(iv) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Institutional (837), May 2006, ASC X12N/005010X223, and Type 1 Errata to Health Care Claim: Institutional (837), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, October 2007, ASC X12N/005010X223A1. (Incorporated by reference in §162.920.)

(c) For the period on and after January 1, 2012, the standards identified in paragraph (b)(2) of this section.

(d) For the period on and after September 21, 2020, the Quantity Prescribed (460–ET) field, as set forth in the Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2007 and equivalent Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), National Council for Prescription Drug Programs, must be treated as required where the transmission meets both of the following:

(1) Is for a Schedule II drug, as defined in 21 CFR 1308.12.

(2) Uses the standard identified in paragraph (b)(2)(i) of this section.

[68 FR 8399, Feb. 20, 2003, as amended at 74 FR 3327, Jan. 16, 2009; 85 FR 4242, Jan. 24, 2020]

Subpart S—Medicaid Pharmacy Subrogation

SOURCE: 74 FR 3328, Jan. 16, 2009, unless otherwise noted.

§162.1901 Medicaid pharmacy subrogation transaction.

The Medicaid pharmacy subrogation transaction is the transmission of a claim from a Medicaid agency to a payer for the purpose of seeking reimbursement from the responsible health plan for a pharmacy claim the State has paid on behalf of a Medicaid recipient.

§162.1902 Standard for Medicaid pharmacy subrogation transaction.

The Secretary adopts the Batch Standard Medicaid Subrogation Implementation Guide, Version 3, Release 0 (Version 3.0), July 2007, National Council for Prescription Drug Programs, as referenced in §162.1902 (Incorporated by reference at §162.920):

(a) For the period on and after January 1, 2012, for covered entities that are not small health plans;

(b) For the period on and after January 1, 2013 for small health plans.

PART 163 [RESERVED]

PART 164—SECURITY AND PRIVACY

Subpart A—General Provisions

Sec.
164.102 Statutory basis.
164.103 Definitions.
164.104 Applicability.
164.105 Organizational requirements.
164.106 Relationship to other parts.

Subpart B [Reserved]

Subpart C—Security Standards for the Protection of Electronic Protected Health Information

164.302 Applicability.
164.304 Definitions.
164.306 Security standards: General rules.
164.308 Administrative safeguards.
164.310 Physical safeguards.
164.312 Technical safeguards.
164.314 Organizational requirements.
164.316 Policies and procedures and documentation requirements.
164.318 Compliance dates for the initial implementation of the security standards.
APPENDIX A TO SUBPART C OF PART 164—SECURITY STANDARDS: MATRIX

Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information

164.400 Applicability.
164.402 Definitions.
164.404 Notification to individuals.
164.406 Notification to the media.
164.408 Notification to the Secretary.
164.410 Notification by a business associate.
164.412 Law enforcement delay.
164.414 Administrative requirements and burden of proof.

Subpart E—Privacy of Individually Identifiable Health Information

164.500 Applicability.
164.501 Definitions.
164.502 Uses and disclosures of protected health information: General rules.
164.504 Uses and disclosures: Organizational requirements.
164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

(iv) 电子数据交换ASC X12标准技术报告第3类--医疗保健索赔：机构(837),2006年5月，ASC X12N/005010X223，以及医疗保健索赔：机构(837)第1类勘误表，电子数据交换ASC X12标准技术报告第3类，2007年10月，ASC X12N/005010X223A1。(通过引用并入162.920。)

(c) 对于2012年1月1日及之后的期间，本节第(b)(2)段所确定的标准。

(d) 对于2020年9月21日及之后的期间，凡传输同时满足以下两项条件时，必须将《电信标准实施指南》D版第0次发布(D.0版，2007年8月)及等效的《批量标准实施指南》第1版第2次发布(1.2版，国家处方药计划委员会)中规定的处方数量(460-ET)字段视为必填：

(1)是针对21 CFR 1308.12中定义的附表II药物。

(1)使用本节第(b)(2)(i)段所确定的标准。

[68 FR 8399,2003年2月20日，经74 FR 3327,2009年1月16日；85 FR 4242,2020年1月24日修订]

S子部分--医疗补助药房代位求偿

来源：74 FR 3328,2009年1月16日，除非另有说明。

162.1901 医疗补助药房子废止交易。

Medicaid药房代位求偿交易是指从Medicaid机构向付款方传输索赔，目的是就州代表Medicaid受益人已支付的药房索赔向责任健康计划寻求报销。

162.1902 医疗补助药品标准梅西代位交易。

部长采纳《批量标准Medicaid代位求偿实施指南》第3版第0版(3.0版),2007年7月，国家处方药计划委员会，如162.920):

(a) 对于2012年1月1日及之后的期间，适用于非小型健康计划的受保护实体；

(b) 对于小型健康计划，自2013年1月1日起(含当日)的期间。

第163部分[保留]

第164部分--安全与隐私

A子部分--一般规定

第
164.102 法定依据。
164.103 定义。
164.104 适用性。
164.105 组织要求。
164.106 与其他部分的关系。

B 子部分[保留]

C 子部分--保护电子受保护健康信息的保护

164.302 适用性。
164.304 定义。
164.306 安全标准：一般规则。
164.308 管理保障措施。
164.310 物理防护措施。
164.312 技术保障措施。
164.314 组织要求。
政策和程序及文档要求。
164.316
安全标准初始实施的合规日期。
164.318
附录 A 至第 164 部分 C 子部分--S E -
安全标准：矩阵

D子部分--发生以下情形时的通知未受保护的健康信息泄露

164.400 适用性。
164.402 定义。
164.404 通知个人。
164.406 通知媒体。
164.408 通知部长。
164.410 业务伙伴的通知。
164.412 执法延迟。
行政要求与举证责任。
164.414

E分部分--个人可识别健康信息的隐私

164.500 适用性。
164.501 定义。
受保护健康信息的使用与披露：一般规则。
164.502
使用与披露：组织要求。
164.504
为实施治疗、付款或医疗保健运营而进行的使用和披露。
164.506

本译本由机器翻译生成，供快速理解条文与内部培训使用；
涉及合规判断或法律适用时，请咨询专业顾问，并以官方英文文本为准。
翻译您自己的文件，请选择桐鸾译馆 · https://www.ivyivy.com.cn
扫码关注服务号

164.508 Uses and disclosures for which an authorization is required.
164.509 Uses and disclosures for which an attestation is required.
164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.
164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.
164.514 Other requirements relating to uses and disclosures of protected health information.
164.520 Notice of privacy practices for protected health information.
164.522 Rights to request privacy protection for protected health information.
164.524 Access of individuals to protected health information.
164.526 Amendment of protected health information.
164.528 Accounting of disclosures of protected health information.
164.530 Administrative requirements.
164.532 Transition provisions.
164.534 Compliance dates for initial implementation of the privacy standards.
164.535 Severability.

AUTHORITY: 42 U.S.C. 1302(a); 42 U.S.C. 1320d–1320d–9; sec. 264, Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2(note)); and secs. 13400–13424, Pub. L. 111–5, 123 Stat. 258–279.

SOURCE: 65 FR 82802, Dec. 28, 2000, unless otherwise noted.

Subpart A—General Provisions

§ 164.102 Statutory basis.

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act, section 264 of Public Law 104–191, and sections 13400–13424 of Public Law 111–5.

[78 FR 5692, Jan. 25, 2013]

§ 164.103 Definitions.

As used in this part, the following terms have the following meanings:

Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with §164.105(a)(2)(iii)(D).

Hybrid entity means a single legal entity:

(1) That is a covered entity;

(2) Whose business activities include both covered and non-covered functions; and

(3) That designates health care components in accordance with paragraph §164.105(a)(2)(iii)(D).

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Plan sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

Required by law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

[68 FR 8374, Feb. 20, 2003, as amended at 74 FR 42767, Aug. 24, 2009; 78 FR 34266, June 7, 2013]

164.508 需要授权的使用和披露。
164.509 需要证明的使用与披露。
164.510 需要个人有机会同意或反对的使用和披露。
164.512 不需要授权或同意或反对机会的使用和披露。
164.514 关于受保护健康信息的使用和披露的其他要求。
164.520 受保护健康信息隐私实践通知。
164.522 请求对受保护健康信息进行隐私保护的权利。
164.524 个人获取受保护健康信息。
164.526 受保护健康信息的修正。
164.528 受保护健康信息披露的 Accounting。
164.530 行政要求。
164.532 过渡条款。
164.534 隐私标准初始实施的合规日期。
164.535 可分割性。

授权依据：42 U.S.C. 1302(a)；42 U.S.C. 1320d–1320d–9；第264条，Pub. L. 104–191，110 Stat. 2033–2034（42 U.S.C. 1320d–2（注释））；以及第13400–13424条，Pub. L. 111–5，123 Stat. 258–279。

来源：65 FR 82802,2000年12月28日，除非另有说明。

A子部分--一般规定

164.102 法定依据。

本部分的规定依据部长根据该法案第十一编C部分、公法104-191第264条以及公法111-5第13400-13424条制定标准、要求和实施规范的权力而通过。

[78 FR 5692,2013年1月25日]

164.103 定义。

在本部分中，下列术语具有以下含义：

共同控制存在于一实体拥有直接或间接重大影响或指导另一实体行动或政策的权力时。

共同所有权存在于一实体或各实体拥有另一实体5%或以上所有权或股权权益时。

受保护功能指受保护实体履行以下职能的功能--

其履行使该实体成为健康计划、医疗保健提供者或医疗保健信息交换中心。

医疗保健组成部分指混合实体根据164.105(a)(2)(iii)(D)指定的混合实体的一个组成部分或多个组成部分的组合。

混合实体指单一法律实体：

(1) 这是一个受保护实体；

(2)其业务活动同时包括受保护和非受保护功能；以及

(3)根据164.105(a)(2)(iii)(D)指定医疗保健组成部分。

执法官员指美国、州、领地、州或领地的政治分区或印第安部落的任何机构或当局的官员或雇员，其依法被授权：

(1)调查或对潜在违法行为进行正式调查；或

(2)起诉或以其他方式进行因涉嫌违法而产生的刑事、民事或行政诉讼。

计划发起人按ERISA第3(16)(B)节、29 U.S.C.1002(16)(B)的定义界定。法律要求是指载于法律中的强制性规定，迫使实体使用或披露受保护健康信息，并可在法院强制执行。法律要求包括但不限于：法院命令和法院签发的令状；由法院、大陪审团、政府或部落监察长、或有权要求提供信息的行政机构签发的传票或传唤令；民事或经授权的调查要求；针对参与该计划的医疗保健提供者的Medicare参与条件；以及要求提供信息的法规或规章，包括在根据提供公共福利的政府计划寻求付款时要求提供此类信息的法规或规章。

[68 FR 8374,2003年2月20日，经74 FR 42767,2009年8月24日；78 FR 34266,2013年6月7日修订]

§ 164.104 Applicability.

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this part apply to the following entities:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) Where provided, the standards, requirements, and implementation specifications adopted under this part apply to a business associate.

[68 FR 8375, Feb. 20, 2003, as amended at 78 FR 5692, Jan. 25, 2013]

§ 164.105 Organizational requirements.

(a)(1) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of this part, other than the requirements of this section, §§ 164.314, and 164.504, apply only to the health care component(s) of the entity, as specified in this section.

(2) *Implementation specifications:*

(i) *Application of other provisions.* In applying a provision of this part, other than the requirements of this section, §§ 164.314, and 164.504, to a hybrid entity:

(A) A reference in such provision to a ''covered entity'' refers to a health care component of the covered entity;

(B) A reference in such provision to a ''health plan,'' ''covered health care provider,'' or ''health care clearinghouse,'' refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable;

(C) A reference in such provision to ''protected health information'' refers to protected health information that is created or received by or on behalf of the health care component of the covered entity; and

(D) A reference in such provision to ''electronic protected health information'' refers to electronic protected health information that is created, received, maintained, or transmitted by or on behalf of the health care component of the covered entity.

(ii) *Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this part. In particular, and without limiting this requirement, such covered entity must ensure that:

(A) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which subpart E of this part would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities;

(C) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by subpart E of this part.

(iii) *Responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities:

(A) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility of complying with this part.

(B) The covered entity is responsible for complying with §§ 164.316(a) and 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section.

(C) The covered entity is responsible for complying with §§ 164.314 and 164.504

164.104 适用性。

(a) 除另有规定外，本部分通过的标准、要求和实施规范适用于以下实体：

(1) 一项健康计划。

(2) 一家医疗保健清算机构。

(3)传输与本子章所涵盖交易相关的任何电子形式健康信息的医疗保健提供者。

(b) 在有所规定的情况下，本部分通过的标准、要求和实施规范适用于业务伙伴。

[68 FR 8375,2003年2月20日，经78 FR 5692,2013年1月25日修订]

164.105 组织要求。

(1) 标准：医疗保健组成部分。

(a)

如果受保护实体是混合实体，则本部分的要求(本节、164.314和164.504的要求除外)仅适用于该实体的医疗保健组成部分，如本节所规定。

(2)实施规范：(i) 其他条款的适用。在将本部分的规定(本节要求、 164.314和164.504除外)适用于混合实体时：

(A) 此类条款中对"受保护实体"指受保护实体的医疗保健组成部分；

(B) 此类条款中对"健康计划"、"受保护医疗保健提供者"或"医疗保健信息交换中心"是指受保护实体的医疗保健组成部分，如果该医疗保健组成部分履行健康计划、医疗保健提供者或医疗保健信息交换中心(视情况而定)的功能；

(C) 此类条款中对.....的引用"受保护健康信息"是指由受保护实体的医疗保健组成部分或代表其创建或接收的受保护健康信息；以及

(D) 此类条款中对.....的引用"电子受保护健康信息"是指由受保护实体的医疗保健组成部分或代表其创建、接收、维护或传输的电子受保护健康信息。

(ii) 保障要求。作为混合实体的受保护实体必须确保该实体的医疗保健组成部分遵守本部分的适用要求。特别是，在不限制此要求的情况下，该受保护实体必须确保：

(A) 其医疗保健组成部分不向受保护实体的另一组成部分披露受保护健康信息，若在医疗保健组成部分和另一组成部分为独立且不同的法律实体的情况下，本部分E子部分将禁止此类披露；

(B) 其医疗保健组成部分就受保护实体的另一组成部分保护电子受保护健康信息，其保护程度与在医疗保健组成部分和另一组成部分为独立且不同的法律实体的情况下本部分C子部分要求保护此类信息的程度相同；

(C) 如果一人同时以该组成部分工作人员的身份为医疗保健组成部分履行职务，并以相同身份就该实体的另一组成部分为该另一组成部分履行职务，则该工作人员不得以本部分E子部分禁止的方式使用或披露在其为医疗保健组成部分工作过程中或附带产生的受保护健康信息。

(iii) 受保护实体的责任。作为混合实体的受保护实体负有以下责任：

(A) 就本子章第160部分C子部分(涉及合规与执法)而言，受保护实体负有遵守本部分的责任。

(B) 受保护实体负责遵守 164.316(a)和164.530(i)，涉及实施政策和程序以确保遵守本部分的适用要求，包括第[段]中的保障要求

(a) (2) (ii) 本节。

(C) 受保护实体负责遵守 164.314 和 164.504

regarding business associate arrangements and other organizational requirements.

(D) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation in accordance with paragraph (c) of this section, provided that, if the covered entity designates one or more health care components, it must include any component that would meet the definition of a covered entity or business associate if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs covered functions.

(b)(1) *Standard: Affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this part.

(2) *Implementation specifications*—(i) *Requirements for designation of an affiliated covered entity.* (A) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this part, if all of the covered entities designated are under common ownership or control.

(B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section.

(ii) *Safeguard requirements.* An affiliated covered entity must ensure that it complies with the applicable requirements of this part, including, if the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, §§ 164.308(a)(4)(ii)(A) and 164.504(g), as applicable.

(c)(1) *Standard: Documentation.* A covered entity must maintain a written or electronic record of a designation as required by paragraphs (a) or (b) of this section.

(2) *Implementation specification: Retention period.* A covered entity must retain the documentation as required by paragraph (c)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

[68 FR 8375, Feb. 20, 2003, as amended at 78 FR 5692, Jan. 25, 2013]

§ 164.106 Relationship to other parts.

In complying with the requirements of this part, covered entities and, where provided, business associates, are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

[78 FR 5693, Jan. 25, 2013]

Subpart B [Reserved]

Subpart C—Security Standards for the Protection of Electronic Protected Health Information

AUTHORITY: 42 U.S.C. 1320d–2 and 1320d–4; sec. 13401, Pub. L. 111–5, 123 Stat. 260.

SOURCE: 68 FR 8376, Feb. 20, 2003, unless otherwise noted.

§ 164.302 Applicability.

A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.

[78 FR 5693, Jan. 25, 2013]

§ 164.304 Definitions.

As used in this subpart, the following terms have the following meanings:

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to ''access'' as used in this subpart, not as used in subparts D or E of this part.)

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

Authentication means the corroboration that a person is the one claimed.

关于业务伙伴安排和其他组织要求。

(D) 受保护实体负责指定属于该受保护实体一个或多个医疗保健组成部分的组件，并依照本节(c)段记录该指定，但前提是，如果受保护实体指定一个或多个医疗保健组成部分，则必须包括任何若作为独立法律实体即符合受保护实体或业务伙伴定义的组件。医疗保健组成部分也可仅在该组件执行受保护功能的范围内包括该组件。

(b)(1) 标准：关联受保护实体。具有关联关系的法律上独立的受保护实体可为实施本部分之目的将其自身指定为单一受保护实体。

(2) 实施规范--(i) 关联受保护实体指定要求。(A)法律上独立的受保护实体可为实施本部分之目的将其自身(包括该受保护实体的任何医疗保健组成部分)指定为单一关联受保护实体，前提是所有被指定的受保护实体处于共同所有权或控制之下。

(B) 关联受保护实体的指定必须记录在案，且该记录须按本节第(c)段的要求保存。

(ii) 保障要求。关联受保护实体必须确保其遵守本部分的适用要求，包括(如果关联受保护实体合并了健康计划、医疗保健提供者或医疗保健信息交换中心的功能) 164.308(a)(4)(ii)(A)和164.504(g)(如适用)。

(c)(1) 标准：文档记录。受保护实体必须按本节第(a)或(b)段的要求保存指定的书面或电子记录。

(2) 实施规范：保留期限。受保护实体必须按本节第(c)(1)段的要求，自文件创建之日起保留该文件6年，或最后生效的日期，以较晚者为准。

[68 FR 8375,2003年2月20日，经78 FR 5692,2013年1月25日修订]

164.106 与其他部分的关系。

在遵守本部分要求时，受保护实体以及(在适用情况下)业务伙伴须遵守本子章第160部分和第162部分的适用条款。

[78 FR 5693,2013年1月25日]

B 子部分[保留]

C 子部分--安全标准，适用于电子受保护健康信息的保护

授权依据：42 U.S.C.1320d-2和1320d-4；第13401条，Pub.L.111-5,123 Stat.260。

来源：68 FR 8376,2003年2月20日，除非另有说明。

164.302 适用性。

受保护实体或业务伙伴必须就受保护实体的电子受保护健康信息遵守本子部分的适用标准、实施规范和要求。

[78 FR 5693,2013年1月25日]

164.304 定义。

在本子部分中，下列术语具有以下含义：访问是指读取、写入、修改或传输数据/信息或以其他方式使用任何系统资源的能力或必要手段。(本定义适用于本子部分中使用的"访问"，不适用于本部分D或E子部分中使用的"访问"。)行政保障措施是指为管理安全措施的选择、开发、实施和维护以保护电子受保护健康信息，以及管理受保护实体或业务伙伴的工作人员在保护该信息方面的行为而采取的行政行动、政策和程序。身份验证是指证实某人确为其所声称之人。

Availability means the property that data or information is accessible and useable upon demand by an authorized person.

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Facility means the physical premises and the interior and exterior of a building(s).

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.

Malicious software means software, for example, a virus, designed to damage or disrupt a system.

Password means confidential authentication information composed of a string of characters.

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Security or Security measures encompass all of the administrative, physical, and technical safeguards in an information system.

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

User means a person or entity with authorized access.

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

[68 FR 8376, Feb. 20, 2003, as amended at 74 FR 42767, Aug. 24, 2009; 78 FR 5693, Jan. 25, 2013]

§ 164.306 Security standards: General rules.

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

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

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

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

(4) Ensure compliance with this subpart by its workforce.

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

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

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

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

(iii) The costs of security measures.

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

(c) *Standards.* A covered entity or business associate must comply with the applicable standards as provided in this section and in §§164.308, 164.310, 164.312, 164.314 and 164.316 with respect

可用性指数据或信息可应授权人员的要求被访问和使用的属性。

保密性指数据或信息不被提供给或披露给未经授权的人员或过程的属性。

加密指使用算法过程将数据转换为一种形式，在该形式下，若不使用保密过程或密钥，赋予其含义的可能性很低。

设施是指建筑物的物理场所及建筑物内外。

信息系统指处于同一直接管理控制下、共享共同功能的一组相互连接的信息资源。系统通常包括硬件、软件、信息、数据、应用程序、通信和人员。

完整性指数据或信息未以未经授权的方式被更改或销毁的属性。

恶意软件指旨在损坏或破坏系统的软件，例如病毒。

密码指由一串字符组成的保密身份验证信息。

物理保障措施指保护受保护实体或业务伙伴的电子信息系统及相关建筑物和设备免受自然和环境危害及未经授权侵入的物理措施、政策和程序。

安全或安全措施涵盖信息系统中的所有管理、物理和技术保障措施。

安全事件指在信息系统中对信息的未经授权的访问、使用、披露、修改或销毁，或对系统运行的干扰，无论未遂或已遂。

技术保障措施指保护电子受保护健康信息并控制对其访问的技术及其使用的政策和程序。

用户指获授权访问的人员或实体。

工作站指电子计算设备，例如笔记本电脑或台式计算机，或执行类似功能的任何其他设备，以及存储在其直接环境中的电子介质。

[68 FR 8376,2003年2月20日，经74 FR 42767,2009年8月24日；78 FR 5693,2013年1月25日修订]

164.306 安全标准：一般规则

规则。

(a) 一般要求。受保护实体和业务伙伴必须执行以下事项：

(1) 确保受保护实体或业务伙伴创建、接收、维护或传输的所有电子受保护健康信息的保密性、完整性和可用性。

(2) 防范对此类信息的安全性或完整性的任何合理预期的威胁或危害。

(3) 防范对本部分子部分E未允许或未要求的此类信息的任何合理预期的使用或披露。

(4) 确保其工作人员遵守本子部分。

(b) 方法的灵活性。(1) 受保护实体和业务伙伴可使用任何使其能够合理且适当地实施本子部分规定的标准和实施规范的安全措施。

(2) 在决定使用哪些安全措施时，受保护实体或业务伙伴必须考虑以下因素：

(i) 受保护实体或业务伙伴的规模、复杂性和能力。

(ii) 受保护实体或业务伙伴的技术基础设施、硬件和软件安全能力。

(iii) 安全措施的成本。

(iv) 对电子受保护健康信息的潜在风险的概率和严重性。

(c) 标准。受保护实体或业务伙伴必须遵守本节以及164.308、164.310、164.312、164.314 和 164.316 中规定的适用标准，涉及

to all electronic protected health information.

(d) *Implementation specifications.* In this subpart:

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

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

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

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and

(ii) As applicable to the covered entity or business associate—

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate—

$(*1*) Document why it would not be reasonable and appropriate to implement the implementation specification; and

$(*2*) Implement an equivalent alternative measure if reasonable and appropriate.

