is covered is permitted, but does not require, to use or disclose protected medical information without the permission of an individual for the following purposes or situations: (1) For an individual (unless required to access or account for disclosure); (2) Treatment, pay and health care operations; (3) Opportunity to agree or object; (4) Incident with other authorized use and disclosure; (5) Public interest and benefits activities; and (6) A limited data set for research, public health or health operations.18 Covered organizations can rely on professional ethics and best judgment when deciding which of these permissive uses and disclosures to make. (1) To the Individual. The organization covered may disclose protected medical information to the person who is the subject of the information. (2) Treatment, Payment, Health Surgery. The organization covered may use and disclose protected medical information for its own health care, payment and operations activities.19 The organization covered may also disclose protected medical information for the treatment of any health care provider, the payment activities of another person in the community and any health care provider, or health operations of another affected organization, including either quality or competency activities or activities either fraud and the detection of abuse and compliance activities if both persons involved have or have had an relationship with an individual and protected health information relates to the relationship. Additional recommendations for health care treatment, payment and operations can be seen. Treatment is the provision, coordination or management of health care and related services to a person by one or more health care providers, consultation between patient providers and referral of a patient to another.20 Payment includes the operation of the health insurance plan to obtain premiums, to determine or perform obligations to cover and provide benefits, as well as to provide or receive reimbursement for medical care provided to the person21, and the activities of the health care facility. get paid or get reimbursed for providing caring for the man. Health operations are of any of the following activities: (a) assessing quality and improving activities, including treatment and coordination of care; (b) Competence activities, including an assessment of the health provider's effectiveness or health insurance plan, certification and accreditation; (c) Conducting or organizing medical reviews, audits or legal services, including fraud and abuse and compliance programmes; (d) Certain insurance features, such as underwriting, risk rating and risk reinsurance; Business planning, development, management and administration; and (f) Business management and the overall administrative activities of the organization, including, but not limited to: de-identification of protected medical information, the creation of a limited data set and a certain fundraising for the benefit of the organization covered.22 Most uses and disclosures of psychotherapeutic notes for treatment, payment and medical operations require the authorization described below.23 Obtaining consent (written authorization from individuals to use and disclose their protected medical information for treatment purposes.23 Payment, and medical operations) is optional under the Privacy Rule for all entities.24 Content consent forms, and the consent process are at the discretion of the covered organization, choosing to obtain consent. (3) Use and disclosure information with the ability to negotiate or object. An informal authorization can be obtained by directly clarifying the identity or circumstances that clearly enable a person to agree, agree or object. Where a person is incapacitated, in an emergency or not available, the organizations covered may generally use such uses and disclosures if the use or disclosure is determined in the best interests of the individual in the exercise of his professional judgment. Object catalogs. It is common practice in many medical facilities, such as hospitals, to maintain a patient's contact information catalog. The provider covered by the insurance may rely on the unofficial permission of a person to list in his agency's catalogue the name, general status, religious affiliation and location in the provider's establishment.25 The Supplier may then report the person's condition and whereabouts to any person requesting his name, and may disclose religious affiliation to the clergy. Members of the clergy are not required to request a person by name when questioning the patient's religious affiliation. For notification and other purposes. The covered organization may also rely on an informal permission of a person to disclose family, family or friends or others identified by the person, protected medical information directly related to the person's involvement in the care or payment of medical care. 26 This provision, for example, allows a pharmacist pharmacist person acting on behalf of the patient. Similarly, the organization covered may rely on the informal permission of a person to use or disclose protected medical information in order to notify (including the identification or location) of family members, personal representatives or others responsible for caring for the person's whereabouts, general condition or death. In addition, protected health information may be disclosed for the purpose of notifying public or private organizations authorized by law or charter to assist in disaster relief efforts. (4) Accidental use and disclosure. The privacy rule does not require that all risks of accidental use or disclosure of protected medical information be eliminated. The use or disclosure of this information, which arises as a result or as an incident, other authorized use or disclosure is permitted as long as the organization has accepted reasonable assurances, as required by the Privacy Rule, and general information has been limited to the minimum necessary as required by the Privacy Rule. additional guidance on the accidental use and disclosure of information. (5) Public interest and benefits of activity. The Privacy Rule authorizes the use and disclosure of protected medical information without the permission or permission of an individual for 12 national priority purposes.28 These disclosures are permitted, although not required, by the Rule in recognition of the important use of medical information outside the health context. Specific terms or restrictions apply to each goal of the public interest, striking a balance between individual privacy interests and the need of the public interest for this information. Required by law. Organizations covered may use and disclose protected medical information without individual authorization, as required by law (including by statute, regulation or court orders).29 Public health activities. Organizations covered may disclose protected medical information: (1) to public health authorities authorized by law to collect or receive such information to prevent or control diseases, injuries or disabilities, as well as public health authorities or other public bodies authorized to receive reports of child abuse and neglect; (2) organizations subject to FDA