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

[68 FR 8376, Feb. 20, 2003; 68 FR 17153, Apr. 8, 2003; 78 FR 5693, Jan. 25, 2013]

§ 164.308 Administrative safeguards.

(a) A covered entity or business associate must, in accordance with §164.306:

(1)(i) *Standard: Security management process.* Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) *Implementation specifications:*

(A) *Risk analysis (Required).* Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

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

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

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

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

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

(ii) *Implementation specifications:*

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

适用于所有电子受保护健康信息。

(d) 实施规范。在本子部分中：

(1) 实施规范分为必需或可寻址。如果某项实施规范为必需，则在该实施规范标题后的括号中出现“Required”一词。如果某项实施规范为可寻址，则在该实施规范标题后的括号中出现“addressable”一词。

(2) 当 164.310、 164.314或164.316中采用的标准包含必需的实施规范时，受保护实体或业务伙伴必须实施这些实施规范。

(3) 当 164.310、 164.314或164.316中采用的标准包含可寻址的实施规范时，受保护实体或业务伙伴必须--

(i) 在结合对保护电子受保护健康信息的可能贡献进行分析时，评估每项实施规范在其环境中是否为合理且适当的保障措施；以及

(ii) 视情况适用于受保护实体或业务伙伴--

(A) 如果合理且适当，则实施该实施规范；或

(B) 如果实施该实施规范不合理或不适当--

$(1) 记录为何实施该实施规范不合理且不适当；以及 $(2) 如果合理且适当，则实施等效的替代措施。

(e) 维护。受保护实体或业务伙伴必须审查并修改根据本子部分实施的安全措施，以确保持续提供对电子受保护健康信息的合理且适当的保护，并根据164.316(b)(2)(iii)更新此类安全措施的文档。

[68 FR 8376，2003年2月20日；68 FR 17153，2003年4月8日；78 FR 5693，2013年1月25日]

164.308 行政保障措施。

(a) 受保护实体或业务伙伴必须根据164.306:

(1)(i) 标准：安全管理流程。实施政策和程序以防止、检测、遏制和纠正安全违规行为。

(ii) 实施规范：

(A) 风险分析*(必需)*。对受保护实体或业务伙伴所持有的电子受保护健康信息的保密性、完整性和可用性所面临的潜在风险和漏洞进行准确且全面的评估。

(B) 风险管理*(必需)*。实施足够的安全措施，将风险和漏洞降低至合理且适当的水平，以符合164.306(a) 的要求。

(C) 制裁政策*(必需)*。对未能遵守受保护实体或业务伙伴安全政策和程序的工作人员实施适当的制裁。

(D) 信息系统活动审查*(必需)*。实施程序以定期审查信息系统活动的记录，例如审计日志、访问报告和安全事件跟踪报告。

(2) 标准：指定安全责任。确定负责制定和实施本子部分所要求的受保护实体或业务伙伴政策和程序的安全官员。

(3)(i) 标准：工作人员安全。实施政策和程序，以确保其工作人员的所有成员按照本节第(a)(4)段的规定对电子受保护健康信息具有适当的访问权限，并防止那些根据本节第(a)(4)段没有访问权限的工作人员成员获得对电子受保护健康信息的访问权限。

(ii) 实施规范：

(A) 授权和/或监督*(可寻址)*。实施程序，以授权和/或监督处理电子受保护健康信息或在可能访问该信息的地点工作的工作人员。

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

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

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

(ii) *Implementation specifications:*

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

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

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

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

(ii) *Implementation specifications.* Implement:

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

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

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

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

(6)(i) *Standard: Security incident procedures.* Implement policies and procedures to address security incidents.

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

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

(ii) *Implementation specifications:*

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

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

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

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

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

(8) *Standard: Evaluation.* Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule

(B) 工作人员审查程序*(*可寻址*)*。实施程序以确定工作人员成员对电子受保护健康信息的访问是适当的。

(C) 终止程序*(*可寻址*)*。实施程序，在工作人员成员的雇佣或其他安排结束时，或按照本节第(a)(3)(ii)(B)段规定的决定要求时，终止对电子受保护健康信息的访问。

(4)(i) 标准：信息访问管理。实施授权访问电子受保护健康信息的政策和程序，这些政策和程序与本部分E子部分的适用要求一致。

(ii) 实施规范：

(A) 隔离医疗保健清算所功能*(*必需*)*。如果医疗保健清算所是较大组织的一部分，清算所必须实施政策和程序，保护清算所的电子受保护健康信息免遭较大组织的未经授权访问。

(B) 访问授权*(*可寻址*)*。
实施授予电子受保护健康信息访问权的政策和程序，例如，通过访问工作站、事务、程序、进程或其他机制。

(C) 访问建立和修改*(*可寻址*)*。实施政策和程序，根据受保护实体或业务伙伴的访问授权政策，建立、记录、审查和修改用户对工作站、事务、程序或流程的访问权。

(5)(i) 标准：意识与培训。为所有工作人员(包括管理层)实施意识与培训计划。

(ii) 实施规范。实施：

(A) 安全提醒*(*可寻址*)*。
定期安全更新。

(B) 防范恶意软件
*(*可寻址*)*。防范、检测和报告恶意软件的程序。

(C) 登录监控*(*可寻址*)*。
监控登录尝试并报告差异的程序。

(D) 密码管理*(*可寻址*)*。创建、更改和保护密码的程序。

(6)(i)标准：安全事件程序。实施处理安全事件的政策和程序。

(ii)实施规范：响应和报告*(*必需*)*。识别并响应可疑或已知的安全事件；在切实可行的范围内减轻受保护实体或业务伙伴已知的安全事件的有害影响；并记录安全事件及其结果。

(7)(i) 标准：应急计划。建立(并根据需要实施)应对紧急情况或其他事件(例如火灾、故意破坏、系统故障和自然灾害)的政策和程序，这些事件会损坏包含电子受保护健康信息的系统。

(ii) 实施规范：

(A) 数据备份计划*(*必需*)*。建立并实施程序，以创建和维护电子受保护健康信息的可检索精确副本。

(B) 灾难恢复计划*(*必需*)*。
制定(并在需要时实施)恢复任何数据丢失的程序。

(C) 紧急模式运行计划
*(*必需*)*。制定(并根据需要实施)程序，使关键业务流程能够在紧急模式下运行期间继续，以保护电子受保护健康信息的安全。

(D) 测试和修订程序
*(*可寻址*)*。实施定期测试和修订应急计划的程序。

(E) 应用和数据关键性分析*(*可寻址*)*。评估特定应用和数据的相对关键性，以支持其他应急计划组件。

(8) 标准：评估。执行定期的技术性和非技术性评估，最初基于本规则下实施的标准

and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

(b)(1) *Business associate contracts and other arrangements.* A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.

(3) *Implementation specifications: Written contract or other arrangement (Required).* Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

§ 164.310 Physical safeguards.

A covered entity or business associate must, in accordance with §164.306:

(a)(1) *Standard: Facility access controls.* Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) *Implementation specifications:*

(i) *Contingency operations (Addressable).* Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) *Facility security plan (Addressable).* Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) *Access control and validation procedures (Addressable).* Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(iv) *Maintenance records (Addressable).* Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) *Standard: Workstation use.* Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

(c) *Standard: Workstation security.* Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

(d)(1) *Standard: Device and media controls.* Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) *Implementation specifications:*

(i) *Disposal (Required).* Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

(ii) *Media re-use (Required).* Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

(iii) *Accountability (Addressable).* Maintain a record of the movements of

以及随后针对影响电子受保护健康信息安全的环境或运营变化，确定受保护实体或业务伙伴的安全政策和程序满足本子部分要求的程度。

在发生紧急情况时，根据灾难恢复计划和紧急模式运行计划访问数据。

(ii)设施安全计划(可寻址)。实施政策和程序，保护设施及其中的设备免遭未经授权的物理访问、篡改和盗窃。

(b)(1) 业务伙伴合同及其他安排。受保护实体仅可在其依照164.314(a)获得令其满意的保证，即业务伙伴将适当保护该信息的情况下，方可允许业务伙伴代表该受保护实体创建、接收、维护或传输电子受保护健康信息。受保护实体无需从作为分包商的业务伙伴处获得此类令其满意的保证。

(iii) 访问控制和验证程序(可寻址)。实施程序，根据人员的角色或职能控制和验证其对设施的访问，包括访客控制，以及对用于测试和修订的软件程序的访问控制。

(iv) 维护记录(可寻址)。
实施政策和程序，记录与安全相关的设施物理组件(例如硬件、墙壁、门和锁)的维修和修改。

(2)业务伙伴仅可在获得满意保证的情况下，允许作为分包商的业务伙伴代表其创建、接收、维护或传输电子受保护健康信息，该保证须符合164.314(a)，即分包商将适当保护该信息。

(b) 标准：工作站使用。实施政策和程序，规定应执行的适当功能、执行这些功能的方式，以及可访问电子受保护健康信息的特定工作站或某类工作站周围环境的物理属性。

(3) 实施规范：书面合同或其他安排(必需)。通过与业务伙伴签订符合164.314(a) 适用要求的书面合同或其他安排，记录本节第(b)(1)或(b)(2)段所要求的满意保证。

(c) 标准：工作站安全。对所有访问电子受保护健康信息的工作站实施物理保护措施，以限制仅授权用户访问。

(d)(1) 标准：设备和介质控制。实施政策和程序，治理包含电子受保护健康信息的硬件和电子介质进出设施的接收和移除，以及这些物品在设施内的移动。

[68 FR 8376,2003年2月20日，经78 FR 5694,2013年1月25日修订]

164.310 物理防护措施。

受保护实体或业务伙伴必须根据164.306 的规定：

(a)(1) 标准：设施访问控制。实施政策和程序，限制对其电子信息系统及存放这些系统的设施的物理访问，同时确保允许经适当授权的访问。

(2) 实施规范：

(i) 处置(必需)。实施政策和程序，处理电子受保护健康信息和/或其存储的硬件或电子介质的最终处置。

(ii) 介质再利用(必需)。实施程序，在电子介质可供再利用之前从电子介质中移除电子受保护健康信息。

(2) 实施规范：(i) 应急操作(可寻址)。建立(并根据需要实施)程序，允许设施访问以支持恢复丢失的

(iii) 问责(可寻址)。
保存以下各项移动的记录：

hardware and electronic media and any person responsible therefore.

(iv) *Data backup and storage (Addressable)*. Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

§ 164.312 Technical safeguards.

A covered entity or business associate must, in accordance with § 164.306:

(a)(1) *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) *Implementation specifications:*

(i) *Unique user identification (Required)*. Assign a unique name and/or number for identifying and tracking user identity.

(ii) *Emergency access procedure (Required)*. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) *Automatic logoff (Addressable)*. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) *Encryption and decryption (Addressable)*. Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) *Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c)(1) *Standard: Integrity*. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) *Implementation specification: Mechanism to authenticate electronic protected health information (Addressable)*. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) *Standard: Person or entity authentication*. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e)(1) *Standard: Transmission security*. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) *Implementation specifications:*

(i) *Integrity controls (Addressable)*. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) *Encryption (Addressable)*. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

§ 164.314 Organizational requirements.

(a)(1) *Standard: Business associate contracts or other arrangements*. The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

(2) *Implementation specifications (Required)*—(i) *Business associate contracts*. The contract must provide that the business associate will—

(A) Comply with the applicable requirements of this subpart;

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

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

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

硬件和电子媒体以及任何负责此事的人员。

(iv) 数据备份和存储(可寻址)。在设备移动之前，根据需要创建电子受保护健康信息的可检索精确副本。

[68 FR 8376,2003年2月20日，经78 FR 5694,2013年1月25日修订]

164.312 技术保障措施。

受保护实体或业务伙伴必须根据164.306 的规定：

(a)(1) 标准：访问控制。对维护电子受保护健康信息的电子信息系统实施技术政策和程序，仅允许已按164.308(a)(4) 规定授予访问权限的人员或软件程序访问。

(2) 实施规范：(i) 唯一用户识别(必需)。分配唯一名称和/或编号以识别和跟踪用户身份。

(ii) 紧急访问程序(必需)。建立(并根据需要实施)在紧急情况下获取必要电子受保护健康信息的程序。

(iii) 自动注销(可寻址)。
实施电子程序，在预定的不活动时间后终止电子会话。

(iv) 加密和解密(可寻址)。实施加密和解密电子受保护健康信息的机制。

(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用电子受保护健康信息的信息系统中的活动。

(c)(1) 标准：完整性。实施政策和程序，保护电子受保护健康信息免遭不当更改或破坏。

(2) 实施规范：验证电子受保护健康信息的机制(可寻址)。实施电子机制以证实电子受保护健康信息未被未经授权地更改或销毁。

(d) 标准：人员或实体认证。实施程序，验证寻求访问电子受保护健康信息的人员或实体确为其声称的身份。

(e) (1) 标准：传输安全。
实施技术安全措施，防止未经授权访问通过电子通信网络传输的电子受保护健康信息。

(2) 实施规范：
(i) 完整性控制(可寻址)。实施安全措施，确保以电子方式传输的电子受保护健康信息在处置之前不会被不当修改而不被发现。

(ii) 加密(可寻址)。实施机制，在认为适当时加密电子受保护健康信息。

[68 FR 8376,2003年2月20日，经78 FR 5694,2013年1月25日修订]

164.314 组织要求。

(a)(1) 标准：业务伙伴合同或其他安排。164.308(b)(3) 所要求的合同或其他安排必须符合本节第(a)(2)(i)、(a)(2)(ii)或(a)(2)(iii)段的要求(视适用情况而定)。

(2) 实施规范(必需)--(i) 业务伙伴合同。合同必须规定业务伙伴将--

(A)遵守本子部分的适用要求；

(B) 依照164.308(b)(2)，确保代表业务伙伴创建、接收、维护或传输电子受保护健康信息的任何分包商，通过签订符合本节的合同或其他安排，同意遵守本子部分的适用要求；以及

(C) 向受保护实体报告其知悉的任何安全事件，包括164.410 所要求的未受保护健康信息泄露。

(ii) 其他安排。如果受保护实体已有符合164.504(e)(3) 要求的其他安排，则其符合本节第(a)(1)段的规定。

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

(b)(1) *Standard: Requirements for group health plans.* Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

(2) *Implementation specifications (Required).* The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

(ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

(iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013; 78 FR 34266, June 7, 2013]

§164.316 Policies and procedures and documentation requirements.

A covered entity or business associate must, in accordance with §164.306:

(a) *Standard: Policies and procedures.* Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

(b)(1) *Standard: Documentation.* (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

(2) *Implementation specifications:*

(i) *Time limit (Required).* Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(ii) *Availability (Required).* Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(iii) *Updates (Required).* Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5695, Jan. 25, 2013]

§164.318 Compliance dates for the initial implementation of the security standards.

(a) *Health plan.* (1) A health plan that is not a small health plan must comply with the applicable requirements of this subpart no later than April 20, 2005.

(2) A small health plan must comply with the applicable requirements of this subpart no later than April 20, 2006.

(iii) 业务伙伴与分包商的合同。本节第(a)(2)(i)和(a)(2)(ii)段的要求适用于164.308(b)(4) 所要求的业务伙伴与分包商之间的合同或其他安排，其适用方式与这些要求适用于受保护实体与业务伙伴之间的合同或其他安排相同。

制定政策和程序以遵守本标准、实施规范或本子部分的其他要求，同时考虑164.306(b)(2)(i)、(ii)、(iii) 和 (iv) 中规定的那些因素。本标准不得被解释为允许或免除违反本子部分任何其他标准、实施规范或其他要求的行为。受保护实体或业务伙伴可随时更改其政策和程序，前提是这些更改已记录在案并按照本子部分实施。

(b)(1) 标准：团体健康计划的要求。除非向计划发起人披露的唯一电子受保护健康信息是依据 164.508授权的，团体健康计划必须确保其计划文件规定计划发起人将合理且适当地保护由计划发起人代表团体健康计划创建、接收、维护或传输的电子受保护健康信息。

(b) (1) 标准：文档记录。(i)
以书面(可为电子)形式维护为遵守本子部分而实施的政策和程序；以及

(ii) 如果本子部分要求对某项行动、活动或评估进行记录，则维护该行动、活动或评估的书面(可以是电子形式)记录。

(2) 实施规范(必需)。团体健康计划的计划文件必须修订，以纳入要求计划发起人--

(i) 实施合理且适当的行政、物理和技术保障措施，以保护其代表团体健康计划创建、接收、维护或传输的电子受保护健康信息的保密性、完整性和可用性；

(2) 实施规范：(i) 时限(必需)。自文档创建之日或最后生效之日(以较晚者为准)起，保留本节第(b)(1)段所要求的文档 6 年。

(ii) 可用性(必需)。使文档可供负责实施该文档所涉程序的人员使用。

(ii) 确保164.504(f)(2)(iii) 所要求的充分分离得到合理且适当的安全措施的支持；

(iii) 更新(必需)。定期审查文档，并根据影响电子受保护健康信息安全的环境或运营变化进行必要更新。

(iii) 确保其向其提供此信息的任何代理人均同意实施合理且适当的安全措施以保护该信息；以及

[68 FR 8376,2003年2月20日，经78 FR 5695,2013年1月25日修订]

(iv) 向团体健康计划报告其知悉的任何安全事件。

164.318 初始合规日期-

[68 FR 8376,2003年2月20日，经78 FR 5694,2013年1月25日；78 FR 34266,2013年6月7日修订]

安全标准的实施。(a) 健康计划。(1) 非小型健康计划的健康计划必须不迟于 4 月 20 日遵守本子部分的适用要求，

164.316 政策和程序及文档要求。

2005.

受保护实体或业务伙伴必须根据164.306 的规定：

(2) 小型健康计划必须不迟于 2006 年 4 月 20 日遵守本子部分的适用要求。

(a) 标准：政策和程序。
实施合理且适当的

(b) *Health care clearinghouse.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 20, 2005.

(c) *Health care provider.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 20, 2005.

APPENDIX A TO SUBPART C OF PART 164—SECURITY STANDARDS: MATRIX

Standards	Sections	Implementation Specifications (R) = Required, (A) = Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information

SOURCE: 74 FR 42767, Aug. 24, 2009, unless otherwise noted.

§ 164.400 Applicability.

The requirements of this subpart shall apply with respect to breaches of protected health information occurring on or after September 23, 2009.

(b) 医疗保健信息交换中心。一项健康医疗信息交换机构须不迟于2005年4月20日遵守本子部分的适用要求。

(c) 医疗服务提供者。受保护的医疗服务提供者必须不迟于2005年4月20日遵守本子部分的适用要求。

附录A至第164部分C子部分--安全标准：矩阵

标准	条款	实施规范(R)= 必需，(A)= 可寻址 可着装
管理保障措施		
安全管理流程	164.308 (a)(1)	风险分析（R） 风险管理 (R) 制裁政策 (R) 信息系统活动审查 (R)
指定的安全责任	164.308 (a)(2)	(R)
工作人员安全	(a)(3)	授权和/或监督（A） 员工审查程序 终止程序 (A)
信息访问管理	164.308 (a)(4)	隔离医疗保健清算所功能(R) 访问授权 (A) 访问权限的建立与修改(A)
安全意识与培训	164.308 (a)(5)	安全提醒（A） 恶意软件防护 (A) 登录监控 (A) 密码管理 (A)
安全事件程序	164.308 (a)(6)	响应和报告（R）
应急计划	(a)(7)	数据备份计划（R） 灾难恢复计划 (R) 紧急模式运行计划 (R) 测试与修订程序 (A) 应用程序与数据关键性分析(A)
评估	164.308 (a)(8)	(R)
业务伙伴合同与 其他安排。	(b)(1)	书面合同或其他安排(R)
物理防护措施		
设施访问控制	164.310 (a)(1)	应急操作（A） 设施安全计划 (A) 访问控制与验证程序(A) 维护记录 (A)
工作站使用	164.310 (b	(R)
工作站安全	(c	
设备和媒体控制	164.310 (d)(1)	处置（R） 介质再利用 (R) 问责 (A) 数据备份与存储 (A)
技术保障措施(见164.312)		
访问控制	164.312 (a)(1)	唯一用户标识（R） 紧急访问程序 (R) 自动注销 (A) 加密与解密 (A)
审计控制	164.312 (b	(R)
完整性	(c)(1)	电子受保护健康信息认证机制(A)
个人或实体认证	164.312 (d	(R)
传输安全	(e)(1)	完整性控制（A） 加密 (A)

D子部分--在未受保护的健康信息泄露事件

来源：74 FR 42767,2009年8月24日，除非另有说明。

164.400 适用性。

本子部分的要求应适用于2009年9月23日或之后发生的受保护健康信息泄露。

§ 164.402 Definitions.

As used in this subpart, the following terms have the following meanings:

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5.

[78 FR 5695, Jan. 25, 2013]

§ 164.404 Notification to individuals.

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

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

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

(c) *Implementation specifications: Content of notification*—(1) *Elements.* The notification required by paragraph (a)

164.402 定义。

在本子部分中，以下术语具有以下含义：

违规指以本部分子部分 E 不允许的方式获取、访问、使用或披露受保护健康信息，从而危及受保护健康信息的安全性或隐私性。

(1) 违规不包括：

(i) 工作人员或根据受保护实体或业务伙伴授权行事的人员对受保护健康信息的任何非故意获取、访问或使用，前提是此类获取、访问或使用是善意且在授权范围内进行的，并且不会导致以本部分子部分 E 不允许的方式进一步使用或披露。

(ii) 有权在受保护实体或业务伙伴处访问受保护健康信息的人员向同一受保护实体或业务伙伴或受保护实体参与的 organized health care arrangement 中另一有权访问受保护健康信息的人员的任何无意披露，且因此类披露而收到的信息不会以本部分子部分 E 不允许的方式进一步使用或披露。

(iii) 受保护实体或业务伙伴善意相信被披露的未经授权人员合理无法保留此类信息的受保护健康信息披露。

(2) 除第款另有规定外

(1) 本定义第M35段所述，以子部分E不允许的方式获取、访问、使用或披露受保护健康信息，即推定为违规，除非受保护实体或业务伙伴(视情况而定)证明，基于至少以下因素的风险评估，受保护健康信息被泄露的可能性很低：

(i) 所涉受保护健康信息的性质和范围，包括标识符类型和重新识别的可能性；

(ii) 使用受保护健康信息或向其作出披露的未经授权人员；

(iii) 受保护健康信息是否实际被获取或查看；以及

(iv) 对受保护健康信息的风险已缓解的程度。

未 *secured* 受保护健康信息指未通过部长根据 Public Law 111-5 第 13402(h)(2) 条发布的指南中指定的技术或方法，使未经授权人员无法使用、无法读取或无法破译的受保护健康信息。

[78 FR 5695,2013年1月25日]

164.404 向个人发出通知。

(a) 标准 -(1) 一般规则。受保护实体在发现未 secured 受保护健康信息违规后，应通知其未 secured 受保护健康信息已因该违规而被访问、获取、使用或披露，或受保护实体合理认为已被访问、获取、使用或披露的每一位个人。

(2) 视为已发现的数据泄露。就本节第(a)(1)段、164.406(a)和164.408(a)而言，数据泄露应自受保护实体首次知悉该泄露之日，或通过行使合理勤勉本应知悉该泄露之日起，视为由受保护实体发现。如果该泄露为受保护实体的工作人员或代理人(根据联邦代理普通法确定)中除实施泄露者以外的任何人员知悉，或通过行使合理勤勉本应知悉，则受保护实体应被视为知悉该泄露。

(b) 实施规范：通知的及时性。除164.412另有规定外，受保护实体应无不当延迟地提供本节(a)段所要求的通知，且在任何情况下不得迟于发现泄露后60个日历日。

(c) 实施规范：通知内容 -(1) 要素。第(a)段所要求的通知

of this section shall include, to the extent possible:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§164.406 Notification to the media.