regulations regarding FDA-regulated products or activities for purposes such as reporting adverse events, product tracking, product recalls, and post-marketing surveillance; (3) persons who may have contracted or contracted an infectious disease when the notification is authorized by law; and (4) employers, employees, at the request of employers, for information regarding work-related illness or injury or work-related medical supervision, because such information is required by the employer under the Occupational Safety and Health Administration (OHSA), Mine Safety and Health Administration (MHSA), or similar state law.30 See additional recommendations on public health activities and and web pages on public health and HIPAA. Victims of abuse, neglect or domestic violence. Under certain circumstances, the organizations covered may disclose protected medical information to the relevant public authorities regarding victims of abuse, neglect or domestic violence.31 Health surveillance activities. Organizations covered may disclose protected health information to health authorities (as defined in the Regulation) for the purposes of legally permitted health surveillance activities, such as audits and investigations necessary to oversee the health system and government benefits programs.32 Judicial and Administrative Proceedings. Organizations covered may disclose protected medical information in a judicial or administrative process if the request for information is made by order of a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other legal process if certain safeguards are provided regarding the notification of an individual or a protective order.33 Targets of law enforcement agencies. Organizations covered may disclose protected medical information to law enforcement officials in order to ensure compliance with the following six circumstances and subject to certain conditions: (1) in accordance with the law (including court orders, court orders, subpoenas) and administrative requests; (2) identify or find a suspect, fugitive, material witness or missing person; 3) in response to a request from a law enforcement official to provide information on the victim or alleged victim of the crime; 4) to warn law enforcement agencies about the death of a person if the organization covered suspects that the cause of death was criminal activity; (5) where the organization is covered, it is considered that protected health information is evidence of a crime committed in its premises; and (6) a medical worker in an emergency medical care that does not take place on its territory when necessary to inform law enforcement about the commission and nature of the crime, the whereabouts of the victims of a crime or crime, and the perpetrator of a crime.34 Covered organizations may disclose protected medical information to funeral directors as needed, as well as to coroners or medical experts to identify the deceased person, determine the cause of death and perform other functions authorized by law.35 The Body, Eye or Tissue Donation. Covered organizations may use or disclose protected medical information to facilitate the donation and transplantation of cadaveric organs, eyes and tissues.36 Research is any systematic investigation aimed at developing or contributing to generalized knowledge.37 The Privacy Rule allows a covered entity to use and disclose protected medical information for research purposes, without the permission of an individual, provided that the organization is required to receive either: (1) documentation that has a change or waiver of individual permission to use or disclose protected medical information about them for research purposes. Approved by the Institutional Review Board or the Privacy Council; (2) The suggestion from the researcher that the use or disclosure of protected medical information is solely for the preparation of the study protocol or for a similar purpose of preparation for research, that the researcher will not remove any protected medical information from the person covered, and that the study requires protected health information for which access is sought; or (3) a view from a researcher that that the requested use or disclosure is intended solely for the study of the protected medical information of deceased persons, that the requested protected health information is necessary for research, and, at the request of the organization covered, the documentation of the deaths of persons requested for information.38 The covered organization may also use or disclose, without the permission of individuals, a limited set of data protected medical information for research purposes (see discussion below).39 See additional recommendations on the research and publication of NIH Health in Research: Understanding hipAA Privacy Rules. A serious threat to health or safety. Organizations covered may disclose protected medical information that they believe is necessary to prevent or mitigate a serious and imminent threat to a person or public when such disclosure is made to someone who they believe can prevent or mitigate a threat (including the purpose of the threat). Covered organizations may also disclose information to law enforcement agencies if information is needed to identify or apprehend a fugitive or violent criminal.40 Major government functions. Permission is not required to use or disclose protected medical information for certain basic government functions. Such functions include: ensuring the proper implementation of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the president, enacting medical definitions of suitability for U.S. State Department employees, protecting the health and safety of inmates or correctional officers, and determining the right to enroll or register in some government employee compensation programs.41 Organizations covered may disclose protected medical information in accordance with permits and comply with employee compensation laws and other similar programs that provide benefits for work-related injuries or illnesses.42 Cm. additional recommendations for employee compensation. (6) Limited data set. The limited data set is protected medical information from some of the specified direct identifiers of individuals and their relatives, family members and employers have been removed.43 A limited data set can be used and disclosed for research, health operations and public health purposes, provided that the recipient enters into a data usage agreement promising certain safeguards for protected medical information under a limited data set. Commissioner and disclosure permission. The covered organization must obtain a person's written permission for any use or disclosure of protected medical information that is not for treatment, payment or medical operations or otherwise permitted or required by the Privacy Rule.44 The covered organization may not be entitled to individual authorization, except in limited circumstances.45 Permission must be written under specific conditions. It may authorize the use and disclosure of protected medical information covered by an organization seeking permission, or by a third party. Examples of disclosures that would require a person's permission include disclosing information to a life insurer for coverage, disclosing to an employer the results of a physical or laboratory test prior to employment or disclosing information to a pharmaceutical firm for their marketing purposes. All permits must be in plain language and contain specific information about the information that will be disclosed or used, the person (s) disclosing and obtaining information, expiration, the right to revoke in writing, and other data. The Privacy Rule contains transitional provisions applicable to permits and other express legal permissions obtained prior to April 14, 2003.46 Psychotherapeutic notes.47 The covered organization must obtain permission from an individual to use or disclose psychotherapeutic notes with the following exceptions: the covered organization that originated the notes can use them for treatment. The person covered may use or disclose, without the permission of an individual, psychotherapeutic notes, for his own training, and defend himself in a trial brought by a person, for HHS to investigate or determine compliance with the confidentiality rules covered by the organization, to prevent a serious and immediate threat to public health or safety, to the health agency for legitimate oversight of the creator of psychotherapeutic notes, for the lawful activities of the coroner or the coroner or the medical examiner or in accordance with the requirements of the law. Marketing. Marketing is any message about a product or service that encourages recipients to purchase or use a product or service.49 The Privacy Rule cuts out the following health-related activities from this definition of marketing: Messages to describe health-related products or services, or payment for them, provided or included in the benefits plan of the organization covered by the organization, making a communication; Reports of participating providers on the network of health care providers or health plan, replacement or improvement of the health plan, as well as health-related products or services, only for health plan participants who add value but are not part of the benefits plan; Communication for the treatment of personality; and communication to treat cases or coordinate human care, or to direct or recommend alternative treatments, therapies, health care providers or or or Solo. Marketing is also an agreement between the organization covered and any other organization under which the organization covered discloses protected medical information in exchange for direct or indirect remuneration so that another organization can report its own products or services that encourage the use or purchase of these products or services. The person covered must obtain permission to use or disclose protected medical information for marketing, except for face marketing messages between the applicant and the individual, as well as to provide the organization's covered advertising gifts of face value. However, no permission is required to make a message that falls under one of the exceptions to the definition of marketing. A marketing authorization, which includes receiving direct or indirect remuneration from a third party by the covered organization, must disclose this fact. See more marketing tips. Limit the use and disclosure to the minimum required. A central aspect of the Privacy Rule is the principle of minimal use and disclosure. The organization covered must make reasonable efforts to use, disclose and request only the minimum amount of protected medical information required to achieve its intended purpose of use, disclosure or request.50 The organization must develop and implement policies and procedures to reasonably limit the use and disclosure required to the minimum required. When the minimum required standard applies to the use or disclosure of information, the organization covered cannot use, disclose or request all medical documentation for a specific purpose unless it can specifically substantiate the entire record as a reasonable amount necessary for this purpose. Additional recommendations for minimum need. The minimum requirement required is not imposed in any of the following circumstances: (a) disclosure or request of a health care provider for treatment; Disclosure to the person who is the subject of the information or to the person's personal representative; (c) Use or disclosure made in accordance with permission; Disclosure to HHS to investigate complaints, verify compliance or enforce compliance; Use or disclosure of information required by law; or (f) use or disclosure required to comply with the HIPAA Transaction Rules or other HIPAA Administrative Simplification Regulations. Access and use. For internal use, the organization covered must develop and implement policies and procedures that restrict the access and use of protected medical information based on roles of their workforce members. These strategies and procedures should identify individuals or classes of persons who have access to protected medical information to carry out their duties, the category of protected medical information to which access is required, and any conditions under which they need information to do their job. Disclosure and disclosure requests. Covered persons should implement policies and procedures (which may be standard protocols) for routine, repetitive disclosures or disclosure requests that restrict protected medical information disclosed by what is the minimum amount reasonably necessary to achieve the disclosure goal. No individual review of each disclosure is required. For non-routine, non-recurring disclosures or requests for disclosure that it makes, the organizations covered must develop criteria to limit the disclosure reasonably necessary to achieve the goal of disclosing and reviewing each of these requests individually in accordance with established criteria. Reasonable addiction. If another covered organization makes a request for the protection of medical information, the organization covered can, if it is reasonable, rely on the request under this minimum required standard. Similarly, the organization covered may rely on requests as minimally necessary protected medical information from: (a) public official, (b) a professional (e.g. a lawyer or accountant) who is a business partner of a covered organization, seeking information to provide services or to a covered organization; or (c) a researcher who provides the documentation or presentation required by the Privacy Rule for the study. Notice and other individual Privacy Rights Practices Notice. Each organization covered, with a few exceptions, must provide a notice of its privacy practices.51 The Privacy Rule requires that the notification contain certain items. The notice should describe how the organization uses and discloses protected medical information. The notice should be responsible for the privacy protection of the organization, the notification of confidentiality practices, and compliance with the terms of the current notice. The notice should describe the rights of individuals, including the right to complain to HHS and to the organization covered, if they believe that their privacy rights have been violated. The notification should contain a contact point for more information and complaints to the affected