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

(b) *Implementation specification: Timeliness of notification.* Except as provided

本节应包括以下内容(在尽可能的范围内):

(A) 对所发生情况的简要描述，包括违规日期和发现违规的日期(若已知);

(B) 对违规所涉未 secured 受保护健康信息类型的描述(例如是否涉及全名、社会安全号码、出生日期、家庭住址、账号、诊断、残疾代码或其他类型的信息);

(C) 个人为保护自身免受违规造成的潜在伤害应采取的任何步骤；

(D) 对所涉受保护实体正在采取何种措施调查违规、减轻对个人的伤害并防止任何进一步违规的简要描述；以及

(E) 个人提出问题或了解更多信息的联系程序，应包括免费电话号码、电子邮件地址、网站或邮寄地址。

(2) 平实语言要求。本节第(a)段所要求的通知应以平实语言书写。

(d) 实施规范：个人通知方式。本节(a)段所要求的通知应按以下形式提供：

(1) 书面通知。(i) 通过一等邮件向个人最后已知地址发送书面通知，或若个人同意电子通知且该同意未被撤回，则通过电子邮件发送。通知可在信息可用时通过一次或多次邮寄提供。

(ii) 如果受保护实体知道个人已死亡并拥有该个人近亲属或个人代表(如子部分 E 的164.502(g)(4) 所规定)的地址，则通过头等邮件向该个人的近亲属或个人代表提供书面通知。通知可在信息可用时通过一次或多次邮寄提供。

(2) 替代通知。在联系信息不足或过时，导致

包括根据本节第(d)(1)(i)段向个人发出的书面通知，应提供合理计算以送达该个人的替代通知形式。如果联系信息不足或过时，导致无法根据第(d)(1)(ii)段向个人的近亲或个人代表发出书面通知，则无需提供替代通知。

(i) 在涉及少于10个人的联系信息不充分或过时的情况下，此类替代通知可通过书面通知的替代形式、电话或其他方式提供。

(ii) 在涉及10个或更多个人的联系信息不充分或过时的情况下，此类替代通知应：

(A) 以在相关受保护实体网站主页上显著张贴为期90天的通知的形式，或在受违规影响个人可能居住的地理区域的主要印刷或广播媒体上显著通知的形式；以及

(B) 包含一个至少保持活跃90天的免费电话号码，个人可通过该号码了解其未受保护的受保护健康信息是否可能包含在违规事件中。

(3) 紧急情况下的额外通知。在受保护实体认为因未受保护的受保护健康信息可能即将被滥用而需要紧急处理的任何情况下，受保护实体可在本节第(d)(1)段规定的通知之外，通过电话或其他适当方式向个人提供信息。

164.406 向媒体发出的通知。

(a) 标准。对于涉及某州或管辖区超过500名居民的未受保护受保护健康信息违规事件，受保护实体应按照164.404(a)(2)的规定在发现违规事件后，通知服务于该州或管辖区的主要媒体机构。

(b) 实施规范：通知的及时性。除另有规定外

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

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

[74 FR 42767, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

§ 164.408 Notification to the Secretary.

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

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

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

[74 FR 42767, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

§ 164.410 Notification by a business associate.

(a) *Standard*—(1) *General rule.* A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

(2) *Breaches treated as discovered.* For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).

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

(c) *Implementation specifications: Content of notification.* (1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.

(2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.

[74 FR 42767, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

§ 164.412 Law enforcement delay.

If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:

(a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

(b) If the statement is made orally, document the statement, including the

在164.412中，受保护实体应无不当延迟地提供本节第(a)段所要求的通知，且在任何情况下不得晚于发现违规事件后60个日历日。

(c) 实施规范：通知的内容。本节第(a)段所要求的通知应符合164.404(c)的要求。

[74 FR 42767,2009年8月24日，经78 FR 5695,2013年1月25日修订]

164.408 向部长发出通知。

(a) 标准。受保护实体应按照164.404(a)(2)的规定在发现未受保护受保护健康信息违规事件后，通知部长。

(b) 实施规范：

涉及*500*名或以上个人的违规事件。对于涉及500名或以上个人的未受保护的受保护健康信息违规事件，受保护实体应，除 164.404(a)所要求通知的同时，按照HHS网站指定的方式提供本节第(a)段所要求的通知。

(c) 实施规范：涉及少于*500*名个人的数据泄露。对于涉及少于500名个人的未受保护健康信息泄露，受保护实体应保存此类泄露的日志或其他文件记录，并应在每个日历年结束后的60天内，按照HHS网站规定的方式，就上一日历年发现的数据泄露提供本节第(a)段所要求的通知。

[74 FR 42767,2009年8月24日，经78 FR 5695,2013年1月25日修订]

164.410 业务伙伴的通知-

交往。

(a) 标准-(1) 一般规则。业务伙伴应在发现未受保护受保护健康信息违规事件后，将该违规事件通知受保护实体。

(2) 视为已发现的违规事件。就本节第(a)(1)段而言，违规事件应视为业务伙伴在以下时间已发现业务伙伴首次知悉该泄露之日，或通过行使合理勤勉本应知悉该泄露之日。如果该泄露为业务伙伴的雇员、高级职员或其他代理人(根据联邦代理普通法确定)中除实施泄露者以外的任何人员知悉，或通过行使合理勤勉本应知悉，则业务伙伴应被视为知悉该泄露。

(b) 实施规范：通知的及时性。除164.412另有规定外，业务伙伴应无不当延迟地提供本节第(a)段所要求的通知，且在任何情况下不得晚于发现违规事件后60个日历日。

(c) 实施规范：通知的内容。(1) 本节第(a)段所要求的通知应尽可能包括识别每一名其未受保护的受保护健康信息在违规事件期间已被或业务伙伴合理认为已被访问、获取、使用或披露的个人。

(2)业务伙伴应在根据本节第(a)段要求的通知时或此后信息可用时尽快向受保护实体提供受保护实体根据164.404(c)须包含在向个人发出的通知中的任何其他可用信息。

[74 FR 42767,2009年8月24日，经78 FR 5695,2013年1月25日修订]

164.412 执法延迟。

如果执法官员向受保护实体或业务伙伴声明，本子部分要求的通知、告知或张贴将妨碍刑事调查或损害国家安全，受保护实体或业务伙伴应：

(a) 如果该声明为书面形式并指明了需要延迟的时间，则在该官员指定的时间段内延迟此类通知、告知或张贴；或

(b) 若声明为口头作出，则记录该声明，包括

identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

§ 164.414 Administrative requirements and burden of proof.

(a) *Administrative requirements.* A covered entity is required to comply with the administrative requirements of §164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart.

(b) *Burden of proof.* In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at §164.402.

Subpart E—Privacy of Individually Identifiable Health Information

AUTHORITY: 42 U.S.C. 1320d–2, 1320d–4, and 1320d–9; sec. 264 of Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2 (note)); and secs. 13400–13424, Pub. L. 111–5, 123 Stat. 258–279.

§ 164.500 Applicability.

(a) Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.

(b) Health care clearinghouses must comply with the standards, requirements, and implementation specifications as follows:

(1) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, the clearinghouse must comply with:

(i) Section 164.500 relating to applicability;

(ii) Section 164.501 relating to definitions;

(iii) Section 164.502 relating to uses and disclosures of protected health information, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(iv) Section 164.504 relating to the organizational requirements for covered entities;

(v) Section 164.512 relating to uses and disclosures for which individual authorization or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(vi) Section 164.532 relating to transition requirements; and

(vii) Section 164.534 relating to compliance dates for initial implementation of the privacy standards.

(2) When a health care clearinghouse creates or receives protected health information other than as a business associate of a covered entity, the clearinghouse must comply with all of the standards, requirements, and implementation specifications of this subpart.

(c) Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.

(d) The standards, requirements, and implementation specifications of this subpart do not apply to the Department of Defense or to any other federal agency, or non-governmental organization acting on its behalf, when providing health care to overseas foreign national beneficiaries.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 78 FR 5695, Jan. 25, 2013]

§ 164.501 Definitions.

As used in this subpart, the following terms have the following meanings:

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political

作出声明的官员的身份，并暂时延迟该通知、告知或张贴，自口头声明之日起不超过30天，除非在此期间提交了本节第(a)段所述的书面声明。

164.414 行政要求以及举证责任。

(a) 行政要求。受保护实体须就本子部分的要求遵守164.530(b)、(d)、(e)、(g)、(h)、(i)和(j)的行政要求。

(b) 举证责任。在发生违反E子部分的使用或披露时，受保护实体或业务伙伴(视情况而定)应承担举证责任，证明所有通知均按本子部分的要求发出，或该使用或披露不构成164.402所定义的违规事件。

E分部分--个人可识别健康信息的隐私

授权依据：42 U.S.C.1320d-2、1320d-4和1320d-9;Pub.L.104-191第264条，110 Stat.2033-2034(42 U.S.C.1320d-2(注释))；以及Pub.L.111-5第13400-13424条，123 Stat.258-279。

164.500 适用性。

(a) 除非本部分另有规定，本子部分的标准、要求和实施规范适用于受保护实体对受保护健康信息的处理。

(b) 医疗信息交换中心必须按以下方式遵守标准、要求和实施规范：

(1)当医疗信息交换中心作为另一受保护实体的业务伙伴创建或接收受保护健康信息时，该交换中心必须遵守：

(i) 第164.500条关于适用性；

(ii) 与定义有关的第 164.501 条；

(iii) 关于受保护健康信息使用和披露的164.502，但交换中心被禁止使用或披露除根据其创建或接收受保护健康信息所依据的业务伙伴合同允许外，不得使用或披露受保护健康信息；

(iv) 关于受保护实体组织要求的164.504;

(v) 关于无需个人授权或同意或反对机会的使用和披露的164.512，但交换中心被禁止使用或披露受保护健康信息，除非在其创建或接收该受保护健康信息所依据的业务伙伴合同允许的范围内；

(vi) 第164.532条关于过渡要求的规定；以及

(vii) 关于隐私标准初始实施合规日期的164.534。

(2)当医疗信息交换中心非作为受保护实体的业务伙伴创建或接收受保护健康信息时，该交换中心必须遵守本子部分的所有标准、要求和实施规范。

(c) 在适用的情况下，本子部分采纳的标准、要求和实施规范适用于业务伙伴对受保护实体受保护健康信息的处理。

(d) 本子部分的标准、要求和实施规范不适用于国防部或任何其他联邦机构，也不适用于代表其行事的非政府组织在向海外外国国民受益人提供医疗服务时的情形。

[65 FR 82802,2000年12月28日，经67 FR 53266,2002年8月14日；68 FR 8381,2003年2月20日；78 FR 5695,2013年1月25日修订]

164.501 定义。

本子部分中使用的下列术语具有以下含义：惩教机构指由美国、州、领地、州或领地的政治分区或印第安部落运营或与其签订合同运营的任何刑罚或惩教设施、监狱、教养院、拘留中心、劳动农场、中途之家或居住社区项目中心，用于关押或改造被指控或被判犯有刑事罪行的人员或其他被合法拘留的人员。被合法拘留包括被裁定为少年犯的少年犯、等待驱逐出境的外国人、通过刑事司法系统被送入精神病机构的人员、证人或其他等待指控或审判的人员。

subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons* held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Designated record set means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Except as prohibited under §164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy

州或领地的下属机构，或印第安部落，用于关押或改造被指控或被判犯有刑事罪行的人员或其他被合法拘押的人员。其他人员被合法拘押包括被裁定为少年犯的少年犯、等待驱逐出境的外国人、通过刑事司法系统被送入精神病院的人员、证人或其他等待指控或审判的人员。

数据汇总指，就业务伙伴以其作为受保护实体的业务伙伴身份创建或接收的受保护健康信息而言，该业务伙伴将该等受保护健康信息与其以另一受保护实体的业务伙伴身份接收的受保护健康信息进行合并，以允许进行与各受保护实体的医疗保健运营相关的数据分析。

指定记录集指：

(1) 由受保护实体维护或为其维护的一组记录，该记录：

(i) 由受保护医疗服务提供者或为其维护的关于个人的医疗记录和账单记录；

(ii) 由健康计划或为其维护的参保、支付、索赔裁定以及病例或医疗管理记录系统；或

(iii) 由受保护实体或为其全部或部分用于对个人做出决策。

(2)就本段而言，术语"记录"指包含受保护健康信息并由受保护实体或为其维护、收集、使用或传播的任何信息项目、集合或分组。

直接治疗关系指个人与医疗服务提供者之间非间接治疗关系的治疗关系。医疗运营指受保护实体的以下任何活动，前提是该活动与受保护功能相关：

(1) 开展质量评估与改进活动，包括结果评价与开发临床指南，前提是此类活动所产生的任何研究不以获取可推广知识为主要目的；患者安全活动(如42 CFR 3.20所定义)；与改善健康或降低医疗成本相关的人群活动、方案制定、病例管理和护理协调、向医疗服务提供者和患者提供有关治疗替代方案的信息；以及不包括治疗的相关功能；

(2) 审查医疗保健专业人员的胜任能力或资质，评估执业人员和提供者的绩效、健康计划绩效，开展培训项目(其中医疗保健领域的学生、受训人员或执业人员在监督下学习，以实践或提高其作为医疗保健提供者的技能)，培训非医疗保健专业人员，以及认证、资质认定、许可或资格授予活动；

(3) 除 164.514(g) 的要求；

(4) 开展或安排医疗审查、法律服务和审计功能，包括欺诈和滥用检测与合规项目；

(5) 业务规划与开发，例如开展与实体管理和运营相关的成本管理和规划相关分析，包括处方集制定与管理、支付方式或承保政策的制定或改进；以及

(6) 实体的业务管理和一般行政活动，包括但不限于：

(i) 与实施和遵守本分章要求相关的管理活动；

(ii) 客户服务，包括为政策提供数据分析

holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Consistent with the applicable requirements of §164.514, creating deidentified health information or a limited data set, and fundraising for the benefit of the covered entity.

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Indirect treatment relationship means a relationship between an individual and a health care provider in which:

(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and

(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

Inmate means a person incarcerated in or otherwise confined to a correctional institution.

Marketing:

(1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing does not include a communication made:

(i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.

(ii) For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

(A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

(B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) *Financial remuneration* means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

Payment means:

(1) The activities undertaken by:

(i) Except as prohibited under §164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its

保单持有人、计划发起人或其他客户，前提是受保护健康信息未向该保单持有人、计划发起人或客户披露。

(iii) 内部申诉的解决；

(iv) 受保护实体与另一受保护实体，或在此类活动后将成为受保护实体的实体之间全部或部分出售、转让、合并或整合，以及与此类活动相关的尽职调查；以及

(v) 符合164.514适用要求，创建去标识化健康信息或有限数据集，以及为受保护实体的利益进行筹款。

卫生监督机构指美国、州、领地、州或领地的政治分区或印第安部落的机构或权力机关，或根据此类公共机构的授权或与其签订合同而行事的人员或实体，包括此类公共机构的雇员或代理人或其承包商或已获其授权的人员或实体，该机构或权力机关依法有权监督医疗保健系统(无论是公共还是私人)或政府项目，在这些项目中健康信息对于确定资格或合规性是必要的，或执行健康信息相关的民权法律。

(1) 医疗服务提供者根据另一医疗服务提供者的医嘱向个人提供医疗服务；以及

(2) 医疗服务提供者通常直接向另一医疗服务提供者提供服务或产品，或报告与医疗服务相关的诊断或结果，由后者向个人提供服务或产品，或向个人报告。

囚犯是指被监禁或以其他方式关押在惩教机构中的人。

营销：

(1) 除第款另有规定外

本定义第(2)项，营销是指就产品或服务进行鼓励接收的沟通，

通信的接收者购买或使用该产品或服务。

(2) 营销不包括以下通信：

(i) 提供续药提醒或以其他方式就目前正在为个人开具的药品或生物制品进行沟通，但仅限于受保护实体为进行该沟通而收到的任何财务报酬与受保护实体进行该沟通的成本合理相关的情况。

(ii) 用于以下治疗和医疗保健运营目的，但受保护实体为进行该沟通而收到财务报酬的情况除外：

(A) 由医疗服务提供者对个人进行治疗，包括为个人进行病例管理或护理协调，或向个人指导或推荐替代治疗、疗法、医疗服务提供者或护理环境；

(B) 描述由作出通信的受保护实体提供或包含在其福利计划中的健康相关产品或服务(或此类产品或服务的付款)，包括关于以下内容的通信：参与医疗保健提供者网络或健康计划网络的实体；健康计划的替换或增强；以及仅向健康计划参保人提供的、为福利计划增加价值但不属于福利计划一部分的健康相关产品或服务；或

(C) 用于病例管理或护理协调、联系个人并提供有关治疗替代方案的信息，以及相关功能，但仅限于这些活动不属于治疗定义范围的情况。

(3) 财务报酬是指来自其产品或服务被描述的第三方或代表该第三方支付的直接或间接付款。直接或间接付款不包括对个人治疗的任何付款。

付款指：

(1) 由以下主体开展的活动：(i) 除164.502(a)(5)(i) 禁止的情况外，健康计划为获取保费或确定或履行其

responsibility for coverage and provision of benefits under the health plan; or

(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan.

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 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.

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 74 FR 42769, Aug. 24, 2009; 78 FR 5695, Jan. 25, 2013]

§ 164.502 Uses and disclosures of protected health information: General rules.

(a) *Standard.* A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) *Covered entities: Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with §164.506;

(iii) Incident to a use or disclosure otherwise permitted or required by this

在健康计划下承保和提供福利的责任；或

(ii) 医疗服务提供者或健康计划为提供医疗服务获取或提供报销；以及

(2) 本定义第(1)款中的活动与接受医疗服务的个人有关，包括但不限于：

(i) 资格或承保范围的确定(包括福利协调或费用分担金额的确定)，以及健康福利索赔的裁决或代位求偿；

(ii) 根据参保人健康状况和人口统计特征对应付金额进行风险调整；

(iii) 账单、索赔管理、收款活动、根据再保险合同获取付款(包括止损保险和超额损失保险)，以及相关医疗保健数据处理；

(iv) 就医必要性、健康计划承保范围、护理适当性或收费合理性对医疗服务进行审查；

(v) 利用审查活动，包括服务预认证和预授权、同步和回顾性服务审查；以及

(vi) 向消费者报告机构披露与收取保费或报销有关的以下任何受保护健康信息：

(A) 姓名和地址；

(B) 出生日期；

(C) 社会安全号码；(D) 付款历史；(E) 账号；以及

(F) 医疗保健提供者和/或健康计划的名称和地址。

心理治疗记录指由身为心理健康专业人员的医疗保健提供者记录的(以任何媒介)记录，记录或分析私人咨询会话或团体、联合或家庭咨询会话期间的谈话内容，并与个人医疗记录的其余部分分开。心理治疗记录不包括药物处方和监测、咨询会话的开始和结束时间、治疗的方式和频率

提供的、临床测试结果，以及以下任何项目的摘要：诊断、功能状态、治疗计划、症状、预后和迄今的进展。公共卫生机构指美国、州、领地、州或领地的政治分区或印第安部落的机构或权力机关，或根据此类公共机构的授权或与其签订合同而行事的人员或实体，包括此类公共机构的雇员或代理人或其承包商或已获其授权的人员或实体，该机构或权力机关作为其官方授权的一部分负责公共卫生事务。研究指旨在开发或贡献可推广知识的系统性调查，包括研究开发、测试和评估。治疗指由一个或多个医疗保健提供者提供、协调或管理医疗保健及相关服务，包括医疗保健提供者与第三方协调或管理医疗保健；医疗保健提供者之间关于患者的咨询；或患者从一个医疗保健提供者转诊至另一个医疗保健提供者以接受医疗保健。

[65 FR 82802,2000年12月28日，经67 FR 53266,2002年8月14日；68 FR 8381,2003年2月20日；74 FR 42769,2009年8月24日；78 FR 5695,2013年1月25日修订]

164.502 受保护健康信息的使用与披露受保护健康信息：一般规则。

(a) 标准。受保护实体或业务伙伴不得使用或披露受保护健康信息，除非本子部分或本子章第160部分C子部分允许或要求。

(1) 受保护实体：允许的使用和披露。受保护实体被允许按以下方式使用或披露受保护健康信息：

(i) 致个人；

(ii) 用于治疗、付款或医疗保健运营，按164.506允许并遵守该条规定；

(iii) 附属于本规则另行允许或要求的使用或披露

subpart, provided that the covered entity has complied with the applicable requirements of §§164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;

(iv) Except for uses and disclosures prohibited under §164.502(a)(5)(i), pursuant to and in compliance with a valid authorization under §164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, §164.510; and

(vi) As permitted by and in compliance with any of the following:

(A) This section.

(B) Section 164.512 and, where applicable, §164.509.

(C) Section 164.514(e), (f), or (g).

(2) *Covered entities: Required disclosures.* A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and required by §164.524 or §164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.

(3) *Business associates: Permitted uses and disclosures.* A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to §164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under §164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.

(4) *Business associates: Required uses and disclosures.* A business associate is required to disclose protected health information:

(i) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.

(ii) To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under §164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.

(5) *Prohibited uses and disclosures*—(i) *Use and disclosure of genetic information for underwriting purposes:* Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of *health plan*, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan:

(A) Except as provided in paragraph (a)(5)(i)(B) of this section:

(*1*) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(*2*) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(*3*) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and

(*4*) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

(B) Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

(ii) *Sale of protected health information:*

(A) Except pursuant to and in compliance with §164.508(a)(4), a covered entity or business associate may not sell protected health information.

(B) For purposes of this paragraph, sale of protected health information means:

子部分，前提是受保护实体已就该等其他允许或要求的使用或披露遵守 164.502(b)、164.514(d)和164.530(c)的适用要求；

(iv) 除 164.508下的有效授权；

(v) 根据164.510项下的协议或该条另行允许的情况；以及

(vi) 在符合并遵守以下任何一项规定的情况下：

(A) 本节。

(B) 第164.512条，以及在适用情况下，第164.509条。

(C) 第164.514(e)、(f)或(g)条。

(2) 受保护实体：强制披露。受保护实体必须披露受保护健康信息：

(i) 在根据 164.528提出请求并要求时，向个人披露；以及

(ii) 当部长根据本子章第160部分C子部分要求调查或确定受保护实体对本子章的遵守情况时。

(3) 商业伙伴：允许的使用和披露。商业伙伴只能根据其商业伙伴合同或依据 164.504(e)(2)(i)(A)或(B)中指定的目的，且此类使用或披露由其合同或其他安排允许。

(4) 业务伙伴：强制使用和披露。业务伙伴必须披露受保护健康信息：

(i) 当部长根据本子章第160部分C子部分要求调查或确定业务伙伴对本子章的遵守情况时。

(ii) 向受保护实体、个人或个人指定人披露，以满足受保护实体在164.524(c)(2)(ii)和(3)(ii)项下的义务。

关于个人请求获取受保护健康信息电子副本的事项。

(5) 禁止的使用和披露 -(i) 为承保目的使用和披露遗传信息：尽管本子部分有任何其他规定，健康计划(不包括属于健康计划定义第(1)(viii)段范围内的长期护理保单签发人)不得为承保目的使用或披露属于遗传信息的受保护健康信息。就本节第(a)(5)(i)段而言，承保目的就健康计划而言指：

(A) 除第款另有规定外

(a) (5) (i)(B) 本节：

(1) 计划、承保范围或保单下福利的资格规则或确定(包括参保和持续资格)，或福利确定(包括作为完成健康风险评估或参与健康促进计划等活动的回报而变更免赔额或其他费用分担机制)；

(2) 计划、承保范围或保单下保费或缴款金额的计算(包括作为完成健康风险评估或参与健康促进计划等活动的回报而提供的折扣、回扣、实物付款或其他保费差异机制)；

(3) 计划、承保范围或保单下任何预先存在的条件排除的适用；以及

(4) 与健康保险或健康福利合同的订立、续签或替换相关的其他活动。

(B) 承保目的不包括在个人根据计划、承保范围或保单寻求福利时对医疗适当性的确定。

(ii) 受保护健康信息的出售：

(A) 除依据并遵守164.508(a)(4) 外，受保护实体或业务伙伴不得出售受保护健康信息。

(B)就本段而言，受保护健康信息的出售是指：

(*1*) Except as provided in paragraph (a)(5)(ii)(B)(*2*) of this section, a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.