organization. Organizations covered must act in accordance with their notices. The rule also contains specific distribution requirements for direct health care providers, all other health care providers, and health plans. Additional recommendations for notification. The distribution of notifications. The health care provider covered by the insurance, which has a direct relationship to treatment with individuals, had until 14 April 2003 to deliver a confidentiality notice to patients as follows: the first meeting to provide personal delivery services (to visit patients), automatic and simultaneous electronic response (for the provision of electronic services) and prompt mailing (for the delivery of telephone services); By posting notice at every service delivery site in a clear and prominent place where people seeking service can reasonably be deducted notice; and in emergencies, the supplier supplier submit your notice as soon as it is feasible after the emergency subsides. The organizations covered, whether they are direct providers of treatment services or indirect treatment providers (such as laboratories) or health insurance plans, must notify any person on request.52 The organization must also make its notice electronically available on any website it supports to serve customers or receive information about benefits. Organizations involved in an organized health care arrangement may use a joint notice of confidentiality if each of them agrees to comply with the contents of the notice regarding protected medical information created or received in connection with participation in the agreement.53 The distribution of joint notification to any organization covered by the organization involved in an organized health care facility, at the first time when an OHCA member is required to provide a notice, satisfies the obligation to distribute other participants in organized health care. The health insurance plan must distribute privacy notices to each of its members by the date of compliance with the Privacy Regulations. The health plan must then notify each new participant when they sign up and send a reminder to each participant at least once every three years that the notification is available on request. The health insurance plan meets its distribution obligations by placing a notice to the named insured, i.e. the subscriber for coverage, which also applies to spouses and dependents. Confirmation of notification. A provider of direct relationships with individuals must make a good faith effort to obtain written confirmation from patients receiving a confidentiality notice.54 The Privacy Rule does not prescribe any specific content for confirmation. The supplier must document the reason for the refusal to receive written confirmation of the patient. The supplier is exempt from the need to request confirmation in an emergency treatment. Access. Except in certain circumstances, individuals are entitled to view and receive a copy of their protected medical information in the designated report on the organization,55 the designated set of records is that a group of records, a slace or covered organization, which is used, in full or in part, to make decisions about individuals, or it is the

medical and payment records of the provider about individuals or the registration of a health insurance plan , payment, consideration of claims, as well as the system of recording cases or medical management.56 Rule excludes from the right of access to protected medical information: psychotherapeutic notes, information collected for trial, laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information, hired by certain research laboratories. With regard to information included in the right of access, the organizations covered may deny an individual access in certain specific situations, such as where a health professional believes that access can be accessed harm to a person or another person. In such situations, a person should be given the right to have such waivers reviewed by a licensed health care professional in order to obtain a second opinion.57 Covered organizations may charge a reasonable, cost-based copying fee and postage. Amendment. The rule gives individuals the right to make changes to their protected medical information under legal entities' insurance if the information is inaccurate or incomplete. 58 If the organization accepts the request for amendments, it must make a reasonable effort to amend the persons who, in the individual's opinion, need it, as well as persons who are known to be able to rely on that information to the detriment of that person.59 If the request is rejected, the organizations concerned must provide that person with a written rebuttal and a rebuttal to that person to submit a statement of dissent. The rule defines the processes of requesting and responding to a request for amendments. The organization covered must amend the protected medical information in its designated report, which is set after receiving notification of amendments from another person covered. Accounting disclosure. Individuals have the right to account for the disclosure of their protected medical information covered by the organization or business partners covered by the organization.60 The maximum accounting period is six years immediately prior to the accounting request, except that the organization covered is not required to account for any disclosures made prior to the date of compliance with the confidentiality rule. The privacy rule does not require disclosure: (a) for treatment, payment or medical operations; (b) To a person or personal representative; (c) To notify or persons involved in a person's health care or pay for medical care, disaster relief or agency directories; (d) In accordance with the permit; (e) A limited set of data; (f) For national security or intelligence purposes; (g) Correctional facilities or law enforcement officers with specific objectives for prisoners or persons legally detained; or (h) an incident involving other permitted or required use or disclosure. The accounting of information to health authorities and law enforcement officials should be temporarily suspended in their written submission that accounting is likely to impede their activities. Requesting a restriction. Individuals have the right to request the organization to restrict the use or disclosure of protected medical information for treatment, payment or operations in the field of health care, disclosure participating in health care or paying for medical care, or disclosing information to notify family members or others of the general condition, whereabouts or death of that person.61 The organization is not required to accept requests for restrictions. The covered organization, which agrees, must abide by the agreed restrictions, with the exception of the exception of treatment of a person in emergency medical care.62 Confidential communication requirements. Health plans and health care providers covered should allow individuals to request alternative means or a place to receive messages of protected medical information through other means other than those commonly used by the organization.63 For example, an individual may require that the provider communicate with