(*2*) Sale of protected health information does not include a disclosure of protected health information:

(*i*) For public health purposes pursuant to §164.512(b) or §164.514(e);

(*ii*) For research purposes pursuant to §164.512(i) or §164.514(e), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;

(*iii*) For treatment and payment purposes pursuant to §164.506(a);

(*iv*) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to §164.506(a);

(*v*) To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;

(*vi*) To an individual, when requested under §164.524 or §164.528;

(*vii*) Required by law as permitted under §164.512(a); and

(*viii*) For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

(iii) *Reproductive health care*—(A) *Prohibition.* Subject to paragraphs (a)(5)(iii)(B) and (C) of this section, a covered entity or business associate may not use or disclose protected health information for any of the following activities:

(*1*) To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care.

(*2*) To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care.

(*3*) To identify any person for any purpose described in paragraphs (a)(5)(iii)(A)(*1*) or (*2*) of this section.

(B) *Rule of applicability.* The prohibition at paragraph (a)(5)(iii)(A) of this section applies only where the relevant activity is in connection with any person seeking, obtaining, providing, or facilitating reproductive health care, and the covered entity or business associate that received the request for protected health information has reasonably determined that one or more of the following conditions exists:

(*1*) The reproductive health care is lawful under the law of the state in which such health care is provided under the circumstances in which it is provided.

(*2*) The reproductive health care is protected, required, or authorized by Federal law, including the United States Constitution, under the circumstances in which such health care is provided, regardless of the state in which it is provided.

(*3*) The presumption at paragraph (a)(5)(iii)(C) of this section applies.

(C) *Presumption.* The reproductive health care provided by another person is presumed lawful under paragraph (a)(5)(iii)(B)(*1*) or (*2*) of this section unless the covered entity or business associate has any of the following:

(*1*) Actual knowledge that the reproductive health care was not lawful under the circumstances in which it was provided.

(*2*) Factual information supplied by the person requesting the use or disclosure of protected health information that demonstrates a substantial factual basis that the reproductive health care was not lawful under the specific

(1) 除第款另有规定外
本节(a)(5)(ii)(B)(2)所述，受保护实体或业务伙伴(如适用)披露受保护健康信息，且该受保护实体或业务伙伴直接或间接从受保护健康信息接收方或代表接收方处获得报酬以交换该受保护健康信息。

受保护实体或业务伙伴不得为以下任何活动使用或披露受保护健康信息：

(1) 仅因寻求、获得、提供或协助生殖健康护理的行为而对任何人进行刑事、民事或行政调查。

(2) 出售受保护健康信息不包括以下受保护健康信息的披露：

(2) 仅因寻求、获得、提供或协助生殖健康护理的行为而对任何人施加刑事、民事或行政责任。

(*i*) 依据 164.514(e) 为公共卫生目的；

(*ii*) 依据 164.514(e)为研究目的，且受保护实体或业务伙伴收到的唯一报酬是为支付为该等目的准备和传输受保护健康信息的成本而收取的合理成本费用；

(3) 为段落中所述任何目的识别任何个人

本节第(a)(5)(iii)(A)(1)或(2)段。(B) 适用规则。本节第(a)(5)(iii)(A)段的禁止仅在相关活动与任何人寻求、获得、提供或协助生殖健康护理有关，且收到受保护健康信息请求的受保护实体或业务伙伴已合理确定存在以下一项或多项条件时适用：

(*iii*) 依据164.506(a) 用于治疗和付款目的；

(*iv*) 为受保护实体的全部或部分出售、转让、合并或整合，以及依据164.506(a) 进行医疗保健运营定义第(6)(iv)段所述的相关尽职调查；

(*v*) 向业务伙伴或由业务伙伴为受保护实体代为开展的活动，或在分包商情况下为业务伙伴代为开展的活动，依据 164.502(e) 和 164.504(e)，且唯一报酬由受保护实体向业务伙伴提供，或由业务伙伴向分包商提供(如适用)，用于开展此类活动；

(1) 该生殖健康护理在提供该护理所在州的法律下，在提供该护理的情形下是合法的。

(2) 该生殖健康护理在提供该护理的情形下受联邦法律(包括美国宪法)保护、要求或授权，无论其在哪个州提供。

(*vi*) 根据 164.528 的要求，向个人提供；

(3) 该推定见第
(a) (5) 本节(iii)(C) 适用。
(C) 推定。由他人提供的生殖健康护理被推定为本节第(a)(5)(iii)(B)(1)或(2)段下的合法护理，除非受保护实体或业务伙伴有以下任一情形：

(*vii*) 法律要求且符合164.512(a) 允许的情形；以及

(*viii*) 为本子部分适用要求所允许并符合的任何其他目的，且受保护实体或业务伙伴收到的唯一报酬是合理的、基于成本的费用，以覆盖为此目的准备和传输受保护健康信息的成本，或其他法律明确允许的费用。

(1) 实际知悉该生殖健康护理在提供该护理的情形下不合法。

(2) 请求使用或披露受保护健康信息的人提供的、证明该生殖健康护理在特定情形下不合法的实质性事实依据的事实信息

(iii) 生殖健康护理 - (A) 禁止。在遵守本节第(a)(5)(iii)(B)和(C)段的前提下，a

circumstances in which it was provided.

(D) *Scope.* For the purposes of this subpart, seeking, obtaining, providing, or facilitating reproductive health care includes, but is not limited to, any of the following: expressing interest in, using, performing, furnishing, paying for, disseminating information about, arranging, insuring, administering, authorizing, providing coverage for, approving, counseling about, assisting, or otherwise taking action to engage in reproductive health care; or attempting any of the same.

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

(2) *Minimum necessary does not apply.* This requirement does not apply to:

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

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

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

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

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

(vi) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

(c) *Standard: Uses and disclosures of protected health information subject to an agreed upon restriction.* A covered entity that has agreed to a restriction pursuant to §164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in §164.522(a).

(d) *Standard: Uses and disclosures of de-identified protected health information*—(1) *Uses and disclosures to create de-identified information.* A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) *Uses and disclosures of de-identified information.* Health information that meets the standard and implementation specifications for de-identification under §164.514(a) and (b) is considered not to be individually identifiable health information, *i.e.*, de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of §164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

(e)(1) *Standard: Disclosures to business associates.* (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with §164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.

(2) *Implementation specification: Documentation.* The satisfactory assurances

提供该信息的具体情形。

(D) 范围。就本子部分而言，寻求、获得、提供或协助生殖健康护理包括但不限于以下任一情形：表达兴趣、使用、实施、提供、支付、传播相关信息、安排、保险、管理、授权、提供承保、批准、咨询、协助或以其他方式采取行动参与生殖健康护理；或试图进行上述任何行为。

(b) 标准：最小必要 -
最低必要原则适用。在使用或披露受保护健康信息，或向另一受保护实体或业务伙伴请求受保护健康信息时，受保护实体或业务伙伴必须作出合理努力，将受保护健康信息限制在实现该使用、披露或请求的预期目的所需的最低必要范围内。

(2) 最低必要标准不适用。
此要求不适用于：

(i) 向医疗保健提供者披露或应其请求用于治疗；

(ii) 向个人作出的使用或披露，如本节第(a)(1)(i)段所允许或本节第(a)(2)(i)段所要求；

(iii) 依据164.508 授权所作的使用或披露；

(iv) 依据本子章第160部分C子部分向部长作出的披露；

(v)164.512(a)所述法律要求的使用或披露；以及

(vi) 为遵守本子章适用要求所必需的使用或披露。

(c) 标准：受已达成限制约束的受保护健康信息的使用和披露。根据 164.522(a)另有规定。

(d) 标准：去标识化受保护健康信息的使用和披露 -(1) 为创建而进行的使用和披露

去标识化信息。受保护实体可以使用受保护健康信息来创建非个人可识别健康信息，或仅为该目的向业务伙伴披露受保护健康信息，无论该去标识化信息是否将由受保护实体使用。

(2) 去标识化信息的使用和披露。符合 164.514适用要求去标识化的信息，前提是：

(i) 披露旨在使编码或以其他方式去标识化的信息可被重新识别的代码或其他记录识别手段，构成对受保护健康信息的披露；以及

(ii) 如果去标识化信息被重新识别，受保护实体只能按本子部分允许或要求的方式使用或披露此类重新识别的信息。

(e)(1) 标准：向业务伙伴的披露。(i) 受保护实体可向业务伙伴披露受保护健康信息，并可允许业务伙伴代表其创建、接收、维护或传输受保护健康信息，前提是受保护实体获得令其满意的保证，即业务伙伴将适当保护该信息。受保护实体无需从作为分包商的业务伙伴处获得此类令其满意的保证。

(ii) 业务伙伴可向作为分包商的业务伙伴披露受保护健康信息，并可允许分包商代表其创建、接收、维护或传输受保护健康信息，前提是业务伙伴依据164.504(e)(1)(i) 获得令其满意的保证，即分包商将适当保护该信息。

(2) 实施规范：文档记录。令其满意的保证

required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of §164.504(e).

(f) *Standard: Deceased individuals.* A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.

(g)(1) *Standard: Personal representatives.* As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

(2) *Implementation specification: Adults and emancipated minors.* If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(3)(i) *Implementation specification: Unemancipated minors.* If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(A) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

(B) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or

(C) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(ii) Notwithstanding the provisions of paragraph (g)(3)(i) of this section:

(A) If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with §164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*;

(B) If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with §164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*; and

(C) Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative under paragraphs (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under §164.524 to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

(4) *Implementation specification: Deceased individuals.* If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

本部分第(e)(1)段所要求的，必须通过与业务伙伴签订的符合164.504(e)适用要求的书面合同或其他书面协议或安排予以记录。

(f) 标准：已故个人。受保护实体必须在本子部分的要求下，对已故个人的受保护健康信息在个人死亡后50年内予以遵守。

(g)(1) 标准：个人代表。如本段所规定，除本节第(g)(3)和(g)(5)段另有规定外，受保护实体必须就本子章而言将个人代表视为个人。

(2) 实施规范：成年人和已独立未成年人。如果根据适用法律，某人有权代表成年人或已独立未成年人就医疗保健相关决策行事，则受保护实体必须在本子章下将该人视为个人代表，涉及与该个人代表相关的受保护健康信息。

(i) 实施规范：

(3)

未解除亲权的未成年人。如果根据适用法律，父母、监护人或 other 以*in loco parentis*身份行事的人员有权代表属于未解除亲权的未成年人的个人就医疗保健相关决定行事，则受保护实体必须在本子章下将该人员视为个人代表，涉及与此类个人代表相关的受保护健康信息，但该人员不得成为未解除亲权的未成年人的个人代表，且该未成年人在涉及与医疗保健服务有关的受保护健康信息时有权作为个人行事，如果：

(A) 未成年人同意该医疗保健服务；法律不要求对该医疗保健服务获得其他同意，无论是否也已获得他人的同意；且未成年人未要求将该人视为个人代表；

(B) 未成年人可以合法获得此类医疗保健服务，而无需父母、监护人或其他代替父母行事的人的同意，且未成年人、法院或法律授权的其他人同意此类医疗服务；或

(C) 父母、监护人或其他代替父母行事的人同意受保护医疗保健提供者与未成年人之间关于此类医疗服务的保密协议。

(ii) 尽管有本节第(g)(3)(i)段的规定：

(A) 如果且在一定程度上，州或其他法律(包括适用判例法)的适用条款允许或要求，受保护实体可以披露或根据164.524 提供访问未独立未成年人的受保护健康信息给父母、监护人或其他代替父母行事的人；

(B) 如果且在一定程度上，州或其他法律(包括适用判例法)的适用条款禁止，受保护实体不得披露或根据164.524 提供访问未独立未成年人的受保护健康信息给父母、监护人或其他代替父母行事的人；以及

(C) 如果父母、监护人或其它以代替父母身份行事的人不是本节(g)(3)(i)(A)、(B)或(C)段所规定的个人代表，且州法或其它法律(包括判例法)中没有适用的访问条款，则受保护实体可以根据164.524向父母、监护人或其它以代替父母身份行事的人提供或拒绝提供访问权限，前提是此类行动符合州法或其它适用法律，且该决定必须由持证医疗保健专业人员在行使专业判断时作出。

(4) 实施规范：已故个人。如果根据适用法律，遗嘱执行人、遗产管理人或其他人有权代表已故个人或其遗产行事，则受保护实体必须在本子章下将该人视为个人代表，涉及与该个人代表相关的受保护健康信息。

(5) *Implementation specification: Abuse, neglect, endangerment situations.* Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative, provided that the conditions at paragraphs (g)(5)(i) and (ii) of this section are met:

(i) Paragraphs (g)(5)(i)(A) and (B) of this section both apply.

(A) The covered entity has a reasonable belief that any of the following is true:

(*1*) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person.

(*2*) Treating such person as the personal representative could endanger the individual.

(B) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

(ii) The covered entity does not have a reasonable belief under paragraph (g)(5)(i)(A) of this section if the basis for their belief is the provision or facilitation of reproductive health care by such person for and at the request of the individual.

(h) *Standard: Confidential communications.* A covered health care provider or health plan must comply with the applicable requirements of §164.522(b) in communicating protected health information.

(i) *Standard: Uses and disclosures consistent with notice.* A covered entity that is required by §164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by §164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in §164.520(b)(1)(iii)(A)–(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

(j) *Standard: Disclosures by whistleblowers and workforce member crime victims*—(1) *Disclosures by whistleblowers.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) *Disclosures by workforce members who are victims of a crime.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in §164.512(f)(2)(i).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53267, Aug. 14, 2002; 78 FR 5696, Jan. 25, 2013; 89 FR 33063, Apr. 26, 2024]

§ 164.504 Uses and disclosures: Organizational requirements.

(a) *Definitions.* As used in this section:

Plan administration functions means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

(5) 实施规范：虐待、忽视、危害情况。尽管有相反州法律或本款任何要求，受保护实体可以选择不将某人视为个人代表，前提是满足本节第(g)(5)(i)和(ii)段的条件：

(i) 本节(g)(5)(i)(A)和(B)两段均适用。

(A) 受保护实体有合理理由相信以下任何一项属实：

(1)该个人已经或可能遭受该人的家庭暴力、虐待或忽视。

(2)将该人视为个人代表可能危及该个人。

(B) 受保护实体在行使专业判断时决定，将该人视为该个人的个人代表不符合该个人的最佳利益。

(ii) 如果受保护实体信念的基础是该人应个人请求为该个人提供或促成生殖健康保健，则受保护实体不具有本节第(g)(5)(i)(A)段下的合理信念。

(h) 标准：保密通信。受保护医疗保健提供者或健康计划在沟通受保护健康信息时必须遵守164.522(b) 的适用要求。

(i) 标准：与通知一致的使用和披露。依据 164.520(b)(1)(iii) 要求在其通知中纳入特定声明的受保护实体，若其意图从事164.520(b)(1)(iii)(A)-(C) 所列活动，则不得为上述活动使用或披露受保护健康信息，除非该所需声明已纳入通知中。

(j) 标准：举报人和工作人员犯罪受害者的披露-(1) 举报人的披露。如果受保护实体的工作人员成员或业务伙伴披露受保护健康信息，前提是：

(i) 工作人员成员或业务伙伴善意相信受保护实体从事了非法行为或其他违反专业或临床标准的行为，或受保护实体提供的护理、服务或条件可能危及一个或多个患者、工作人员或公众；以及

(ii) 披露对象为：

(A) 依法授权调查或以其他方式监督受保护实体相关行为或条件的健康监督机构或公共卫生当局，或适当的医疗保健认证组织，目的是报告受保护实体未能满足专业标准或不当行为的指控；或

(B) 由工作人员成员或业务伙伴聘请或代表其聘请的律师，目的是确定工作人员成员或业务伙伴就本节第(j)(1)(i)段所述行为方面的法律选择。

(2) 作为犯罪受害者的工作人员成员的披露。如果作为犯罪行为受害者的工作人员成员向执法官员披露受保护健康信息，受保护实体不被视为违反本子部分的要求，前提是：

(i) 披露的受保护健康信息是关于犯罪行为的疑似实施者；以及

(ii) 披露的受保护健康信息限于164.512(f)(2)(i) 中列出的信息。

[65 FR 82802,2000年12月28日，经67 FR 53267,2002年8月14日；78 FR 5696,2013年1月25日；89 FR 33063,2024年4月26日修订]

164.504 使用与披露：组织-组织要求。

(a) 定义。本节中使用的：

计划管理功能指团体健康计划的计划发起人代表团体健康计划执行的管理功能，不包括计划发起人就计划发起人的任何其他福利或福利计划执行的功能。

Summary health information means information, that may be individually identifiable health information, and:

(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

(2) From which the information described at §164.514(b)(2)(i) has been deleted, except that the geographic information described in §164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

(b)–(d) [Reserved]

(e)(1) *Standard: Business associate contracts.* (i) The contract or other arrangement required by §164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in §164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(iii) A business associate is not in compliance with the standards in §164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(2) *Implementation specifications: Business associate contracts.* A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by §164.410;

(D) In accordance with §164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with §164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with §164.528;

(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart

摘要健康信息指可能是个人可识别健康信息的信息，并且：

(1)该信息总结计划发起人根据团体健康计划为其提供健康福利的个人的索赔历史、索赔费用或索赔类型；以及

(2)已删除 164.514(b)(2)(i)(B)所述地理信息只需汇总至五位邮政编码级别。

(b)-(d)[保留](e)(1) 标准：业务伙伴合同。(i)164.502(e)(2) 要求的合同或其他安排必须满足本节第(e)(2)、(e)(3)或(e)(5)段的要求(如适用)。

(ii) 如果受保护实体知道业务伙伴存在构成重大违约或违反业务伙伴在合同或其他安排下义务的活动或实践模式，则受保护实体不符合164.502(e)和本段的标准，除非受保护实体采取了合理步骤来纠正违约或终止违规(如适用)，并且如果此类步骤不成功，则在可行的情况下终止了合同或安排。

(iii) 如果业务伙伴知道分包商存在构成重大违约或违反分包商在合同或其他安排下义务的活动或实践模式，则业务伙伴不符合164.502(e)和本段的标准，除非业务伙伴采取了合理步骤来纠正违约或终止违规(如适用)，并且如果此类步骤不成功，则在可行的情况下终止了合同或安排。

(2) 实施规范：业务伙伴合同。受保护实体与业务伙伴之间的合同必须：

(i) 确立业务伙伴对受保护健康信息的允许和 required 使用与披露。合同不得授权业务伙伴以如果由受保护实体实施将违反本子部分要求的方式，但以下除外：

(A) 合同可以允许业务伙伴为业务伙伴的适当管理和行政使用和披露受保护健康信息，如本节第(e)(4)段所规定；以及

(B) 合同可以允许业务伙伴提供与受保护实体医疗保健运营相关的数据聚合服务。

(ii) 规定业务伙伴将：

(A) 不得使用或进一步披露信息，除非合同允许或要求或法律要求；

(B) 使用适当保障措施并在适用情况下遵守本部分 C 子部分关于电子受保护健康信息的规定，以防止使用或披露信息超出其合同规定；

(C) 向受保护实体报告其知悉的任何未由合同规定的信息使用或披露，包括164.410 要求的安全未受保护健康信息泄露；

(D) 根据164.502(e)(1)(ii)，确保代表业务伙伴创建、接收、维护或传输受保护健康信息的任何分包商同意遵守适用于该业务伙伴的关于此类信息的相同限制和条件；

(E) 根据164.524 提供受保护健康信息；

(F) 提供受保护健康信息以供修订，并根据164.526 将任何修订纳入受保护健康信息；

(G) 提供根据164.528 提供披露记录所需的信息；

(H) 在业务伙伴履行受保护实体在本子部分项下义务的范围内，遵守本子部分的要求；

that apply to the covered entity in the performance of such obligation.

(I) Make 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 available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(3) *Implementation specifications: Other arrangements.* (i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with this paragraph and §164.314(a)(1), if applicable, by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section and §164.314(a)(2), if applicable.

(B) The covered entity may comply with this paragraph and §164.314(a)(1), if applicable, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section and §164.314(a)(2), if applicable.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in §160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and §164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and §164.314(a)(1), if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(iv) A covered entity may comply with this paragraph and §164.314(a)(1) if the covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the covered entity has a data use agreement with the business associate that complies with §§164.514(e)(4) and 164.314(a)(1), if applicable.

(4) *Implementation specifications: Other requirements for contracts and other arrangements.* (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the protected health information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or

(B)(*1*) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and

适用于受保护实体在履行该义务时。

(I) 将其从受保护实体处收到或代表受保护实体创建或收到的、与使用和披露受保护健康信息相关的内部做法、账簿和记录提供给部长，以便确定受保护实体对本子部分的遵守情况；以及

(J) 在合同终止时，如果可行，返还或销毁业务伙伴从受保护实体收到或代表受保护实体创建或收到的、业务伙伴仍以任何形式保留的所有受保护健康信息，并且不保留此类信息的任何副本；或者，如果此类返还或销毁不可行，则将合同保护扩展到该信息，并将进一步使用和披露限制在使信息返还或销毁不可行的那些目的上。

(iii) 如果受保护实体确定业务伙伴违反了合同的实质性条款，授权受保护实体终止合同。

(3) 实施规范：其他安排。(i) 如果受保护实体及其业务伙伴均为政府实体：

(A) 受涵盖实体可通过与业务伙伴签订包含实现本节第(e)(2)段及（如适用）164.314(a)(1)。

(B) 如果其他法律(包括受保护实体或其业务伙伴通过的法规)包含适用于业务伙伴的要求，且这些要求实现了本节第(e)(2)款和(如适用) 164.314(a)(1)。

(ii) 如果法律要求业务伙伴代表受保护实体履行某项功能或活动，或向受保护实体提供本子章160.103 中业务伙伴定义所述的服务，则该受保护实体可以向业务伙伴披露受保护健康信息--

在遵守法律强制要求所必需的范围内，业务伙伴无需满足本款及(如适用) 164.314(a)(1)所要求的令人满意的保证，并且如果此类尝试失败，则记录该尝试以及无法获得此类保证的原因。

(iii) 如果本节第(e)(2)(iii)款要求的终止授权与受保护实体或其业务伙伴的法定义务不一致，受保护实体可以在其其他安排中省略该终止授权。

(iv) 如果受保护实体仅向业务伙伴披露有限数据集以供业务伙伴执行医疗保健运营职能，且受保护实体与该业务伙伴签订了符合 164.514(e)(4)及(如适用)164.314(a)(1)的数据使用协议，则受保护实体可遵守本款及164.314(a)(1)。

(4) 实施规范：合同和其他安排的其他要求。(i) 受保护实体与业务伙伴之间的合同或其他安排可以允许业务伙伴使用其以受保护实体业务伙伴身份收到的受保护健康信息，如果必要：

(A) 用于业务伙伴的适当管理和行政；或

(B)履行业务伙伴的法律责任。

(ii) 受保护实体与业务伙伴之间的合同或其他安排可以允许业务伙伴披露其以业务伙伴身份收到的受保护健康信息，用于本节第(e)(4)(i)款所述目的，如果：

(A) 该披露为法律所要求；或

(B)(1) 业务伙伴从信息被披露给的人处获得合理保证，即该信息将被保密，并且

used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and

(*2*) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(5) *Implementation specifications: Business associate contracts with subcontractors.* The requirements of §164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by §164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(f)(1) *Standard: Requirements for group health plans.* (i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under §164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.

(ii) Except as prohibited by §164.502(a)(5)(i), the group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for purposes of:

(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

(B) Modifying, amending, or terminating the group health plan.

(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) *Implementation specifications: Requirements for plan documents.* The plan documents of the group health plan must be amended to incorporate provisions to:

(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

(B) Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

(E) Make available protected health information in accordance with §164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with §164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;

仅在法律要求或向其披露信息的目的所必需的范围内使用或进一步披露；以及

(2) 该人将其知悉的任何信息保密性已被违反的情形通知业务伙伴。

(5) 实施规范：业务伙伴与分包商的合同。 164.502(e)(1)(ii)所要求的合同或其他安排，其适用方式与这些要求适用于受保护实体与业务伙伴之间的合同或其他安排相同。

(f)(1) 标准：团体健康计划的要求。(i) 除本节第(f)(1)(ii)或(iii)段规定或164.508另行授权的情形外，团体健康计划为向计划发起人披露受保护健康信息，或为安排或允许健康保险承保人或HMO就该团体健康计划向计划发起人披露受保护健康信息，必须确保计划文件按照本子部分的要求限制计划发起人对该等信息的使用和披露。

(ii) 除164.502(a)(5)(i)禁止的情况外，团体健康计划，或就该团体健康计划而言的健康保险承保人或HMO，可向计划发起人披露摘要健康信息，如果计划发起人出于以下目的请求摘要健康信息：

(A) 从健康计划获取保费投标，以根据团体健康计划提供健康保险覆盖；或

(B)修改、修订或终止团体健康计划。

(iii) 团体健康计划，或就该团体健康计划而言的健康保险承保人或 HMO，可以向计划发起人披露有关个人是否参加团体健康计划、是否参加或已退出该计划提供的健康保险承保人或 HMO 的信息。

(2) 实施规范：计划文件的要求。团体健康计划的计划文件必须修订，以纳入以下条款：

(i) 确立计划发起人对此类信息的允许和必要使用与披露，但该等允许和必要的使用与披露不得与本子部分不一致。

(ii) 规定团体健康计划仅在收到计划发起人的认证后，方可向计划发起人披露受保护健康信息，该认证须表明计划文件已修订以纳入以下条款，且计划发起人同意：

(A) 除计划文件允许或要求或法律要求外，不得使用或进一步披露该信息；

(B) 确保其向其提供从团体健康计划收到的受保护健康信息的任何代理人同意遵守适用于计划发起人的有关该信息的相同限制和条件；

(C) 不得将信息用于与雇佣相关的行动和决定，或与计划发起人的任何其他福利或员工福利计划相关的用途；

(D) 向团体健康计划报告其知悉的任何与本条规定的使用或披露不一致的信息使用或披露；

(E) 根据164.524 提供受保护健康信息；

(F) 提供受保护健康信息以供修订，并根据164.526 将任何修订纳入受保护健康信息；

(G) 提供根据164.528 提供披露记录所需的信息；

(H) 将其与使用和披露从团体健康计划收到的受保护健康信息相关的内部做法、账簿和记录提供给部长，以便确定团体健康计划对本子部分的遵守情况；

(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and

(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.

(3) *Implementation specifications: Uses and disclosures.* A group health plan may:

(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;

(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;

(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by §164.520(b)(1)(iii)(C) is included in the appropriate notice; and (iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

(g) *Standard: Requirements for a covered entity with multiple covered functions.* (1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.

(2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53267, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 78 FR 5697, Jan. 25, 2013]

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

(a) *Standard: Permitted uses and disclosures.* Except with respect to uses or disclosures that require an authorization under §164.508(a)(2) through (4) or that are prohibited under §164.502(a)(5)(i), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

(b) *Standard: Consent for uses and disclosures permitted.* (1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.

(I) 在可行的情况下，返还或销毁计划发起人仍以任何形式保留的从团体健康计划收到的所有受保护健康信息，并在不再需要用于披露目的时不得保留此类信息的副本，但若此类返还或销毁不可行，则将进一步的使用和披露限制在使信息返还或销毁不可行的那些目的上；以及

(J) 确保建立本节第(f)(2)(iii)段所要求的充分隔离。

(iii) 规定团体健康计划与计划发起人之间的充分分离。计划文件必须：

(A) 描述计划发起人控制下将被授予访问待披露受保护健康信息的那些员工或员工类别或其他人员，但任何在正常业务过程中接收与团体健康计划下的付款、医疗保健运营或其他相关事项有关的受保护健康信息的员工或人员必须包含在此类描述中；

(B) 将本条(f)(2)(iii)(A)段所述此类员工和其他人员的访问和使用限制在计划发起人为团体健康计划执行的计划管理功能范围内；以及

(C) 提供有效的机制，以解决本条(f)(2)(iii)(A)段所述人员不遵守本段要求的计划文件条款的任何问题。

(3) 实施规范：使用和披露。团体健康计划可以：

(i) 仅按照本条(f)(2)段的规定，向计划发起人披露受保护健康信息以执行计划发起人执行的计划管理功能；

(ii) 不允许团体健康计划的健康保险发行人或HMO向计划发起人披露受保护健康信息，除非本段允许；

(iii) 不得披露，且不得允许健康保险发行机构或HMO向计划发起人披露受保护健康信息，除非本段允许，除非本节164.520(b)(1)(iii)(C)所要求的声明包含在适当的通知中；以及(iv) 不得为与就业相关的行动或决策的目的或与计划发起人的任何其他福利或雇员福利计划相关而向计划发起人披露受保护健康信息。

(g) 标准：对具有多项受保护功能的受保护实体的要求。(1) 履行多项受保护功能、从而构成健康计划、受保护医疗服务提供者和医疗保健信息交换中心任意组合的受保护实体，必须遵守本子部分中适用于其所履行的健康计划、医疗服务提供者或医疗保健信息交换中心受保护功能的标准、要求和实施规范。

(2) 执行多项受保护功能的受保护实体可以使用或披露仅接受受保护实体的健康计划或医疗保健提供者服务(而非两者)的个人的受保护健康信息，但仅限于与正在执行的适当功能相关的目的。

[65 FR 82802,2000年12月28日，经67 FR 53267,2002年8月14日；68 FR 8381,2003年2月20日；78 FR 5697,2013年1月25日修订]

164.506 为实施治疗、付款和医疗保健运营而使用和披露信息

治疗、支付或医疗保健运营之外。

(a) 标准：允许的使用和披露。除需要根据 164.502(a)(5)(i)被禁止的使用或披露外，受保护实体可以按照本条(c)段的规定为治疗、付款或医疗保健运营使用或披露受保护健康信息，前提是此类使用或披露与本子部分的其他适用要求一致。

(b) 标准：允许的使用和披露的同意。(1) 受保护实体可以获得个人的同意，以使用或披露受保护健康信息以执行治疗、付款或医疗保健运营。

(2) Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under §164.508, is required or when another condition must be met for such use or disclosure to be permissible under this subpart.

(c) *Implementation specifications: Treatment, payment, or health care operations.* (1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.

(2) A covered entity may disclose protected health information for treatment activities of a health care provider.

(3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.

(4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:

(i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or

(ii) For the purpose of health care fraud and abuse detection or compliance.

(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

[67 FR 53268, Aug. 14, 2002, as amended at 78 FR 5698, Jan. 25, 2013]

§ 164.508 Uses and disclosures for which an authorization is required.

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

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

(i) To carry out the following treatment, payment, or health care operations:

(A) Use by the originator of the psychotherapy notes for treatment;

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

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

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

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

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

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

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

(4) *Authorization required: Sale of protected health information.* (i) Notwithstanding any provision of this subpart,

(2) 当根据164.508需要授权或必须满足另一条件才能使此类使用或披露在本子部分下被允许时，本条(b)段下的同意不得有效允许使用或披露受保护健康信息。

(c) 实施规范：
治疗、付款或医疗保健运营。(1) 受保护实体可为自身的治疗、付款或医疗保健运营使用或披露受保护健康信息。

(2) 受保护实体可以为医疗保健提供者的治疗活动披露受保护健康信息。

(3) 受保护实体可以向另一受保护实体或医疗保健提供者披露受保护健康信息，用于接收信息实体的付款活动。

(4) 受保护实体可以向另一受保护实体披露受保护健康信息，用于接收信息实体的医疗保健运营活动，前提是每个实体与作为所请求受保护健康信息主体的个人有或曾有 relationship，该受保护健康信息与此类 relationship 相关，且披露是：

(i) 用于第[编号]段所列目的
(1) 或医疗保健运营定义的第(2)项；或

(ii) 用于医疗保健欺诈和滥用行为的检测或合规目的。

(5) 参与有组织医疗保健安排的受保护实体可以就有组织医疗保健安排的任何医疗保健运营活动向有组织医疗保健安排的其他参与者披露有关个人的受保护健康信息。

[67 FR 53268,2002年8月14日，经78 FR 5698,2013年1月25日修订]

164.508 使用与披露的授权
需要授权的情形。

(a) 标准：使用和披露的授权 -(1) 需要授权：一般规则。除非本子章另有允许或要求，受保护实体不得使用或披露受保护健康信未经本节下有效授权的使用或披露。当受保护实体获得或收到对其使用或披露受保护健康信息的有效授权时，此类使用或披露必须符合该授权。

(2) 需要授权：心理治疗记录。尽管本子部分有任何规定，除164.532中的过渡条款外，受保护实体必须获得对心理治疗记录的任何使用或披露的授权，但以下情况除外：

(i) 执行以下治疗、付款或医疗保健运营：

(A) 由心理治疗笔记的创建者用于治疗；

(B) 受保护实体为其自身培训项目使用或披露，在这些项目中，心理健康领域的学生、受训人员或从业者在监督下学习实践或提高其在团体、联合、家庭或个人咨询方面的技能；或

(C) 受保护实体使用或披露以在个人提起的法律诉讼或其他程序中为自己辩护；以及

(ii) 根据 164.512(a)允许的使用或披露； 164.512(g)(1)；或164.512(j)(1)(i)。

(3) 需要授权：营销。
(i) 尽管本子部分有任何规定，除164.532中的过渡条款外，受保护实体必须获得授权才能为营销目的使用或披露受保护健康信息，除非该通信的形式为：

(A) 受保护实体与个人进行的面谈沟通；或

(B)由受保护实体提供的名义价值的促销礼品。

(ii) 如果营销涉及164.501中营销定义第(3)段所定义的来自第三方向受保护实体的财务报酬，授权必须声明涉及此类报酬。

(4) 需要授权：出售受保护健康信息。(i) 尽管本子部分有任何规定，

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

(b) *Implementation specifications: General requirements*—(1) *Valid authorizations.* (i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (a)(4)(ii), (c)(1), and (c)(2) of this section, as applicable.

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

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

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

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

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

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

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

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

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

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

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

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

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

(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health

除 164.501所定义的受保护健康信息出售的披露获得授权。(ii) 此类授权必须声明该披露将导致向覆盖实体支付报酬。

(b) 实施规范：一般要求 -(1) 有效授权。(i) 有效授权是满足本条(a)(3)(ii)、(a)(4)(ii)、(c)(1)和(c)(2)段要求(如适用)的文件。

(ii) 有效的授权书除本节要求的要素外，还可包含额外的要素或信息，但该等额外要素或信息不得与本节要求的要素相抵触。

(2) 缺陷授权书。提交的文件如有下列任何缺陷，授权书即属无效：

(i) 有效期已过，或受保护实体已知悉有效期事件已发生；

(ii) 授权书未就本节(c)款所述要素(如适用)完整填写；

(iii) 受保护实体已知该授权已被撤销；

(iv) 授权违反本节第(b)(3)或(4)段(如适用);

(v) 受保护实体已知悉授权书中任何重要信息为虚假。

(3) 复合授权。受保护健康信息使用或披露的授权不得与任何其他文件结合形成复合授权，但以下情况除外：

(i) 为研究而使用或披露受保护健康信息的授权书，可与同一或另一研究的任何其他类型书面许可合并。该例外包括将为研究而使用或披露受保护健康信息的授权书与同一研究的另一授权书合并，或与以下授权书合并：

创建或维护研究数据库或存储库，或同意参与研究。如果受保护实体医疗服务提供者根据本节第(b)(4)(i)段的规定，将提供与研究相关的治疗作为提供其中一项授权的前提条件，则根据本段创建的任何复合授权必须明确区分有条件部分和无条件部分，并向个人提供选择加入无条件授权中所述研究活动的机会。

(ii) 使用或披露心理治疗笔记的授权书，仅可与另一份使用或披露心理治疗笔记的授权书合并。

(iii) 本节规定的授权(用于使用或披露心理治疗笔记的授权除外)可与本节规定的任何其他此类授权合并，但受保护实体以提供本节第(b)(4)段所述治疗、付款、健康计划参保或福利资格为条件而要求提供其中一项授权的情形除外。本段关于在一项授权以提供本节第(b)(4)段所述治疗、付款、健康计划参保或福利资格为条件时禁止合并授权的规定，不适用于依照本节第(b)(3)(i)段创建的复合授权。

(4) 禁止以授权书为条件。受保护实体不得以个人提供授权书为条件，向其提供治疗、付款、健康计划参保或福利资格，但下列情形除外：

(i) 受保护医疗保健提供者可以个人提供本节项下为该研究使用或披露受保护健康信息的授权书为条件，提供与研究相关的治疗；

(ii) 健康计划可以个人提供该健康计划所要求的授权书为条件，办理健康计划参保或福利资格；

plan prior to an individual's enrollment in the health plan, if:

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

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

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

(5) *Revocation of authorizations.* An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

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

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

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

(c) *Implementation specifications: Core elements and requirements*—(1) *Core elements.* A valid authorization under this section must contain at least the following elements:

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

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

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

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

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

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

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

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

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

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

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

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

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

(iii) The potential for information disclosed pursuant to the authorization

在个人加入健康计划之前制定计划，如果：

(A) 所寻求的授权书系用于该健康计划对个人的资格或参保决定，或用于其承保或风险评级决定；且

(B) 该授权书并非用于本节(a)(2)款项下使用或披露心理治疗笔记；且

(iii) 受保护实体可以个人提供向该第三方披露受保护健康信息的授权书为条件，提供仅为生成受保护健康信息以向第三方披露的医疗保健服务。

(5) 撤销授权书。个人可随时撤销本节项下提供的授权书，但撤销须以书面形式作出，下列情形除外：

(i) 受保护实体已依赖该行动采取行动；或

(ii) 如授权书系作为获得保险承保的条件而取得，其他法律赋予保险人就保单项下索赔或保单本身提出异议的权利。

(6) 文件记录。受保护实体必须按164.530(j)的要求，记录并保存本节项下任何已签署的授权书。

(c) 实施规范：核心要素与要求 -(1) 核心要素。本节项下的有效授权书必须至少包含以下要素：

(i) 对拟使用或披露信息的描述，该描述须以具体且有意义的方式指明该信息。

(ii) 获授权提出所请求使用或披露的人员或人员类别的姓名或其他具体标识。

(iii) 受保护实体可向其作出所请求使用或披露的人员或人员类别的姓名或其他具体标识。

(iv) 对所请求使用或披露的每一目的的描述。当个人主动提出授权且未(或.....)时，“应个人请求”的表述即为对目的的充分描述。

选择不提供目的声明。

(v) 与个人或使用或披露目的相关的有效期或有效期事件。如授权书系为研究(包括创建和维护研究数据库或研究存储库)而使用或披露受保护健康信息，则“研究结束”“无”或类似表述即为充分。

(vi) 个人的签名和日期。如果授权由个人的个人代表签署，还必须提供该代表代表个人行事的权限描述。

(2) 必需声明。除核心要素外，授权书还必须包含足以使个人知悉以下全部事项的声明：

(i) 个人有权以书面形式撤销授权书，以及下列任一内容：

(A) 撤销权的例外情形以及个人撤销授权书方式的说明；或

(B) 在164.520所要求通知中已包含本节(c)(2)(i)(A)款信息的范围内，援引受保护实体的通知。

(ii) 能否以授权书为条件提供治疗、付款、参保或福利资格，须说明下列任一内容：

(A) 当本节(b)(4)款关于禁止以授权书为条件的规定适用时，受保护实体不得以个人是否签署授权书为条件提供治疗、付款、参保或福利资格；或

(B) 当依据本节(b)(4)款，受保护实体可以未能取得该授权书为条件提供治疗、健康计划参保或福利资格时，个人拒绝签署授权书对其产生的后果。

(iii) 依据该授权披露信息的可能性

to be subject to redisclosure by the recipient and no longer be protected by this subpart.

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

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

[67 FR 53268, Aug. 14, 2002, as amended at 78 FR 5699, Jan. 25, 2013]

§ 164.509 Uses and disclosures for which an attestation is required.

(a) *Standard: Attestations for certain uses and disclosures of protected health information to persons other than covered entities or business associates.* (1) A covered entity or business associate may not use or disclose protected health information potentially related to reproductive health care for purposes specified in §164.512(d), (e), (f), or (g)(1), without obtaining an attestation that is valid under paragraph (b)(1) of this section from the person requesting the use or disclosure and complying with all applicable conditions of this part.

(2) A covered entity or business associate that uses or discloses protected health information potentially related to reproductive health care for purposes specified in §164.512(d), (e), (f), or (g)(1), in reliance on an attestation that is defective under paragraph (b)(2) of this section, is not in compliance with this section.

(b) *Implementation specifications: General requirements*—(1) *Valid attestations.* (i) A valid attestation is a document that meets the requirements of paragraph (c)(1) of this section.

(ii) A valid attestation verifies that the use or disclosure is not otherwise prohibited by §164.502(a)(5)(iii).

(iii) A valid attestation may be electronic, provided that it meets the requirements in paragraph (c)(1) of this section, as applicable.

(2) *Defective attestations.* An attestation is not valid if the document submitted has any of the following defects:

(i) The attestation lacks an element or statement required by paragraph (c) of this section.

(ii) The attestation contains an element or statement not required by paragraph (c) of this section

(iii) The attestation violates paragraph (b)(3) of this section.

(iv) The covered entity or business associate has actual knowledge that material information in the attestation is false.

(v) A reasonable covered entity or business associate in the same position would not believe that the attestation is true with respect to the requirement at paragraph (c)(1)(iv) of this section.

(3) *Compound attestation.* An attestation may not be combined with any other document except where such other document is needed to satisfy the requirements at paragraph (c)(iv) of this section or at §164.502(a)(5)(iii)(C), as applicable.

(c) *Implementation specifications: Content requirements and other obligations*—(1) *Required elements.* A valid attestation under this section must contain the following elements:

(i) A description of the information requested that identifies the information in a specific fashion, including one of the following:

(A) The name of any individual(s) whose protected health information is sought, if practicable.

(B) If including the name(s) of any individual(s) whose protected health information is sought is not practicable, a description of the class of individuals whose protected health information is sought.

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

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

(iv) A clear statement that the use or disclosure is not for a purpose prohibited under §164.502(a)(5)(iii).

(v) A statement that a person may be subject to criminal penalties pursuant to 42 U.S.C. 1320d-6 if that person knowingly and in violation of HIPAA obtains individually identifiable health information relating to an individual or discloses individually identifiable health information to another person.

接收方可能重新披露且不再受本子部分保护。

(3) 通俗语言要求。授权书必须以通俗语言书写。

(4) 向个人提供副本。如果受保护实体就使用或披露受保护健康信息向个人寻求授权，该受保护实体必须向该个人提供一份已签署授权的副本。

[67 FR 53268,2002年8月14日，经78 FR 5699,2013年1月25日修订]

164.509 使用与披露用于需要证明的情形。

(a) 标准：向受保护实体或业务伙伴以外的人员特定使用和披露受保护健康信息的证明。(1) 受保护实体或业务伙伴不得为164.512(d)、(e)、(f)或(g)(1)规定的目的，使用或披露可能与生殖健康保健相关的受保护健康信息，除非从请求使用或披露的人员处获得根据本节第(b)(1)段有效的证明，并遵守本部分所有适用条件。

(2)受保护实体或业务伙伴，若依据本节第(b)(2)段规定存在缺陷的证明，为164.512(d)、(e)、(f)或(g)(1)所规定的目的，使用或披露可能与生殖健康护理相关的受保护健康信息，则不符合本节规定。

(b) 实施规范：一般要求-(1) 有效证明(i) 有效证明是符合本节第(c)(1)段要求的文件。

(ii) 有效证明须核实该使用或披露不受164.502(a)(5)(iii)另行禁止。

(iii) 有效证明可以采用电子形式，前提是其在适用情况下符合本节第(c)(1)段的要求。

(2) 有缺陷的证明。如果所提交的文件存在下列任何缺陷，则该证明无效：

(i) 该证明缺少本节第(c)段所要求的要素或声明。

(ii) 该证明包含本节第(c)段未要求的要素或声明

(iii) 该证明违反了本节第(b)(3)段的规定。

(iv) 受保护实体或业务伙伴实际知晓该证明中的重要信息是虚假的。

(v) 处于相同地位的合理受保护实体或业务伙伴不会相信该证明就本节第(c)(1)(iv)段的要求而言是真实的。

(3) 复合证明。证明不得与任何其他文件合并，但为满足本节第(c)(iv)段或164.502(a)(5)(iii)(C)(在适用情况下)的要求而需要该其他文件的情形除外。

(c) 实施规范：内容要求和其他义务 -(1) 必需要素。本节规定的有效证明必须包含下列要素：

(i) 对所请求信息的描述，须以特定方式识别该信息，包括下列之一：

(A) 在可行的情况下，其受保护健康信息被寻求的任何个人的姓名。

(B) 如果列入其受保护健康信息被寻求的任何个人的姓名不可行，则描述其受保护健康信息被寻求的个人类别。

(ii) 被请求作出使用或披露的人员或人员类别的姓名或其他特定标识。

(iii) 受保护实体将向其作出所请求的使用或披露的人员或人员类别的姓名或其他特定标识。

(iv) 明确声明该使用或披露并非出于164.502(a)(5)(iii)所禁止的目的。

(v) 声明：任何人如果明知并违反HIPAA而获取与个人有关的个人可识别健康信息，或向他人披露个人可识别健康信息，则可能依据42 U.S.C.1320d-6受到刑事处罚。

(vi) Signature of the person requesting the protected health information, which may be an electronic signature, and date. If the attestation is signed by a representative of the person requesting the information, a description of such representative's authority to act for the person must also be provided.

(2) *Plain language requirement.* The attestation must be written in plain language.

(d) *Material misrepresentations.* If, during the course of using or disclosing protected health information in reasonable reliance on a facially valid attestation, a covered entity or business associate discovers information reasonably showing that any representation made in the attestation was materially false, leading to a use or disclosure for a purpose prohibited under §164.502(a)(5)(iii), the covered entity or business associate must cease such use or disclosure.