that person through the specified address or phone number. Similarly, an individual may require the supplier to send messages in a closed envelope rather than on a postcard. Health plans should take reasonable consideration into account if a person indicates that disclosing all or part of protected medical information may endanger a person. A health insurance plan cannot question a person's claim of a threat. Any organization covered may be subject to a confidential request for a message from a person indicating an alternative address or method of contact and explaining how any payment will be made. HHS recognizes that the organizations covered range from the smallest provider to the largest, multi-city health plan. Therefore, the flexibility and scalability of the Rule are designed to allow covered entities to analyze their own needs and implement solutions that are appropriate for their own environment. What is appropriate for a specific organization covered will depend on the nature of the organization's activities, as well as on the size and resources of the organization covered. Privacy policies and procedures. The organization covered must develop and implement written privacy policies and procedures consistent with the Privacy Regulation.64 Staff Privacy. The organization covered must appoint a privacy officer responsible for the development and implementation of its privacy policies and procedures, as well as the contact or contact office responsible for receiving complaints and providing individuals with information about the privacy practices of the affected organization.65 Training and management of the workforce. The workforce comprises staff, volunteers, interns, and others whose conduct is under the direct control of the organization (regardless of whether the organization is paid for).66 The organization involved must train all members of the workforce in its policies and procedures, as necessary and appropriately, to carry out their functions.67 The organization must have and apply appropriate sanctions against members of the workforce. that violates its privacy policies and procedures or privacy rules.68 Mitigation. The organization covered should mitigate, as far as possible, any the impact, which she learns was caused by the use or disclosure of protected medical information by her employees or business partners, in violation of her privacy policies and procedures or privacy rules. The organization covered must maintain reasonable and appropriate administrative, technical and physical safeguards For example, intentional or unintentional use or disclosure of protected medical information in violation of the Privacy Rule and limiting its accidental use and disclosure in accordance with other authorized or mandatory use or disclosure.70 For example, such safeguards may include shredding documents containing protected medical information before giving up it, protecting medical records by blocking and locking or skipping the code, and restricting access to keys or pass code. More advice on random use and disclosure can be found. Complaints. The organization covered must have procedures for individuals to complain about its compliance with its privacy policies and procedures and privacy rules.71 The organization must explain these procedures in its privacy practice notice.72 Among other things, the affected organization must determine who individuals can file complaints with the affected organization and report that complaints can also be submitted to the HHS secretary. Retribution and denial. The organization concerned may not retaliate against a person for exercising the rights of the Privacy Rule, for assisting in the investigation of HHS or other relevant authority, or for opposing an act or practice that a person believes in good faith violates the Privacy Rule.73 An within-73 organization may not require an individual to waive any right under the Privacy Rule as a condition for receiving treatment. , payment, as well as enrollment or benefits eligibility.74 documentation and record deduction. The organization covered must maintain up to six years after the date of their establishment or the last date of introduction into force, its privacy policies and procedures, privacy notices, the location of complaints and other actions, activities and designations that are required to be documented.75 A fully insured health insurance plan for the Exclusion group. The only administrative obligations with which a fully insured group health plan, which has no more than enrolment data and consolidated medical information, are required to comply (1) the prohibition of retaliation and waiver of individual rights, and (2) the documentation requirements for the plan documents, if such documents are changed to ensure that protected medical information is disclosed to the health insurance issuer or HMO that provides the group's health insurance plan.76 Organizational Options.76 The Organizational Options Rule contains provisions relating to various organizational issues that may affect the functioning of privacy protections. Hybrid education. The Privacy Rule allows a person who is single person and who performs both covered and un-covered functions to be elected as a hybrid. 77 (Actions that make a person or organization a covered organization are its covered functions. 78) To be a hybrid entity, the organization covered must outline in writing its operations, which perform covered functions as one or more components of health care. After the appointment of this appointment, most of the requirements of the Privacy Rules health-only components only. The entity covered, which does not make this designation, is fully subject to the Privacy Rule. Affiliated organization. Legitimately, individual organizations that are linked by common property or control may designate themselves (including their health components) as a single covered organization to comply with the Privacy Regulations.79 The designation must be in writing. An affiliated organization, performing several covered functions, must perform its various covered functions in accordance with the provisions of the Privacy Rule applicable to these covered functions. Organized health organization. The Privacy Rule defines relationships in which participating organizations share protected medical information to manage and benefit their common enterprise as organized health mechanisms. 80 organizations covered in an organized health care mechanism can share secure medical information with each other for joint health operations. The organization covered, performing several of the functions covered, must perform its various covered functions in accordance with the provisions of the Privacy Regulation applicable to these covered functions.82 The organization covered may not use or disclose protected medical information of a person who receives services from one covered function (e.g. a health care provider) for another covered function (e.g., a health insurance plan) if a person is not affiliated with another function. Disclosure of a group plan plan for plan sponsors. The group health insurance plan and the health insurer or HMO proposed by the plan may disclose the following protected medical information to the plan sponsor - the employer, the union, or other employee organization that sponsors and supports the group health care plan83: information about registration or registration for a group health plan or health insurer or HMO proposed by the plan. At the request of the plan's sponsor, consolidated health information for the plan sponsor is used to obtain premium health insurance applications through a group health plan, or to modify, modify or terminate the group's health plan. Summary health information is information that summarizes the history of claims, claims costs, or types of claims experiences of individuals for whom the plan sponsor has provided health benefits through the group's health plan, and that is devoid of all individual identifiers except the five-digit postcode (although it should not qualify as deidentified by protected medical information). Protected health information members of the group's health insurance plan to sponsor the plan plan management functions. The plan must receive certification from the plan's sponsor that the program of the health plan has been amended to limit the sponsor's use of the plan and the disclosure of protected medical information. These restrictions should include the notion that the plan plan will not use or disclose protected medical information for any employment-related actions or decisions or any other benefit plan. Other provisions: Personal representatives and minor personal representatives. The Privacy Rule requires a person to consider a personal representative as well as an individual in relation to the use and disclosure of protected medical information, as well as human rights under Rule.84 A personal representative is legally authorized to make medical decisions on behalf of an individual or to act in the interests of the deceased person or property. The Confidentiality Rule allows for an exception if the organization covered has a reasonable belief that the individual may abuse or neglect that person, or that the treatment of that person as a personal representative may otherwise endanger that person. Special case: Juvenile. In most cases, parents are the personal representatives of their minor children. Therefore, in most cases, parents can exercise individual rights, such as access to medical records, on behalf of their minor children. In some exceptional cases, the parent is not considered a personal representative. In such situations, the Privacy Rule applies to state and other legislation in order to determine the rights of parents to access and control the protected medical information of their minor children. If state and other laws make no mention of parents' access to the protected medical information of a minor, the organization covered has the right to provide or deny parents access to the minor's medical information, provided that the decision is made by a licensed health care professional in the exercise of professional judgment. See additional recommendations for personal representatives. Pre-emption of state law. In general, state laws contrary to the Privacy Rule are pre-empted by federal requirements, meaning that federal requirements will be applied.85 Contrary to the means that the person covered will not be able to comply with both state and federal requirements, or that the provision of state law is an impediment to achieving all the objectives and objectives of the HIPAA.86 Act of Privacy provision provides for exclusion from the general rule of federal law. that (1) relate to the confidentiality of individually identifiable medical information and provide greater protection of confidentiality or the right to privacy in relation to such information, (2) provide for reporting of illness or injury, child abuse, or death, or for public health surveillance, investigation or intervention, or (3) require certain health plan reporting, such as management or financial audit. Definition of an exception. In addition, pre-emption of opposing state legislation will not happen if HHS responds to a request from a state or other entity or person to establish that state law is necessary to prevent fraud and abuse of abuse to provide or pay for health care, it is necessary to ensure proper government regulation of insurance and health plans to the extent that it is expressly permitted by law or regulation, is necessary for the state to report on the provision of medical care or expenses necessary for the purposes of service of irresistible public health, safety or social necessity, and, in the case of the privacy regulations, if the Secretary determines that intrusion into private life is justified in balancing the necessary; or has, as its primary purpose, the regulation of production, registration, distribution, distribution or other control over any controlled substances (as defined in 21 U.S.C. 802), or it is considered a controlled substance under state law. Enforcement and fines for non-compliance. The Privacy Standards of Individually Identifiable Medical Information (Privacy Rule) establish a number of national standards for the use and disclosure of a person's medical information, called protected medical information, under the control of covered organizations, as well as standards for granting individuals privacy rights to understand and monitor how their health information is used. The Department of Health and Human Services, the Office of Civil Rights (OIG), is responsible for managing and enforcing these standards and can investigate complaints and verify compliance. In accordance with the privacy guidelines provided by the Privacy Code, OCR will seek to work with the organizations covered and may provide technical assistance to help them voluntarily comply with the Privacy Rule. Covered persons who voluntarily do not comply with these standards may be fined in the form of civil funds. In addition, some violations of the Privacy Rule may be prosecuted. These punishment provisions are explained below. Penalties for civil money. OCR may impose a fine on the person covered for non-compliance with the Privacy Rule. Fines would vary considerably depending on factors such as the date of the violation, whether the organization was aware of the non-compliance or whether the non-compliance was caused by wilful neglect. Fines may not exceed the calendar year limit for numerous violations of the same requirement. For violations that occurred before 2/18/2009 for violations that occurred on or after 2/18/2009 A fine of up to $100 for violation of $100 to $50,000 or more for violation of Calendar Year Cap $25,000 $150,000 penalty will not be imposed for violations in certain circumstances, circumstances, such as non-compliance: caused wilful neglect, and was corrected within a 30-day period after the organization knew or should have known about the non-compliance occurred (if the period was extended at the discretion of the OCR); or the Ministry of Justice has criminally penalized non-compliance (see below). In addition, OCR may punishment if failure was caused by a reasonable reason and the punishment would be excessive given the nature and extent of non-compliance. Before the OCD imposes a fine, it will notify the person concerned and allow the person concerned to provide written evidence of