[89 FR 33063, Apr. 26, 2024]

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.

A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

(a) *Standard: Use and disclosure for facility directories*—(1) *Permitted uses and disclosure.* Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:

(i) Use the following protected health information to maintain a directory of individuals in its facility:

(A) The individual's name;

(B) The individual's location in the covered health care provider's facility;

(C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and

(D) The individual's religious affiliation; and

(ii) Use or disclose for directory purposes such information:

(A) To members of the clergy; or

(B) Except for religious affiliation, to other persons who ask for the individual by name.

(2) *Opportunity to object.* A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.

(3) *Emergency circumstances.* (i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:

(A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and

(B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.

(ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.

(b) *Standard: Uses and disclosures for involvement in the individual's care and notification purposes*—(1) *Permitted uses and disclosures.* (i) A covered entity may, in accordance with paragraphs (b)(2), (b)(3), or (b)(5) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care.

(vi) 请求受保护健康信息的人员的签名(可以是电子签名)和日期。如果该证明由请求信息人员的代表签署，则还必须提供该代表代为行事的权限说明。

(2) 平实语言要求。该证明必须以平实语言书写。

(d) 重大虚假陈述如果在合理依赖表面有效的证明使用或披露受保护健康信息的过程中，受保护实体或业务伙伴发现合理表明证明中的任何陈述在重大方面虚假的信息，导致用于164.502(a)(5)(iii)禁止的目的，受保护实体或业务伙伴必须停止此类使用或披露。

[89 FR 33063，2024年4月26日]

164.510 使用和披露要-为个人提供同意或反对的机会。

受保护实体可以使用或披露受保护健康信息，前提是个人事先被告知该使用或披露，并有机会按照本节适用要求同意、禁止或限制该使用或披露。受保护实体可以口头告知个人本节所允许的使用或披露，并取得个人的口头同意或反对。

(a) 标准：设施目录的使用和披露-(1) 允许的使用和披露除非根据本节第(a)(2)或(3)段表达反对，受保护医疗保健提供者可以：

(i) 使用下列受保护健康信息在其设施内维护个人名录：

(A) 个人的姓名；

(B)个人在受保护医疗保健提供者设施内的位置；

(C) 以不传达个人具体医疗信息的概括性术语描述的个人状况；以及

(D)个人的宗教归属；以及

(ii) 为目录目的使用或披露此类信息：

(A) 致神职人员；或

(B) 除宗教信仰外，向指名询问该个人的其他人披露。

(2) 反对机会。受保护医疗保健提供者必须告知个人其可能列入名录的受保护健康信息以及其可能向其披露此类信息的人员(包括向神职人员披露有关宗教信仰的信息)，并向个人提供机会，以限制或禁止本节第(a)(1)段所允许的部分或全部使用或披露。

(3) 紧急情况。(i) 如果由于个人无行为能力或紧急治疗情形而无法切实提供本节第(a)(2)段所要求的反对使用或披露的机会，受保护医疗保健提供者可以为设施名录使用或披露本节第(a)(1)段所允许的部分或全部受保护健康信息，前提是该披露：

(A) 符合受保护医疗保健提供者所知的个人先前表达的任何偏好；以及

(B) 符合受保护医疗保健提供者在运用专业判断后确定的个人最佳利益。

(ii) 当切实可行时，受保护医疗保健提供者必须告知个人，并提供本节第(a)(2)段所要求的反对为名录目的使用或披露的机会。

(b) 标准：为参与个人护理和通知目的而进行的使用和披露-(1) 允许的使用和披露。(i) 受保护实体可依照本节第(b)(2)、(b)(3)或(b)(5)段，向个人的家庭成员、其他亲属或亲密私人朋友，或该个人指定的任何其他人员，披露与该人员参与个人医疗保健或与个人医疗保健相关的付款直接相关的受保护健康信息。

(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (b)(3), (b)(4), or (b)(5) of this section, as applicable.

(2) *Uses and disclosures with the individual present.* If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:

(i) Obtains the individual's agreement;

(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

(iii) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

(3) *Limited uses and disclosures when the individual is not present.* If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

(4) *Uses and disclosures for disaster relief purposes.* A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2), (b)(3), or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

(5) *Uses and disclosures when the individual is deceased.* If the individual is deceased, a covered entity may disclose to a family member, or other persons identified in paragraph (b)(1) of this section who were involved in the individual's care or payment for health care prior to the individual's death, protected health information of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5699, Jan. 25, 2013]

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

Except as provided by § 164.502(a)(5)(iii), a covered entity may use or disclose protected health information without the written authorization of the individual, as described in § 164.508, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section and § 164.509. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given verbally.

(a) *Standard: Uses and disclosures required by law.* (1) A covered entity may

(ii) 受保护实体可使用或披露受保护健康信息，以通知或协助通知(包括识别或定位)个人的家庭成员、个人代表或负责照护该个人的其他人员，告知该个人的位置、一般状况或死亡情况。为此类通知目的而使用或披露受保护健康信息，必须符合本节第(b)(2)、(b)(3)、(b)(4)或(b)(5)段的规定(视情况适用)。

(2) 个人在场时的使用和披露。如果个人在场，或在根据本节第(b)(1)款允许的使用或披露之前以其他方式可联系到，并且有能力做出医疗保健决定，则受保护实体可以使用或披露受保护健康信息，如果该实体：

(i) 获得个人的同意；

(ii) 向个人提供反对该披露的机会，且个人未表达反对；或

(iii) 根据专业判断的行使，从具体情况中合理推断个人不反对该披露。

(3) 个人不在场时的有限使用和披露。如果个人不在场，或由于个人的无行为能力或紧急情况而无法切实提供同意或反对使用或披露的机会，受保护实体可行使专业判断，确定披露是否符合个人的最佳利益，如果是，则仅披露与该人员参与个人护理或与个人医疗保健相关的支付或通知目的直接相关的受保护健康信息。受保护实体可运用专业判断及其对常见做法的经验，合理推断个人的最佳利益，允许某人代表个人领取已配好的处方药、医疗用品、X光片或其他类似形式的受保护健康信息。

(4) 灾害救援目的的使用和披露。受保护实体可向依法或依其章程授权协助灾害救援工作的公共或私人实体使用或披露受保护健康信息，以便与此类实体协调本节第(b)(1)(ii)段允许的使用或披露。本节第(b)(2)、(b)(3)或(b)(5)段的要求适用于此类使用和披露，但以受保护实体行使专业判断确定该要求不干扰应对紧急情况的能力为限。

(5) 个人死亡时的使用和披露。如果个人已死亡，受保护实体可向家庭成员或本节第(b)(1)段所确定的、在该个人死亡前参与其照护或医疗费用支付的其他人员，披露与该人员参与相关的个人受保护健康信息，除非这样做与受保护实体已知的个人先前明示的任何偏好不一致。

[65 FR 82802,2000年12月28日，经67 FR 53270,2002年8月14日；78 FR 5699,2013年1月25日修订]

164.512 使用和披露不要求授权或同意或反对机会的情形。

除 164.508所述），也无需个人同意或反对的机会（如 164.509的适用要求。当本节要求受涵盖实体告知个人本节允许的使用或披露，或个人可能同意该使用或披露时，受涵盖实体的信息和个人的同意可以口头方式提供。

(a) 标准：法律要求的使用和披露。(1) 受保护实体可以

use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

(b) *Standard: Uses and disclosures for public health activities*—(1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(iii) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

(A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

(B) To track FDA-regulated products;

(C) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or

(D) To conduct post marketing surveillance;

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who provides health care to the individual at the request of the employer:

(*1*) To conduct an evaluation relating to medical surveillance of the workplace; or

(*2*) To evaluate whether the individual has a work-related illness or injury;

(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

(*1*) By giving a copy of the notice to the individual at the time the health care is provided; or

(*2*) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

(vi) A school, about an individual who is a student or prospective student of the school, if:

(A) The protected health information that is disclosed is limited to proof of immunization;

使用或披露受保护健康信息，但以该使用或披露为法律要求，且该使用或披露符合并限于该法律的相关要求为限。

(2)受保护实体必须满足本节第(c)、(e)或(f)款所述的要求，以进行法律要求的使用或披露。

(b) 标准：公共卫生活动的使用和披露-(1) 允许的使用和披露。受保护实体可以为本节所述公共卫生活动和目的使用或披露受保护健康信息，向：

(i) 经法律授权为预防或控制疾病、伤害或残疾而收集或接收此类信息的公共卫生机构，包括但不限于报告疾病、伤害、出生或死亡等生命事件，以及开展公共卫生监测、公共卫生调查和公共卫生干预；或经公共卫生机构指示，向与公共卫生机构合作的外国政府机构官员披露；

(ii) 经法律授权接收儿童虐待或忽视报告的公共卫生机构或其他适当的政府机构；

(iii) 受食品药品监督管理局(FDA)管辖的人员，就该人员负有责任的FDA监管产品或活动，用于与该FDA监管产品或活动的质量、安全性或有效性相关的活动。此类目的包括：

(A) 收集或报告不利事件(或与食品或膳食补充剂相关的类似活动)、产品缺陷或问题(包括产品使用或标签方面的问题)，或生物产品偏差；

(B) 用于追踪FDA监管的产品；

(C) 使产品召回、修理或更换，或追溯(包括定位和通知已收到被召回、撤回或作为追溯对象产品的个人)；或

(D) 进行上市后监督；

(iv) 可能已接触传染病或以其他方式有感染或传播疾病或状况风险的人员，如果受保护实体或公共卫生机构经法律授权在开展公共卫生干预或调查时有必要通知该人员；或

(v) 雇主，关于作为该雇主工作人员成员的个人，如果：

(A) 受保护实体是应雇主请求向个人提供医疗保健的受保护医疗保健提供者：

(1)进行与工作场所医疗监测相关的评估；或

(2)评估个人是否有与工作相关的疾病或伤害；

(B) 所披露的受保护健康信息由关于与工作相关的疾病或伤害或工作场所相关医疗监测的发现组成；

(C) 雇主需要此类发现以遵守其根据29 CFR第1904至1928部分、30 CFR第50至90部分或具有类似目的的州法律记录此类疾病或伤害或履行工作场所医疗监测职责的义务；以及

(D) 受保护医疗保健提供者向个人提供书面通知，说明与工作场所医疗监测和与工作相关的疾病和伤害有关的受保护健康信息被披露给雇主：

(1)在提供医疗保健时向个人提供通知副本；或

(2)如果医疗保健在雇主的工作场所提供，则在提供医疗保健的地点显眼处张贴通知。

(vi) 学校，关于作为该校学生或准学生的个人，如果：

(A) 所披露的受保护健康信息仅限于免疫接种证明；

(B) The school is required by State or other law to have such proof of immunization prior to admitting the individual; and

(C) The covered entity obtains and documents the agreement to the disclosure from either:

(*1*) A parent, guardian, or other person acting *in loco parentis* of the individual, if the individual is an unemancipated minor; or

(*2*) The individual, if the individual is an adult or emancipated minor.

(2) *Permitted uses.* If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) *Standard: Disclosures about victims of abuse, neglect, or domestic violence*—(1) *Permitted disclosures.* Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;

(ii) If the individual agrees to the disclosure; or

(iii) To the extent the disclosure is expressly authorized by statute or regulation and:

(A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

(B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(2) *Informing the individual.* A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:

(i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

(ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(3) *Rule of construction.* Nothing in this section shall be construed to permit disclosures prohibited by §164.502(a)(5)(iii) when the sole basis of the report of abuse, neglect, or domestic violence is the provision or facilitation of reproductive health care.

(d) *Standard: Uses and disclosures for health oversight activities*—(1) *Permitted disclosures.* A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;

(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

(2) *Exception to health oversight activities.* For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity

(B) 州或其他法律要求学校在录取个人之前拥有此类免疫接种证明；以及

(C) 受保护实体获得并记录以下任一方的披露同意：

(1)个人的父母、监护人或以代替父母身份行事的其他人，如果个人是未 emancipated 的未成年人；或

(2) 个人，如果该个人是成年人或已解放的未成年人。

(2) 允许的使用。如果受保护实体同时也是公共卫生机构，则受保护实体在所有根据本节第(b)(1)款允许为公共卫生活动披露此类信息的情形下，均被允许使用受保护健康信息。

(c) 标准：关于虐待、忽视或家庭暴力受害者的披露-(1) 允许的披露。除本节第(b)(1)(ii)段允许的儿童虐待或忽视报告外，受保护实体可向依法授权接收此类虐待、忽视或家庭暴力报告的政府机构(包括社会服务或保护服务机构)披露其合理认为是个体虐待、忽视或家庭暴力受害者的受保护健康信息：

(i) 在法律要求披露的范围内，且披露符合并限于此类法律的相关要求；

(ii) 如果个人同意该披露；或

(iii) 在法规或规章明确授权披露的范围内，并且：

(A) 受保护实体在行使专业判断时认为披露对于防止对个人或其他潜在受害者的严重伤害是必要的；或

(B) 如果个人因无行为能力而无法同意，经授权接收报告的执法或其他公职人员表示，寻求披露的受保护健康信息不打算用于对个人不利，并且依赖于等待个人能够同意披露会实质性且不利地影响披露。

(2) 通知个人。根据本节第(c)(1)款允许进行披露的受保护实体必须及时通知个人此类报告已经或将会做出，除非：

(i) 受保护实体在行使专业判断时认为，告知个人会使该个人面临严重伤害的风险；或

(ii) 受保护实体将告知个人代表，且受保护实体合理认为该个人代表对虐待、忽视或其他伤害负有责任，并且告知该人将不符合受保护实体在行使专业判断时所确定的该个人的最佳利益。

(3) 解释规则。本节中的任何内容均不得解释为允许164.502(a)(5)(iii)所禁止的披露，当虐待、忽视或家庭暴力报告的唯一依据是提供或促进生殖健康护理时。

(d) 标准：健康监督活动的使用和披露 -(1) 允许的披露。受保护实体可以向健康监督机构披露受保护健康信息，用于法律授权的监督活动，包括审计；民事、行政或刑事调查；检查；许可或纪律处分；民事、行政或刑事诉讼或行动；或对以下进行适当监督所需的其他活动：

(i) 医疗保健系统；

(ii) 健康信息与受益人资格相关的政府福利计划；

(iii) 受政府监管计划约束的实体，其健康信息对于确定是否符合计划标准是必要的；或

(iv) 受民权法律约束的实体，其健康信息对于确定合规性是必要的。

(2) 健康监督活动的例外。就本节第(d)(1)款允许的披露而言，健康监督活动

does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

(i) The receipt of health care;

(ii) A claim for public benefits related to health; or

(iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

(3) *Joint activities or investigations.* Nothwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.

(4) *Permitted uses.* If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.

(e) *Standard: Disclosures for judicial and administrative proceedings*—(1) *Permitted disclosures.* A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or

(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or

(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.

(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and

(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:

(*1*) No objections were filed; or

(*2*) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

(v) For purposes of paragraph (e)(1) of this section, a qualified protective order means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties

不包括个人是调查或活动对象的调查或其他活动，且此类调查或其他活动并非源于且不直接相关于：

(i) 接受医疗保健；

(ii) 与健康相关的公共福利申请；或

(iii) 当患者的健康是公共福利或服务申请的核心组成部分时，获得或接受公共福利或服务的资格。

(3) 联合活动或调查。

尽管有本节第(d)(2)款的规定，如果健康监督活动或调查与涉及与健康无关的公共福利申请的监督活动或调查同时进行，则该联合活动或调查就本节第(d)款而言被视为健康监督活动。

(4) 允许的使用。如果受保护实体同时也是健康监督机构，该受保护实体可以按照第(e)段允许的方式将受保护健康信息用于健康监督活动。

(d) 本节。

(e) 标准：司法和行政程序的披露 -(1) 允许的披露。受保护实体可以在任何司法或行政程序过程中披露受保护健康信息：

(i) 响应法院或行政法庭的命令，前提是受保护实体仅披露该命令明确授权的受保护健康信息；或

(ii) 响应传票、证据开示请求或其他合法程序，且未附有法院或行政法庭的命令，如果：

(A) 受保护实体从寻求信息的当事方收到本节第(e)(1)(iii)段所述的满意保证，即该当事方已做出合理努力以确保作为所请求受保护健康信息主体的个人已收到该请求的通知；或

(B) 受保护实体从寻求信息的当事方收到本节第(e)(1)(iv)段所述的满意保证，即该方已作出合理努力以获得符合本节第(e)(1)(v)款要求的合格保护令。

(iii) 就本款而言

本节第(e)(1)(ii)(A)款，如果受保护实体从寻求受保护健康信息的一方收到书面声明及随附文件，证明以下事项，则受保护实体收到满意保证：

(A) 请求此类信息的当事方已善意尝试向个人提供书面通知(或者，如果个人的位置未知，则将通知邮寄至个人的最后已知地址)；

(B) 该通知包含关于请求受保护健康信息的诉讼或程序的充分信息，以允许个人向法院或行政法庭提出异议；且

(C) 个人向法院或行政法庭提出异议的时间已过，且：

(1) 未提出异议；或

(2) 个人提交的所有异议已由法院或行政法庭解决，且所寻求的披露与此类解决方案一致。

(iv) 就本款而言

本节第(e)(1)(ii)(B)款，如果受保护实体从寻求受保护健康信息的一方收到书面声明及随附文件，证明以下事项，则受保护实体收到满意保证：

(A) 引起信息请求的争议各方已同意合格的保护令，并将其提交给对争议有管辖权的法院或行政法庭；或

(B) 寻求受保护健康信息的当事方已向此类法院或行政法庭请求合格的保护令。

(v) 就本节第(e)(1)段而言，合格保护令是指，对于根据本节第(e)(1)(ii)段请求的受保护健康信息，法院或行政法庭的命令或当事方的约定

to the litigation or administrative proceeding that:

(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and

(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(v) of this section.

(2) *Other uses and disclosures under this section.* The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.

(f) *Standard: Disclosures for law enforcement purposes.* A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.

(1) *Permitted disclosures: Pursuant to process and as otherwise required by law.* A covered entity may disclose protected health information:

(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or

(ii) In compliance with and as limited by the relevant requirements of:

(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(B) A grand jury subpoena; or

(C) An administrative request for which response is required by law, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

(*1*) The information sought is relevant and material to a legitimate law enforcement inquiry;

(*2*) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

(*3*) De-identified information could not reasonably be used.

(2) *Permitted disclosures: Limited information for identification and location purposes.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) The covered entity may disclose only the following information:

(A) Name and address;

(B) Date and place of birth;

(C) Social security number;

(D) ABO blood type and rh factor;

(E) Type of injury;

(F) Date and time of treatment;

(G) Date and time of death, if applicable; and

(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

(3) *Permitted disclosure: Victims of a crime.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other

诉讼或行政程序：

(A) 禁止各方使用
或披露受保护健康信息用于除请求该信息的诉讼或程序以外的任何目的；以及

(B) 要求将 cov- 返还
受保护实体或销毁受保护健康信息(包括所有制作的副本)在诉讼或程序结束时。

(vi) 尽管有第
本节第(e)(1)(ii)段，受保护实体可根据本节第(e)(1)(ii)段所述合法程序披露受保护健康信息，而无需获得本节第(e)(1)(ii)(A)或(B)段规定的满意保证，如果受保护实体做出合理努力向个人提供足以满足本节第(e)(1)(iii)段要求的通知，或寻求足以满足本节第(e)(1)(v)段要求的合格保护令。

(2) 本节下的其他使用和披露。本款的规定不取代本节中另行允许或限制受保护健康信息使用或披露的其他规定。

(f) 标准：向执法部门披露
执法目的。如果本节第(f)(1)至(f)(6)款的条件(如适用)得到满足，受保护实体可为执法目的向执法官员披露受保护健康信息。

(1) 允许的披露：依据程序及法律另有要求。受保护实体可披露受保护健康信息：

(i) 按照法律(包括相关法律)的要求
要求报告某些类型伤口或其他身体伤害的法律，但受本节第(b)(1)(ii)款或(c)(1)(i)款约束的法律除外；或

(ii) 在遵守并限于
根据以下相关要求：
(A) 法院命令或法院指令
令状，或司法官员签发的传票或传唤令；

(B) 大陪审团传票；或
(C) 一项行政请求，旨在
法律要求的响应，包括行政传票或传票、民事或授权调查要求，或法律授权的类似程序，前提是：

(1) 所寻求的信息与合法的执法调查相关且重要；

(2) 该请求在考虑到寻求信息的目的的情况下，在合理可行的范围内具有特定性和有限的范围；且

(3) 去标识化信息无法被合理使用。

(2) 允许的披露：用于识别和定位目的的有限信息。除本节第(f)(1)款允许的法律要求的披露外，受保护实体可响应执法官员为识别或定位嫌疑人、逃犯、重要证人或失踪人员而提出的此类信息请求，披露受保护健康信息，前提是：

(i) 受保护实体仅可披露以下信息：

(A) 姓名和地址；
(B) 出生日期和地点；(C) 社会安全号码；

(D) ABO 血型和 Rh 因子；(E) 伤害类型；

(F) 治疗日期和时间；
(G) 死亡日期和时间(如适用)；以及

(H) 区分性身体特征的描述，包括身高、体重、性别、种族、头发和眼睛颜色、面部毛发(胡须或八字胡)的有无、疤痕和纹身。

(ii) 除第款允许的情况外
本节第(f)(2)(i)款，受保护实体不得为识别或定位之目的，根据本节第(f)(2)款披露与个人DNA或DNA分析、牙科记录、或体液或组织的分型、样本或分析有关的任何受保护健康信息。

(3) 允许的披露：犯罪受害者。除本节第(f)(1)段允许的法律要求的披露外，受保护实体可以响应执法官员的请求，披露关于个人是或疑似是犯罪受害者的受保护健康信息，其他

than disclosures that are subject to paragraph (b) or (c) of this section, if:

(i) The individual agrees to the disclosure; or

(ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(4) *Permitted disclosure: Decedents.* A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

(5) *Permitted disclosure: Crime on premises.* A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

(6) *Permitted disclosure: Reporting crime in emergencies.* (i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(A) The commission and nature of a crime;

(B) The location of such crime or of the victim(s) of such crime; and

(C) The identity, description, and location of the perpetrator of such crime.

(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.

(g) *Standard: Uses and disclosures about decedents*—(1) *Coroners and medical examiners.* A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.