the circumstances that would reduce or prohibit the fine. This evidence must be submitted to OCR within 30 days of receiving the notice. In addition, if the OCD states that it intends to impose a fine, the organization covered has the right to request an administrative hearing to appeal the proposed penalty. Criminal penalties. A person who knowingly obtains or discloses individually identifiable medical information in violation of the Privacy Rule may be sentenced to up to $50,000 in criminal charges and up to one year's imprisonment. The criminal penalty increases to $100,000 and up to five years in prison if the wrongful conduct includes false claims, and up to $250,000 and up to 10 years in prison if the wrongful conduct includes intent to sell, transfer or use identifiable health information for commercial gain, personal gain or malicious harm. The Ministry of Justice is responsible for criminal prosecutions in accordance with the Schedule of Compliance of Secret Dates. All organizations covered, with the exception of small health plans, had until 14 April 2003.90, but had until 14 April 2004 to comply with the Health Plan. Small health plans. A health plan with annual revenues of no more than $5 million is a small health plan.91 Health Plans that file certain federal tax returns and reporting receipts for these returns must use guidance provided by the Small Business Administration in the 13th Code of Federal Regulations (CFR) 121.104 to calculate annual revenue. Health plans that do not report income to the Internal Revenue Service (IRS), such as group health plans regulated by the Retirement Income Act 1974 (ERISA), which are exempt from income tax filings, must use proxy measures to determine their annual income.92See What is a small health insurance plan? Copies of the Rules and related materials see our Text of All Rules section of our site for a full set of rules on facilitating HIPAA's administrative procedures and understanding HIPAA for additional guidance materials. End Notes 1 Pub. L. 104-191. 2 65 FR 82462. 3 67 FR 53182. 4 45 C.F.R. No 160.102, 160.103. 5 Even if an organization, such as a community health centre, does not meet the definition of a health plan, it may nevertheless meet the definition of medical services and, if it transmits medical information electronically in connection with operations for which the HHS Secretary has adopted standards in accordance with HIPAA, can still be covered by the organization. 6 45 C.F.R. No 160.102, 160.103; See Social Insurance Act No. 1172 (a) (3), 42 U.S.C. No. 1320d-1 (a) (3). Transaction standards are set by the HIPAA Transaction Rule at 45 years of age Part 162. 7 45 C.F.R. No 160.103. 8 45 K.F.R. No 164.500 (b). 9 45 C.F.R. No 160.103. 10 45 C.F.R. No 164.502 (e), 164.504 (e). 11 45 C.F.R. No 164.532 12 45 C.F.R. No 160.103. 13 45 C.F.R. No 160.103 14 45 C.F.R. No 164.502 (d) (2), 164.514 (a) and (b). 15 The following identifiers of a person or relatives, employers or members of a household person must be removed to achieve the method of de-identification of safe harbor: (A) Names; (b) All geographical units are smaller than the state, including street addresses, city, county, plot, postcode and their equivalent geocodes, with the exception of the original three-digit postcode if, according to current publicly available data from the Census Bureau (1), geographic units formed by combining all postcodes with the same three original figures contain more than 20,000 people; and (2) the initial three postcode figures for all such geographic units containing 20,000 or less are changed by 000; (c) All dated elements (except the year) for dates directly related to that person, including date of birth, date of admission, date of discharge, date of death; and all ages over 89 and all dated elements (including a year) indicating such age, except that such ages and elements may be aggregated into one category at age 90 and over; (D) phone numbers; (E) fax numbers; (F) Email addresses: (G) Social Security numbers; (H) Medical Records; The number of beneficiaries of the health insurance plan; (J) Account numbers; (K) Certificates/license numbers; (L) vehicle identifiers and serial numbers, including license plates; (M) device identifiers and serial numbers; Web universal resource locators (URLs); (O) Internet Protocol Address Numbers (IP); (P) biometric identifiers, including fingerprints and voices; (B) Full face photographic images and any comparable images; and ® and any other unique identification number, characteristic or code, except where it is permitted for re-identification purposes, subject to certain conditions. In addition to removing the above identifiers, the organization covered may not have any actual knowledge that the remaining information can be used alone or in conjunction with any other information to identify the person who applied for that information. 45 K.F.R. No 164.514 (b). 16 45 C.F.R. No 164.502 (a). 17 45 C.F.R. No 164.502 (a)(2). 18 45 C.F.R. No 164.502 (a)(1). 19 45 C.F.R. No 164.506 (c). 20 45 C.F.R. No 164.501. 21 45 C.F.R. No 164.501. 22 45 C.F.R. No 164.501. 23 45 C.F.R. No 164.508(a)(2) 24 45 C.F.R. No 164.506 (b). 25 45 C.F.R. No 164.510 (a). 26 45 K.F.R. No 164.510 (b). 27 45 C.F.R. No 164.502(a)(1)(iii). 28 See 45 C.F.R. No 164.512. 29 45 C.F.R. No 164.512(a). 30 45 C.F.R. No 164.512 (b). 31 45 C.F.R. No 164.512(a), (c). 32 45 C.F.R. No 164.512 (d). 33 45 C.F.R. No (e). 34 45 C.F.R. No 164.512 (f). 35 45 C.F.R. No 164,512 (g). 36 45 C.F.R. No 164.512(h). 37 Правило конфиденциальности определяет исследования как систематическое расследование, включая научно-исследовательские разработки, разработки, and assessments designed to develop or promote generalized knowledge. 45 K.F.R. No 164.501. 38 45 C.F.R. No 164.512(i). 39 45 CFR No 164.514 (e). 40 45 C.F.R. No 164.512 (j). 41 45 C.F.R. No 164.512 (k). 42 45 K.F.R. No 164.512 (l). 43 45 C.F.R. No 164.514 (e). A limited data set is protected by medical information that excludes the following direct identifiers or relatives, employers or family members of an individual: (i) Names; (ii) Information about the postal address, beyond the city or city, state and postcode; Phone numbers; (iv) Fax numbers; (v) Email addresses: vi) Social Security numbers; (vii) Medical records numbers; Number of beneficiaries of the health insurance plan; Accounts numbers; Certificate/license numbers; vehicle identifiers and serial numbers, including license plates; device identifiers and serial numbers; (xiii) web-universal resource locators (URLs); 14) Internet Protocol Address Numbers (IP); (xv) biometric identifiers, including fingerprints and voices; (xvi) Full face photographic images and any comparable images. 45 K.F.R. No 164.514 (e)(2). 44 45 C.F.R. No 164.508. 45 The organization covered may determine the provision of medical care solely to obtain protected medical information for disclosure to a third party by giving permission to disclose information to a third party. For example, a doctor covered by insurance may be trained to provide the issuer with a physical certificate of life insurance to allow an individual to disclose the results of the survey to the life insurance issuer. A health insurance plan may determine the eligibility for individual authorization requested prior to enrollment (except for psychotherapeutic notes) to determine human rights or enrollment, or for underwriting or risk rating. A covered health care provider may provide treatment related to research (e.g. clinical trials) on a person who gives permission to use or disclose a person's protected medical information for the study. 45 C.F.R. 508 (b)(4). 46 45 CFR No 164.532. 47 Psychotherapeutic notes mean notes recorded (in any environment) by a doctor who is a mental health specialist documenting or analyzing the content of the conversation during a private counseling session or group, joint or family counseling session and which are separated from the rest of the person's medical record. Psychotherapeutic notes exclude prescription medications and monitoring, counseling sessions start and stop times, modalities and frequency of treatment furnished, clinical test results, and any summary of the following items: diagnosis, functional condition, treatment plan, symptoms, prognosis, and progress on день. 45 К.Ф.Р. No 164,501. 48 45 C.F.R. No 164,508 (a)(2). 49 45 C.F.R. No 164,501 и 164,508 (a)(3). 50 45 C.F.R. No 164.502 (b) и и (d). 51 45 C.F.R. No. 164.520 (a) and (b). A group health insurance plan, or health insurer or HMO for a group health plan that intends to disclose protected health information (including enrollment data or summary health information) to the plan's sponsor, should be informed in the notice. Special applications are also required in the notice if the organization is intended to contact individuals about health benefits or services, alternatives to treatment or appointment reminders, or to raise funds for the affected organization. 52 45 C.F.R. No 164.520 (c). 53 45 C.F.R. No 164.520 (d). 54 45 C.F.R. No 164.520 (c). 55 45 C.F.R. No 164.524. 56 45 C.F.R. No 164.501. 57 The organization covered may deny the person access, provided that the person is entitled to such a waiver, considered by a licensed health professional (who is designated as a substitute organization and who was not involved in the initial waiver decision), when a licensed health professional has determined, in the exercise of professional judgment, that (a) requested access may endanger the life or physical safety of an individual or another person; (b) Protected medical information mentions another person (unless the other person is not a health care provider) and the requested access may cause significant damage to that other person; or (c) The request for access is made by the person's personal representative, and the granting of access to such a personal representative may well cause substantial harm to the person or another person. The organization covered may deny access to individuals without giving a person the opportunity to consider the following protected situations: (a) protected health information falls under the right of access; (b) A prisoner's request for protected medical information in certain circumstances; (c) The information that the provider generates or receives from the research, including treatment for which the person has agreed not to have access to consent to participate in the study (as long as access to information is restored at the end of the study); (d) For records subject to the Privacy Act, information that may be denied under the Privacy Act, 5 U.S.C. No. 552a; and (e) information obtained in accordance with the promise of confidentiality from a source other than the health care provider, if the provision of access is likely to reveal the source. 45 K.F.R. No 164.524. 58 45 C.F.R. No 164.526. 59 Covered organizations may refuse a person's request for amendments only under certain circumstances. The organization covered may refuse a request if it can exclude information from an individual's access; (b) did not create information (unless does not provide reasonable grounds to believe that the creator is no longer available); (c) Determines that the information is accurate and complete; or (d) doesn't hold holds in the set record. 164.526 (a)(2). 60 45 C.F.R. No 164.528. 61 45 C.F.R. No 164.522(a). 62 45 C.F.R. No 164.522(a). In addition, the restriction agreed upon by the organization does not apply in accordance with this subdi promoted to prevent the use or disclosure of information permitted or required under No. 164.502 (a) (2) (ii), 164.510 (a) or 164.512. 63 45 C.F.R. No 164.522 (b). 64 45 C.F.R. No 164.530 (i). 65 45 C.F.R. No 164.530(a). 66 45 C.F.R. 160.103. 67 45 C.F.R. No 164.530 (b). 68 45 C.F.R. No 164.530 (e). 69 45 C.F.R. No 164.530 (f). 70 45 C.F.R. No 164.530 (c). 71 45 C.F.R. No 164.530 (d). 72 45 C.F.R. No 164.520 (b)(1)(vi). 73 45 C.F.R. No 164.530 (g). 74 45 K.F.R. No. 164.530 (h). 75 45 C.F.R. No 164.530 (j). 76 45 C.F.R. No 164.530 (k). 77 45 C.F.R. No 164.103, 164.105. 78 45 C.F.R. No 164.103. 79 45 C.F.R. No164.105. Common ownership exists if a legal entity owns a property or a share of five per cent or more in another organization; general control exists if an entity has direct or indirect power to significantly influence or direct the actions or policies of another organization. 45 K.F.R. No 164.103. 80 Privacy Rule at 45 C.F.R. No. 160.103 defines five types of organized health care mechanisms: a clinically integrated environment in which people typically receive medical care from more than one health care provider. An organized health system in which participating organizations conduct a collaborative process and work together to review the use, quality assessment and improvement of risk-sharing activities or activities. A group health insurance plan and a health insurer or HMO that insures the benefits of the plan with respect to protected medical information created or received by an insurer or HMO that relates to individuals who are or have been participants or beneficiaries of a group health plan. All group health plans supported by the same plan sponsor. All group health plans supported by the same plan sponsor, as well as all health insurers and GMOs that insure the benefits of the plans, with respect to protected medical information created or received by insurers or GMOs that relates to individuals who are or have been participants or beneficiaries of group health plans. 81 45 C.F.R. No 164.506 (c)(5). 82 45 K.F.R. No. 164.504 (d). 83 45 C.F.R. No 164.504 (f). 84 45 C.F.R. 164.502 (g). 85 45 C.F.R. No160.203. 86 45 C.F.R. No 160.202. 87 45 C.F.R. 160.304 88 Pub. L. 104-191; 42 U.S.C. No1320d-5. 89 Pub L. 104-191; 42 U.S.C. No1320d-6. 90 45 C.F.R. No 164.534. 91 45 C.F.R. No 160.103. 92 Fully insured health insurance plans must use the total amount of insurance premiums they paid for health insurance benefits during the last fiscal year plan. Self-insured plans, both funded and not funded, must use the total amount paid for the medical claims of an employer, plan sponsor or charitable foundation, depending on the circumstances, on behalf of the plan during the last full fiscal year of the plan. Plans that provide health benefits through a combination of purchased purchases and self-insurance should combine power of attorney to determine their total annual revenues. Content created by the Office of Civil Rights (OCR) Content was last reviewed on July 26, 2013.