(2) *Funeral directors.* A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

(h) *Standard: Uses and disclosures for cadaveric organ, eye or tissue donation purposes.* A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

(i) *Standard: Uses and disclosures for research purposes*—(1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:

(i) *Board approval of a waiver of authorization.* The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by

比受本节(b)或(c)款约束的披露，如果：

(i) 个人同意该披露；或

(ii) 受保护实体因无行为能力或其他紧急情况而无法获得个人的同意，前提是：

(A) 执法官员表示此类信息是确定受害者以外的人是否违法所必需的，且此类信息不打算用于对受害者不利；

(B) 执法官员表示，依赖于该披露的即时执法活动将因等待个人能够同意披露而受到重大不利影响；且

(C) 该披露符合受保护实体在行使专业判断时所确定的个人的最佳利益。

(4) 允许的披露：死者。受保护实体可以向执法官员披露关于已死亡个人的受保护健康信息，目的是提醒执法部门该个人的死亡，如果受保护实体怀疑该死亡可能源于犯罪行为。

(5) 允许的披露：场所内犯罪。受保护实体可以向执法官员披露受保护实体善意认为构成发生在受保护实体场所内的犯罪行为证据的受保护健康信息。

(6) 允许披露：在紧急情况下报告犯罪。(i) 在应对医疗紧急情况时提供紧急医疗保健的受保护实体(而非在受保护实体场所内发生的此类紧急情况)，如果此类披露似乎对于向执法部门警示以下事项是必要的，则可以向执法官员披露受保护健康信息：

(A)犯罪的委托和性质；

(B)此类犯罪的地点或此类犯罪受害者的地点；以及

(C) 该犯罪的实施者的身份、描述和地点。

(ii) 如果受保护实体认为本节第(f)(6)(i)段所述的医疗紧急情况是由需要紧急医疗保健的个人的虐待、忽视或家庭暴力造成的，则本节第(f)(6)(i)段不适用，为执法目的向执法官员进行的任何披露均受本节第(c)段约束。

(g) 标准：关于死者的使用和披露 -(1) 验尸官和法医。受保护实体可以为识别死者、确定死因或法律授权的其他职责的目的，向验尸官或法医披露受保护健康信息。同时履行验尸官或法医职责的受保护实体可以为本节该段所述目的使用受保护健康信息。

(2) 殡葬承办人。受保护实体可以依照适用法律，在必要范围内向殡葬承办人披露受保护健康信息，以便其履行与死者相关的职责。如果殡葬承办人履行职责需要，受保护实体可以在个人死亡之前并合理预期其死亡的情况下披露受保护健康信息。

(h) 标准：用于尸体器官、眼睛或组织捐赠目的的使用和披露。受保护实体可以为促进器官、眼睛或组织捐赠和移植的目的，向器官采购组织或其他从事尸体器官、眼睛或组织采购、储存或移植的实体使用或披露受保护健康信息。

(i) 标准：用于研究目的的使用和披露 -(1) 允许的使用和披露。受保护实体可以为研究使用或披露受保护健康信息，无论研究资金来源如何，前提是：

(i) 委员会批准授权豁免。受保护实体获得文件证明，对以下条款所要求的个人授权的变更或全部或部分豁免

§ 164.508 for use or disclosure of protected health information has been approved by either:

(A) An Institutional Review Board (IRB), established in accordance with 7 CFR lc.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(B) A privacy board that:

(*1*) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

(*2*) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

(*3*) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(ii) *Reviews preparatory to research.* The covered entity obtains from the researcher representations that:

(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) *Research on decedent's information.* The covered entity obtains from the researcher:

(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

(2) *Documentation of waiver approval.* For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

(i) *Identification and date of action.* A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

(ii) *Waiver criteria.* A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;

(*1*) An adequate plan to protect the identifiers from improper use and disclosure;

(*2*) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

(*3*) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;

(B) The research could not practicably be conducted without the waiver or alteration; and

(C) The research could not practicably be conducted without access to and use of the protected health information.

(iii) *Protected health information needed.* A brief description of the protected health information for which use or access has been determined to be necessary by the institutional review board or privacy board, pursuant to paragraph (i)(2)(ii)(C) of this section;

(iv) *Review and approval procedures.* A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or

164.508 所要求的个人授权用于使用或披露受保护健康信息的全部或部分变更或豁免已获以下之一批准：

(A) 一个机构审查委员会（IRB），依据7 CFR lc.107、10 CFR 745.107、14 CFR 1230.107、15 CFR 27.107、16 CFR 1028.107设立，21 CFR 56.107、22 CFR 225.107、24 CFR 60.107、28 CFR 46.107、32 CFR 219.107、34 CFR 97.107、38 CFR 16.107、40 CFR 26.107、45 CFR 46.107、45 CFR 690.107或49 CFR 11.107 ；或

(B) 一个隐私委员会，其：

(1) 其成员具有不同背景和必要的适当专业能力，以审查研究方案对个人隐私权及相关利益的影响；

(2) 至少包括一名与受保护实体无关联、与任何开展或赞助研究的实体无关联、且与任何此类实体的关联人员无亲属关系的成员；以及

(3) 没有任何成员参与审查其存在利益冲突的任何项目。

(ii) 研究前审查。

受保护实体从研究人员处获得以下陈述：

(A) 寻求使用或披露仅是为了在必要时审查受保护健康信息，以准备研究方案或用于研究准备阶段的类似目的；

(B) 研究人员在审查过程中不得从受保护实体移除任何受保护健康信息；以及

(C) 寻求使用或访问的受保护健康信息为研究目的所必需。

(iii) 对死者信息的研究。受保护实体从研究人员处获得：

(A) 声明所寻求的使用或披露仅用于对死者受保护健康信息的研究；

(B) 应受保护实体要求，提供此类个人死亡的文件证明；以及

(C) 声明所寻求使用或披露的受保护健康信息是研究目的所必需的。

(2) 豁免批准的文档记录。

为使基于变更或豁免批准文件的使用或披露根据本节第(i)(1)(i)段获得许可，该文件必须包括以下全部内容：

(i) 识别信息和行动日期。一份声明，指明 IRB 或隐私委员会以及授权变更或豁免获得批准的日期；

(ii) 豁免标准。一份声明，说明 IRB 或隐私委员会已确定授权的全部或部分变更或豁免满足以下标准：

(A) 受保护健康信息的使用或披露对个人隐私构成的风险不超过最小风险，至少基于以下要素的存在；

(1) 有适当计划保护标识符免遭不当使用和披露；

(2) 有适当计划在研究进行过程中尽早销毁标识符，除非有健康或研究理由保留标识符或法律另有要求保留；以及

(3) 有充分的书面保证，确保受保护健康信息不会被重复使用或披露给任何其他个人或实体，除非法律要求、用于研究研究的授权监督，或用于本子部分允许使用或披露受保护健康信息的其他研究；

(B) 研究在没有豁免或变更的情况下无法切实进行；以及

(C) 研究在没有访问和使用受保护健康信息的情况下无法切实进行。

(iii) 所需的受保护健康信息。根据本节第(i)(2)(ii)(C)段，机构审查委员会或隐私委员会确定使用或访问所必需的受保护健康信息的简要描述；

(iv) 审查和批准程序。一份声明，说明授权的变更或豁免已根据正常或

expedited review procedures, as follows:

(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);

(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;

(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

(v) *Required signature.* The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

(j) *Standard: Uses and disclosures to avert a serious threat to health or safety*—(1) *Permitted disclosures.* A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:

(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:

(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in §164.501.

(2) *Use or disclosure not permitted.* A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:

(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or

(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.

(3) *Limit on information that may be disclosed.* A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.

(4) *Presumption of good faith belief.* A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered

快速审查程序，具体如下：

(A) IRB 必须遵循共同规则的要求，包括正常审查程序(7 CFR 1c.108(b)、10 CFR 745.108(b)、14 CFR

1230.108 (b)、15 CFR 27.108(b)、16 CFR
1028.108 (b)、21 CFR 56.108(b)、22 CFR
225.108 (b)、24 CFR 60.108(b)、28 CFR
46.108 (b)、32 CFR 219.108(b)、34 CFR
97.108 (b)、38 CFR 16.108(b)、40 CFR
26.108 (b)、45 CFR 46.108(b)、45 CFR
690.108(b) 或 49 CFR 11.108(b)) 或快速审查程序(7 CFR 1c.110、10 CFR 745.110、14 CFR 1230.110、

15 CFR 27.110、16 CFR 1028.110、21 CFR
56.110、22 CFR 225.110、24 CFR 60.110、28 CFR
46.110、32 CFR 219.110、34 CFR 97.110、38 CFR
16.110、40 CFR 26.110、45 CFR 46.110、45 CFR
690.110或49 CFR
11.110)；

(B) 隐私委员会必须在多数隐私委员会成员出席的召集会议上审查拟议研究，包括至少一名满足本节第(i)(1)(i)(B)(2)段所述标准的成员，且授权的变更或豁免必须经出席会议的多数隐私委员会成员批准，除非隐私委员会选择按照该段使用加速审查程序

(C) 如果研究对作为受保护健康信息主体的个人的隐私构成的风险不超过最小风险，隐私委员会可采用快速审查程序。如果隐私委员会选择采用快速审查程序，对授权变更或豁免的审查和批准可由隐私委员会主席或由主席指定的一名或多名隐私委员会成员进行；以及

(v) 所需签名。授权变更或豁免的文件必须由 IRB 或隐私委员会(如适用)的主席或主席指定的其他成员签署。

(j) 标准：为避免对健康或安全造成严重威胁而进行的使用和披露 -(1) 允许的披露。受保护实体可以，在符合适用法律的情况下

以及道德行为标准，使用或披露受保护健康信息，如果受保护实体善意地认为该使用或披露：

(i)(A) 为防止或减轻对个人或公众健康或安全的严重且迫在眉睫的威胁所必需；且

(B) 向合理能够防止或减轻该威胁的一个人或多人(包括威胁的目标对象)披露；或

(ii) 为执法当局识别或抓捕某一个人所必需：

(A) 因该个人陈述承认参与了暴力犯罪，且受保护实体合理认为该犯罪可能已对受害者造成严重身体伤害；或

(B) 从所有情况来看，该个人似乎已从惩教机构或合法羁押中逃脱，该等术语的定义见164.501。

(2) 不允许的使用或披露。如果受保护实体通过以下方式获知本节第(j)(1)(ii)(A)段所述的信息，则不得依据本节第(j)(1)(ii)(A)段进行使用或披露：

(i) 在影响实施构成本节第(j)(1)(ii)(A)段所述披露依据的犯罪行为的倾向的治疗过程中，或在咨询或治疗过程中；或

(2) (iv)(C) 本节；
(i)

(ii) 通过该个人请求启动或转介接受本节第(j)(2)(i)段所述的治疗、咨询或治疗。

(3) 可披露信息的限制。依据本节第(j)(1)(ii)(A)段所作的披露仅应包含本节第(j)(1)(ii)(A)段所述的陈述以及本节第(f)(2)(i)段所述的受保护健康信息。

(4) 善意相信的推定。依据本节第(j)(1)款使用或披露受保护健康信息的受涵盖实体，如果该相信是基于受涵盖

entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

(k) *Standard: Uses and disclosures for specialized government functions*—(1) *Military and veterans activities*—(i) *Armed Forces personnel.* A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the FEDERAL REGISTER the following information:

(A) Appropriate military command authorities; and

(B) The purposes for which the protected health information may be used or disclosed.

(ii) *Separation or discharge from military service.* A covered entity that is a component of the Departments of Defense or Homeland Security may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

(iii) *Veterans.* A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.

(iv) *Foreign military personnel.* A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the FEDERAL REGISTER pursuant to paragraph (k)(1)(i) of this section.

(2) *National security and intelligence activities.* A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (*e.g.*, Executive Order 12333).

(3) *Protective services for the President and others.* A covered entity may disclose protected health information to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

(4) *Medical suitability determinations.* A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

(i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12968;

(ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or

(iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.

(5) *Correctional institutions and other law enforcement custodial situations*—(i) *Permitted disclosures.* A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

(A) The provision of health care to such individuals;

(B) The health and safety of such individual or other inmates;

实体的实际知悉或对具有表面知识或权限的人的可靠陈述的信赖，则推定其就本节第(j)(1)(i)或(ii)段所述的信念善意行事。

(k) 标准：特殊政府功能的使用和披露-(1) 军事和退伍军人活动-(i) 武装部队人员。受保护实体可为适当军事指挥当局认为必要的活动，使用和披露武装部队人员的受保护健康信息，以确保军事任务的正确执行，前提是适当军事当局已在FEDERAL REGISTER上发布通知，公布以下信息：

(A)适当的军事指挥机构；以及

(B) 受保护健康信息可被使用或披露的目的。

(ii) 退伍或解除军职。作为国防部或国土安全部组成部分的受保护实体，可在武装部队成员退伍或解除军职时，向退伍军人事务部(DVA)披露该个人的受保护健康信息，以便DVA根据退伍军人事务部长管理的法律确定该个人是否有资格或有权享受福利。

(iii) 退伍军人。作为退伍军人事务部组成部分的受保护实体，可向该部中确定依据退伍军人事务部长所执行法律获得福利的资格或权利、或提供该等福利的组成部分，使用和披露受保护健康信息。

(iv) 外国军事人员。受保护实体可向相应的外国军事当局使用和披露身为外国军事人员的个人的受保护健康信息，其目的与依据本节第(k)(1)(i)段在F EDERAL R EGISTER上发布的公告所允许的对武装部队人员的使用和披露目的相同。

(2) 国家安全和情报活动。受保护实体可以向授权的联邦官员披露受保护健康信息，用于开展《国家安全法》(50 U.S.C.401,等)及实施授权(例如，第12333号行政命令)所授权的合法情报、反情报和其他国家安全活动。

(3) 总统及其他人员的保护服务。受保护实体可以向授权的联邦官员披露受保护健康信息，用于向总统或18 U.S.C.3056授权的其他人员、或外国国家元首或22 U.S.C.2709(a)(3)授权的其他人员提供保护服务，或用于开展18 U.S.C.871和879授权的调查。

(4) 医疗适用性判定。
作为国务院组成部分的受保护实体可以使用受保护健康信息进行医疗适宜性判定，并可以向需要访问此类信息的国务院官员披露个人是否被判定为医疗适宜，用于以下目的：

(i) 为根据第10450号和第12968号行政命令进行的所需安全审查之目的；

(ii) 为根据《外交服务法》第101(a)(4)条和第504条确定全球可用性或海外强制服务可用性所必需；或

(iii) 对于一个家庭要陪伴一个根据《外交服务法》第101(b)(5)和904条，海外外交服务成员；

(5) 惩教机构及其他执法羁押情形 - (i) 允许的披露。受保护实体可向对囚犯或其他个人拥有合法羁押权的惩教机构或执法官员披露有关该囚犯或个人的受保护健康信息，前提是该惩教机构或该执法官员表示此类受保护健康信息对于以下目的是必要的：

(A)向此类个人提供医疗保健；

(B)该人员或其他囚犯的健康与安全；

(C) The health and safety of the officers or employees of or others at the correctional institution;

(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

(E) Law enforcement on the premises of the correctional institution; or

(F) The administration and maintenance of the safety, security, and good order of the correctional institution.

(ii) *Permitted uses.* A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.

(iii) *No application after release.* For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

(6) *Covered entities that are government programs providing public benefits.* (i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

(7) *National Instant Criminal Background Check System.* A covered entity may use or disclose protected health information for purposes of reporting to the National Instant Criminal Background Check System the identity of an individual who is prohibited from possessing a firearm under 18 U.S.C. 922(g)(4), provided the covered entity:

(i) Is a State agency or other entity that is, or contains an entity that is:

(A) An entity designated by the State to report, or which collects information for purposes of reporting, on behalf of the State, to the National Instant Criminal Background Check System; or

(B) A court, board, commission, or other lawful authority that makes the commitment or adjudication that causes an individual to become subject to 18 U.S.C. 922(g)(4); and

(ii) Discloses the information only to:

(A) The National Instant Criminal Background Check System; or

(B) An entity designated by the State to report, or which collects information for purposes of reporting, on behalf of the State, to the National Instant Criminal Background Check System; and

(iii)(A) Discloses only the limited demographic and certain other information needed for purposes of reporting to the National Instant Criminal Background Check System; and

(B) Does not disclose diagnostic or clinical information for such purposes.

(l) *Standard: Disclosures for workers' compensation.* A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5699, Jan. 25, 2013; 78 FR 34266, June 7, 2013; 81 FR 395, Jan. 6, 2016; 89 FR 33064, Apr. 26, 2024]

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

(a) *Standard: De-identification of protected health information.* Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify

(C) 惩教机构官员或雇员或其他人员的健康与安全；

(D) 此类个人及负责运送囚犯或将其从一个机构、设施或场所转移至另一机构、设施或场所的官员或其他人员的健康与安全；

(E)惩教机构场所内的执法活动；或

(F) 惩教机构的安全、安保及良好秩序的行政管理和维护。

(ii) 允许的使用。作为惩教机构的受保护实体可将囚犯个人的受保护健康信息用于此类受保护健康信息可被披露的任何目的。

(iii) 释放后不适用。就本条款而言，个人在假释、缓刑、监督释放或以其他方式不再处于合法羁押状态时，即不再属于囚犯。

(6) 提供公共福利的政府计划的受保护实体。(i) 作为提供公共福利的政府计划的健康计划，可将与该健康计划的资格或参保有关的受保护健康信息披露给管理提供公共福利的政府计划的另一机构，前提是此类政府机构之间共享资格或参保信息，或在此类所有政府机构均可访问的单一或合并数据系统中维护此类信息，是法规或规章所要求或明确授权的。

(ii) 作为政府机构管理提供公共福利的政府项目的受保护实体，可以向另一个作为政府机构管理提供公共福利的政府项目的受保护实体披露与该政府项目相关的受保护健康信息，前提是这些项目服务于相同或相似的人群，且披露受保护健康信息对于协调此类项目的受保护功能或改善与此类项目受保护功能相关的行政和管理是必要的。

(7) 国家即时犯罪背景调查系统。受保护实体

可以为向国家即时犯罪背景调查系统报告根据18 U.S.C.922(g)(4)被禁止持有枪支的个人身份的目的使用或披露受保护健康信息，前提是受保护实体：

(i) 是州机构或其他实体，且该实体是或包含以下实体：

(A) 由州指定代表州向国家即时犯罪背景调查系统报告或为此目的收集信息的实体；或

(B) 作出导致个人受18 U.S.C.922(g)(4)约束的拘禁或裁决的法院、委员会、专门小组或其他合法机构；以及

(ii) 仅向以下对象披露信息：(A) 国家即时犯罪背景调查系统；或

(B) 由州指定代表州向国家即时犯罪背景调查系统报告或为此目的收集信息的实体；以及

(iii)(A) 仅披露向国家即时犯罪背景调查系统报告所需的有限人口统计信息和某些其他信息；以及

(B) 不为上述目的披露诊断或临床信息。

(l) 标准：工伤赔偿披露。受保护实体可按照与工伤赔偿或其他类似项目(由法律规定，为与工作相关的伤害或疾病提供无过错福利)相关法律的授权并在遵守该法律所必需的范围内披露受保护健康信息。

[65 FR 82802,2000年12月28日，经67 FR 53270,2002年8月14日；78 FR 5699,2013年1月25日；78 FR 34266,2013年6月7日；81 FR 395,2016年1月6日；89 FR 33064,2024年4月26日修订]

164.514 其他相关要求

用于受保护健康信息的使用与披露。

(a) 标准：受保护健康信息的去标识化。不识别个人且没有合理依据认为该信息可用于识别个人的健康信息

an individual is not individually identifiable health information.

(b) *Implementation specifications: Requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(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 the Census:

(*1*) The geographic unit 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 an 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

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(c) *Implementation specifications: Re-identification.* A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

(1) *Derivation.* The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(2) *Security.* The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

(d)(1) *Standard: minimum necessary requirements.* In order to comply with §164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.

(2) *Implementation specifications: Minimum necessary uses of protected health information.* (i) A covered entity must identify:

(A) Those persons or classes of persons, as appropriate, in its workforce

个人不是可单独识别的健康信息。

(b) 实施规范：受保护健康信息去标识化的要求。受保护实体仅在以下情况下方可确定健康信息不属于可单独识别的健康信息：

(1) 具备适当知识和经验、熟悉公认的统计和科学原则与方法以使信息无法单独识别的人员：

(i) 应用此类原则和方法，确定信息被预期接收者单独使用或与其他合理可获得的信息结合使用以识别作为信息主体的个人的风险非常小；以及

(ii) 记录支持该判定的分析方法和结果；或

(2)(i) 删除以下个人或个人的亲属、雇主或家庭成员标识符：

(A) 姓名；

(B) 所有小于州的地理分区，包括街道地址、城市、县、辖区、邮政编码及其等效地理代码，但以下情况除外：根据人口普查局当前公开可用的数据，邮政编码的前三位数字：

(1) 将所有具有相同前三位数字的邮政编码合并形成的地理单元包含超过20,000人；以及

(2) 所有此类包含20,000人或以下人口的地理单元的邮政编码前三位数字改为000。

(C) 与个人直接相关的日期的所有要素(年份除外)，包括出生日期、入院日期、出院日期、死亡日期；以及所有超过89岁的年龄和表明该年龄的所有日期要素(包括年份)，但此类年龄和要素可汇总为90岁或以上的单一类别；

(D) 电话号码；

(E) 传真号码；

(F) 电子邮件地址；(G) 社会安全号码；(H) 病历号码；

(I) 健康计划受益人编号；

(J) 账号；

(K) 证书/许可证编号；

(L) 车辆标识符和序列号，包括车牌号；

(M) 设备标识符和序列号；

(N) Web 通用资源定位符 (URLs);

(O)互联网协议(IP)地址号码；

(P)生物识别标识符，包括指纹和声纹；

(Q)全脸照片图像及任何可比图像；以及

(R) 任何其他唯一识别号码、特征或代码，但本条(c)款允许的除外；以及

(ii) 受保护实体没有实际知识表明该信息可单独使用或与其他信息结合使用以识别作为信息主体的个人。

(c) 实施规范：重新识别。受保护实体可分配代码或其他记录识别方式，以允许受保护实体重新识别根据本条去标识化的信息，前提是：

(1) 派生。该代码或其他记录识别方式并非派生自或关联于有关个人的信息，且不能以其他方式被转换以识别该个人；以及

(2) 安全。受保护实体不得将代码或其他记录识别方式用于任何其他目的，且不得披露重新识别机制。

(d)(1) 标准：最低必要要求。为遵守164.502(b)和本条，受保护实体在请求、使用和披露受保护健康信息方面必须满足本条(d)(2)至(d)(5)款的要求。

(2) 实施规范：受保护健康信息的最小必要使用。(i) 受保护实体必须确定：

(A) 其工作人员中适当的那些人员或人员类别

who need access to protected health information to carry out their duties; and

(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

(3) *Implementation specification: Minimum necessary disclosures of protected health information.* (i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must:

(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(A) Making disclosures to public officials that are permitted under §164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(B) The information is requested by another covered entity;

(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(D) Documentation or representations that comply with the applicable requirements of §164.512(i) have been provided by a person requesting the information for research purposes.

(4) *Implementation specifications: Minimum necessary requests for protected health information.* (i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii) For all other requests, a covered entity must:

(A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(5) *Implementation specification: Other content requirement.* For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

(e)(1) *Standard: Limited data set.* A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.

(2) *Implementation specification: Limited data set:* A limited data set is protected health information that excludes the following direct identifiers

需要访问受保护健康信息以履行职责的人员；以及

(B) 对于每个此类人员或人员类别，确定需要访问的受保护健康信息类别以及适用于此类访问的任何条件。

(ii) 受保护实体必须做出合理努力，将本条(d)(2)(i)(A)款所确定的人员或类别的访问限制在与本条(d)(2)(i)(B)款一致的受保护健康信息范围内。

(3) 实施规范：受保护健康信息的最小必要披露。(i) 对于受保护实体以常规和反复方式进行的任何类型的披露，受保护实体必须实施政策和程序(可以是标准协议)，将披露的受保护健康信息限制在实现披露目的合理必要的范围内。

(ii) 对于所有其他披露，受保护实体必须：

(A) 制定旨在将披露的受保护健康信息限制在完成寻求披露之目的合理必要的信息范围内的标准；以及

(B) 根据此类标准逐案审查披露请求。

(iii) 在以下情况下，如果此种依赖在具体情形下是合理的，受保护实体可以依赖所请求的披露作为所述目的的最小必要信息：

(A) 向164.512允许的公共官员进行披露，如果该公共官员表示所请求的信息是所述目的的最低必要；

(B)该信息由另一受保护实体请求；

(C) 信息是由作为其工作人员成员的专业人员或受保护实体的业务伙伴为向受保护实体提供专业服务而请求的，前提是该专业人员声明所请求的信息是所述目的的最小必要信息；或

(D) 为研究目的请求信息的人已提供符合164.512(i)适用要求的文件或声明。

(4) 实施规范：受保护健康信息的最小必要请求。(i) 当向其他受保护实体请求受保护健康信息时，受保护实体必须将任何请求限制在完成请求目的合理必要的信息范围内。

(ii) 对于以常规和反复方式提出的请求，受保护实体必须实施政策和程序(可以是标准协议)，将请求的受保护健康信息限制在完成请求目的合理必要的范围内。

(iii) 对于所有其他请求，受保护实体必须：

(A) 制定旨在将受保护健康信息请求限制在完成请求目的合理必要的信息范围内的标准；以及

(B) 根据此类标准逐案审查披露请求。

(5) 实施规范：其他内容要求。对于本节(d)段要求适用的所有使用、披露或请求，受保护实体不得使用、披露或请求整个医疗记录，除非整个医疗记录被特别证明为合理完成使用、披露或请求目的所需的范围。

(e)(1) 标准：有限数据集。受保护实体可以使用或披露符合本条(e)(2)和(e)(3)款要求的有限数据集，前提是受保护实体按照本条(e)(4)款与有限数据集接收方签订数据使用协议。

(2) 实施规范：有限数据集：有限数据集是排除以下直接标识符的受保护健康信息

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; and
(xvi) Full face photographic images and any comparable images.

(3) *Implementation specification: Permitted purposes for uses and disclosures.* (i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.

(ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.

(4) *Implementation specifications: Data use agreement*—(i) *Agreement required.* A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.

(ii) *Contents.* A data use agreement between the covered entity and the limited data set recipient must:

(A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;

(B) Establish who is permitted to use or receive the limited data set; and

(C) Provide that the limited data set recipient will:

(*1*) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

(*2*) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

(*3*) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

(*4*) Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

(*5*) Not identify the information or contact the individuals.

(iii) *Compliance.* (A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(1) Discontinued disclosure of protected health information to the recipient; and

(2) Reported the problem to the Secretary.

(B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.

个人或个人的亲属、雇主或家庭成员：

(i) 姓名；
(ii) 邮政地址信息，但镇或城市、州和邮政编码除外；

(iii) 电话号码；(iv) 传真号码；(v) 电子邮件地址；(vi) 社会安全号码；(vii) 病历号码；(viii) 健康计划受益人号码；

(ix) 账号；(x) 证书/许可证号码；(xi) 车辆标识符和序列号，包括车牌号码；

(十二) 设备标识符和序列号；

(xiii) 网络通用资源定位符(URL);

(xiv) 互联网协议(IP)地址号码；

(xv) 生物识别标识符，包括指纹和声纹；以及

(十六) 全脸照片图像及任何可比图像。

(3) 实施规范：使用和披露的允许目的。(i) 受保护实体仅可为研究、公共卫生或医疗保健运营目的使用或披露本节(e)(1)段下的有限数据集。

(ii) 受保护实体可以使用受保护健康信息创建符合本条(e)(2)款要求的有限数据集，或仅为该目的向业务伙伴披露受保护健康信息，无论该有限数据集是否将由受保护实体使用。

(4) 实施规范：数据使用协议-(i) 需要协议。受保护实体只有在以符合本节要求的数据使用协议形式获得满意保证，即有限数据集接收方仅将为有限目的使用或披露受保护健康信息时，方可使用或披露本条(e)(1)款下的有限数据集。

(ii) 内容。受保护实体与有限数据集接收方之间的数据使用协议必须：

(A) 确立有限数据集接收方对此类信息的允许使用和披露，与本条(e)(3)款一致。数据使用协议不得授权有限数据集接收方以如果由受保护实体实施将违反本子部分要求的方式使用或进一步披露信息；

(B)确定谁被允许使用或接收有限数据集；以及

(C) 规定有限数据集接收方将：

(1)不得以数据使用协议允许或法律另有要求之外的方式使用或进一步披露信息；

(2)使用适当保障措施防止以数据使用协议规定之外的方式使用或披露信息；

(3)向受保护实体报告其知悉的任何非数据使用协议所规定的信息使用或披露；

(4)确保其向其提供有限数据集的任何代理人均同意适用于有限数据集接收方对此类信息的相同限制和条件；以及

(5) 不识别信息或联系个人。

(iii) 合规。(A) 如果受保护实体知悉有限数据集接收方存在构成重大违反或违背数据使用协议的活动或做法模式，则受保护实体不符合本条(e)款的标准，除非受保护实体采取合理步骤纠正违约或终止违规行为(视情况而定)，且如果此类步骤不成功：

(1)停止向接收方披露受保护健康信息；以及

(2) 已向部长报告该问题。

(B) 作为有限数据集接收方并违反数据使用协议的受保护实体将不符合本条(e)款的标准、实施规范和

(f) *Fundraising communications*—(1) *Standard: Uses and disclosures for fundraising.* Subject to the conditions of paragraph (f)(2) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of §164.508:

(i) Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;

(ii) Dates of health care provided to an individual;

(iii) Department of service information;

(iv) Treating physician;

(v) Outcome information; and

(vi) Health insurance status.

(2) *Implementation specifications: Fundraising requirements.* (i) A covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by §164.520(b)(1)(iii)(A) is included in the covered entity's notice of privacy practices.

(ii) With each fundraising communication made to an individual under this paragraph, a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

(iii) A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

(iv) A covered entity may not make fundraising communications to an individual under this paragraph where the individual has elected not to receive such communications under paragraph (f)(2)(ii) of this section.

(v) A covered entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

(g) *Standard: Uses and disclosures for underwriting and related purposes.* If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such protected health information for such purpose or as may be required by law, subject to the prohibition at §164.502(a)(5)(i) with respect to genetic information included in the protected health information.

(h)(1) *Standard: Verification requirements.* Prior to any disclosure permitted by this subpart, a covered entity must:

(i) Except with respect to disclosures under §164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and

(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.

(2) *Implementation specifications: Verification*—(i) *Conditions on disclosures.* If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

(A) The conditions in §164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(B) The documentation required by §164.512(i)(2) may be satisfied by one or more written statements, provided

(f) 筹款通讯 -(1)
标准：用于筹款的利用和披露。在符合本节第(f)(2)段条件的前提下，受保护实体可为自身利益筹集资金的目的，使用或向业务伙伴或机构相关基金会披露以下受保护健康信息，无需符合164.508要求的授权：

(i) 与个人相关的人口统计信息，包括姓名、地址、其他联系信息、年龄、性别和出生日期；

(ii) 向个人提供医疗保健的日期；

(iii) 服务信息部门；

(iv) 主治医师；(v) 结果信息；以及(vi) 健康保险状态。

(2) 实施规范：
筹款要求。(i) 受保护实体不得以本节第(f)(1)段另行允许的筹款目的使用或披露受保护健康信息，除非受保护实体的隐私实践通知中包含164.520(b)(1)(iii)(A)要求的声明。

(ii) 对于根据本段向个人进行的每一次筹款通信，受保护实体必须向该个人提供明确且显著的机会，使其可以选择不再接收任何进一步的筹款通信。个人选择不再接收进一步筹款通信的方法不得导致该个人承担不当负担或超过名义成本。

(iii) 受保护实体不得以个人在接收筹款通信方面的选择作为治疗或付款的条件。

(iv) 如果个人已根据段落选择不接收此类通信，受保护实体不得根据本段向该个人进行筹款通信

(2) (ii) 本节。
(f)
(v) 受保护实体可以向已选择不再接收进一步筹款通信的个人提供一种重新选择接收此类通信的方法。

(g) 标准：承保及相关目的的利用与披露。如果健康计划为承保、保费评级或与健康保险或健康福利合同的订立、续签或替换相关的其他活动之目的接收受保护健康信息，且此类健康保险或健康福利未与该健康计划达成安排，则该健康计划仅可为该目的或法律要求的目的利用或披露此类受保护健康信息，但须遵守164.502(a)(5)(i)中关于受保护健康信息中所含遗传信息的禁止规定。

(h)(1) 标准：验证要求。在本子部分允许的任何披露之前，受保护实体必须：

(i) 除164.510下的披露外，如果受保护实体不知道请求受保护健康信息的人的身份或该人的任何此类权限，则核实请求受保护健康信息的人的身份以及该人根据本子部分访问受保护健康信息的权限；以及

(ii) 当根据本子部分，此类文件、声明或陈述是披露的条件时，从请求受保护健康信息的人处获取任何文件、声明或陈述，无论是口头还是书面形式。

(2) 实施规范：
核实 - (i) 披露条件。如果本子部分以请求受保护健康信息的人提供特定文件、声明或陈述为披露条件，受保护实体在情况下合理的情况下，可依赖表面上符合适用要求的文件、声明或陈述。

(A)164.512(f)(1)(ii)(C)中的条件可通过行政传票或类似程序或通过单独的书面声明满足，该声明表面上证明适用要求已满足。

(B)164.512(i)(2)要求的文件可通过一份或多份书面声明满足，前提是

that each is appropriately dated and signed in accordance with §164.512(i)(2)(i) and (v).

(ii) *Identity of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(B) If the request is in writing, the request is on the appropriate government letterhead; or

(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii) *Authority of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv) *Exercise of professional judgment.* The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with §164.510 or acts on a good faith belief in making a disclosure in accordance with §164.512(j).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5700, Jan. 25, 2013; 78 FR 34266, June 7, 2013]

§164.520 Notice of privacy practices for protected health information.

(a) *Standard: Notice of privacy practices*—(1) *Right to notice.* Except as provided by paragraph (a)(3) or (4) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) *Notice requirements for covered entities creating or maintaining records subject to 42 U.S.C. 290dd-2.* As provided in 42 CFR 2.22, an individual who is the subject of records protected under 42 CFR part 2 has a right to adequate notice of the uses and disclosures of such records, and of the individual's rights and the covered entity's legal duties with respect to such records.

(3) *Exception for group health plans.* (i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or

(B) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in §164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and

(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.

(iii) A group health plan that provides health benefits solely through an

每份声明均按照164.512(i)(2)(i)和(v)适当注明日期并签署。

(ii) 公职人员身份。当向公职人员或代表公职人员行事的人披露受保护健康信息时，受保护实体在情况下合理的情况下，可依赖以下任何一项来核实身份：

(A) 如果请求是当面提出的，出示机构身份徽章、其他官方凭证或其他政府身份证明；

(B) 如果请求是书面的，请求应使用适当的政府信头；或

(C) 如果披露对象是代表公职人员行事的人，则需提供使用适当政府信头的书面声明，说明该人是在政府授权下行事，或其他机构证据或文件，如服务合同、谅解备忘录或采购订单，证明该人代表公职人员行事。

(iii) 公职人员的权限。当受保护健康信息的披露对象是公职人员或代表公职人员行事的人时，受保护实体可以依赖以下任何一项来验证权限，如果此种依赖在情况下是合理的：

(A) 关于请求信息所依据的法律权限的书面声明，或者，如果书面声明不可行，则为此类法律权限的口头声明；

(B) 如果请求是根据大陪审团或司法或行政法庭发出的法律程序、令状、传票、命令或其他法律程序提出的，则推定为构成法律权限。

(iv) 专业判断的行使。
如果覆盖实体依赖专业判断的行使，根据 164.512(j)基于善意信念进行披露，则满足本段的验证要求。

[65 FR 82802,2000年12月28日，经67 FR 53270,2002年8月14日；78 FR 5700,2013年1月25日；78 FR 34266,2013年6月7日修订]

164.520 隐私惯例通知
用于受保护健康信息。

(a) 标准：隐私实践通知 - (1) 通知权。除本节第(a)(3)或(4)段规定外，个人有权获得受保护实体可能进行的受保护健康信息利用和披露的充分通知，以及个人权利和受保护实体在受保护健康信息方面的法律义务。

(2) 创建或维护受*42 U.S.C.290dd-2*约束记录的受保护实体的通知要求。根据42 CFR 2.22规定，作为受42 CFR第2部分保护记录主体的个人有权获得此类记录的利用和披露的充分通知，以及个人权利和受保护实体在此类记录方面的法律义务。

(3) 团体健康计划的例外。(i) 参加团体健康计划的个人有权获得通知：

(A) 从团体健康计划中，如果且在此范围内，该个人未通过与健康保险发行机构或HMO的保险合同在团体健康计划下获得健康福利；或

(B) 从健康保险发行机构或HMO处，就团体健康计划而言，该个人通过该团体健康计划获得健康福利。

(ii) 仅通过与健康保险发行机构或HMO的保险合同提供健康福利的团体健康计划，并且除164.504(a)定义的摘要健康信息或关于个人是否参与团体健康计划、或是否注册或已退出计划提供的健康保险发行机构或HMO的信息外，还创建或接收受保护健康信息的，必须：

(A)根据本节规定维护一份通知；以及

(B) 应任何人的请求提供此类通知。本节(c)(1)段的规定不适用于此类团体健康计划。

(iii) 仅通过以下方式提供健康福利的团体健康计划

insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in §164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.

(4) *Exception for inmates.* An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.

(b) *Implementation specifications: Content of notice*—(1) *Required elements.* The covered entity, including any covered entity receiving or maintaining records subject to 42 U.S.C. 290dd-2, must provide a notice that is written in plain language and that contains the elements required by this paragraph.

(i) *Header.* The notice must contain the following statement as a header or otherwise prominently displayed:

''THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.''

(ii) *Uses and disclosures.* The notice must contain:

(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.

(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization.

(C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, such as 42 CFR part 2, the description of such use or disclosure must reflect the more stringent law as defined in §160.202 of this subchapter.

(D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law, such as 42 CFR part 2.

(E) A description of the types of uses and disclosures that require an authorization under §164.508(a)(2)–(a)(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization as provided by §164.508(b)(5).

(F) A description, including at least one example, of the types of uses and disclosures prohibited under §164.502(a)(5)(iii) in sufficient detail for an individual to understand the prohibition.

(G) A description, including at least one example, of the types of uses and disclosures for which an attestation is required under §164.509.

(H) A statement adequate to put the individual on notice of the potential for information disclosed pursuant to this subpart to be subject to redisclosure by the recipient and no longer protected by this subpart

(iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) or (B) of this section must include a separate statement informing the individual of such activities, as applicable:

(A) In accordance with §164.514(f)(1), the covered entity may contact the individual to raise funds for the covered entity and the individual has a right to opt out of receiving such communications;

(B) In accordance with §164.504(f), the group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan;

(C) If a covered entity that is a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of *health plan*, intends to use or disclose

与健康保险发行机构或HMO签订的保险合同，并且除164.504(a)所定义的汇总健康信息或关于个人是否参与团体健康计划、或是否已加入或已退出该计划所提供的健康保险发行机构或HMO的信息之外，不创建或接收受保护健康信息的，无需维护或提供本节所要求通知。

(4) 囚犯例外。囚犯无权根据本节获得通知，本节的要求不适用于作为受保护实体的惩教机构。

(b) 实施规范：通知内容--(1) 必需要素。受保护实体，包括任何接收或维护受42 U.S.C.290dd-2约束的记录的受保护实体，必须提供以平实语言书写的通知，且该通知包含本段所要求的要素。

(i) 标题。通知必须包含以下声明作为标题或以其他方式显著展示：

"本通知描述您的医疗信息可能如何被使用和披露，以及您如何获取这些信息。请仔细阅读。"

(ii) 使用与披露。通知必须包含：

(A) 对受保护实体根据本子部分允许为以下每个目的进行的利用和披露类型的描述，包括至少一个示例：治疗、支付和医疗保健运营。

(B) 对受保护实体根据本子部分允许或要求未经个人书面授权使用或披露受保护健康信息的其他每个目的的描述。

(C) 如果本节(b)(1)(ii)(A)或(B)段所述任何目的的利用或披露被其他适用法律(如42 CFR part 2)禁止或实质性限制，则对此类利用或披露的描述必须反映本子章160.202定义的更严格法律。

(D) 对于本节(b)(1)(ii)(A)或(B)段所述的每个目的，描述必须包含足够的细节，以使个人注意到本子部分和其他适用法律(如42 CFR part 2)允许或要求的利用和披露。

(E) 对依据 164.508(b)(5)的规定撤销授权。

(F) 对164.502(a)(5)(iii)下禁止的利用和披露类型的描述，包括至少一个示例，细节足够个人理解该禁止。

(G) 对根据164.509需要证明的利用和披露类型的描述，包括至少一个示例。

(H) 足以使个人注意到根据本子部分披露的信息可能被接收者再披露且不再受本子部分保护的声明。

(iii) 特定使用或披露的单独声明。受保护实体若打算从事以下任何活动，本节第(b)(1)(ii)(A)或(B)段所要求的描述必须包含单独声明，酌情告知个人此类活动：

(A) 根据164.514(f)(1)，受保护实体可以联系个人为受保护实体筹集资金，且个人有权选择不接收此类通信；

(B) 根据164.504(f)，团体健康计划，或就团体健康计划而言的健康保险发行机构或HMO，可以向计划发起人披露受保护健康信息；

(C) 如果作为健康计划的受保护实体，不包括属于健康计划定义第(1)(viii)段范围内的长期护理保单发行机构，打算使用或披露

protected health information for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing protected health information that is genetic information of an individual for such purposes;

(D) Substance use disorder treatment records received from programs subject to 42 CFR part 2, or testimony relaying the content of such records, shall not be used or disclosed in civil, criminal, administrative, or legislative proceedings against the individual unless based on written consent, or a court order after notice and an opportunity to be heard is provided to the individual or the holder of the record, as provided in 42 CFR part 2. A court order authorizing use or disclosure must be accompanied by a subpoena or other legal requirement compelling disclosure before the requested record is used or disclosed; or

(E) If a covered entity that creates or maintains records subject to 42 CFR part 2 intends to use or disclose such records for fundraising for the benefit of the covered entity, the individual must first be provided with a clear and conspicuous opportunity to elect not to receive any fundraising communications.

(iv) *Individual rights.* The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by §164.522(a), including a statement that the covered entity is not required to agree to a requested restriction, except in case of a disclosure restricted under §164.522(a)(1)(vi);

(B) The right to receive confidential communications of protected health information as provided by §164.522(b), as applicable;

(C) The right to inspect and copy protected health information as provided by §164.524;

(D) The right to amend protected health information as provided by §164.526;

(E) The right to receive an accounting of disclosures of protected health information as provided by §164.528; and

(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.

(v) *Covered entity's duties.* The notice must contain:

(A) A statement that the covered entity is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices, and to notify affected individuals following a breach of unsecured protected health information;

(B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and

(C) For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with §164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.

(vi) *Complaints.* The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.

(vii) *Contact.* The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by §164.530(a)(1)(ii).

(viii) *Effective date.* The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

(2) *Optional elements.* (i) In addition to the information required by paragraph (b)(1) of this section, if a covered entity

为承保目的使用受保护健康信息时，声明受保护实体被禁止为此类目的使用或披露属于个人遗传信息的受保护健康信息；

164.528 所提供的信息；以及

(D) 从受42 CFR part 2约束的项目收到的物质使用障碍治疗记录，或转述此类记录内容的证词，不得在针对个人的民事、刑事、行政或立法程序中使用或披露，除非基于书面同意，或根据42 CFR part 2的规定，在向个人或记录持有人提供通知和听证机会后作出的法院命令。授权使用或披露的法院命令必须附有传票或其他强制披露的法律要求，然后才能使用或披露所请求的记录；或

(F) 个人(包括已同意按本节第(c)(3)段以电子方式接收通知的个人)有权应请求从受保护实体获得通知的纸质副本。

(v) 受保护实体的义务。通知必须包含：

(A) 声明：受保护实体依法须维护受保护健康信息的隐私，向个人提供其法律义务和隐私实践的通知，并在发生未受保护健康信息泄露后通知受影响的个人；

(B) 声明：受保护实体须遵守当前有效通知的条款；以及

(C) 为使受保护实体将通知中所述的隐私实践变更适用于受保护实体在发布修订通知之前创建或接收的受保护健康信息，根据164.530(i)(2)(ii)，需提供声明，表明其保留更改通知条款的权利，并使新通知条款对其维护的所有受保护健康信息生效。该声明还必须描述其将如何向个人提供修订通知。

(E) 如果创建或维护受42 CFR part 2约束的记录之受保护实体，打算为受保护实体的利益使用或披露该等记录以进行筹款，必须首先向个人提供清晰且醒目的机会，使其选择不接收任何筹款通讯。

(iv) 个人权利。通知必须包含关于个人对受保护健康信息所享权利的声明，以及个人如何行使这些权利的简要说明，具体如下：

(A) 依据 164.522(a)(1)(vi)受到限制的披露；

(vi) 投诉。通知必须包含声明：如果个人认为其隐私权受到侵犯，可以向受保护实体和部长投诉；简要说明个人如何向受保护实体提出投诉；以及声明：个人不会因提出投诉而遭到报复。

(B) 按164.522(b)规定(如适用)，接收受保护健康信息保密通讯的权利；

(vii) 联系方式。通知必须包含按164.530(a)(1)(ii)要求可供联系以获取进一步信息的人员或办公室的姓名或职务以及电话号码。

(C) 按164.524规定，查阅和复制受保护健康信息的权利；

(viii) 生效日期。通知必须包含通知首次生效的日期，该日期不得早于通知打印或以其他方式发布的日期。

(D)根据164.526规定享有的修改受保护健康信息的权利；

(E)有权获得受保护健康信息披露记录的权利

(2) 可选要素。(i) 除本节第(b)(1)段要求的信息外，如果受保护实体

elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by §164.512(j)(1)(i).

(ii) For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with §164.530(i)(2)(ii), the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.

(3) *Revisions to the notice.* The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

(c) *Implementation specifications: Provision of notice.* A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.

(1) *Specific requirements for health plans.* (i) A health plan must provide the notice:

(A) No later than the compliance date for the health plan, to individuals then covered by the plan;

(B) Thereafter, at the time of enrollment, to individuals who are new enrollees.

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.

(v) If there is a material change to the notice:

(A) A health plan that posts its notice on its web site in accordance with paragraph (c)(3)(i) of this section must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan.

(B) A health plan that does not post its notice on a web site pursuant to paragraph (c)(3)(i) of this section must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.

(2) *Specific requirements for certain covered health care providers.* A covered health care provider that has a direct treatment relationship with an individual must:

(i) Provide the notice:

(A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or

(B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

(ii) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;

(iii) If the covered health care provider maintains a physical service delivery site:

(A) Have the notice available at the service delivery site for individuals to request to take with them; and

选择限制其根据本子部分被允许进行的使用或披露，受保护实体可以在其通知中描述其更有限的使用或披露，但受保护实体不得在其通知中包含影响其进行法律要求或164.512(j)(1)(i)允许的使用或披露的权利的限制。

(ii) 为使受保护实体按164.530(i)(2)(ii)将其更有限的使用和披露变更适用于发布修订通知之前创建或接收的受保护健康信息，通知必须包含本节第(b)(1)(v)(C)段所要求的声明。

(3) 通知的修订。每当通知中所述的使用或披露、个人权利、受保护实体的法律义务或其他隐私实践发生重大变更时，受保护实体必须及时修订并分发其通知。除法律要求外，通知任何条款的重大变更不得在反映该重大变更的通知生效日期之前实施。

(c) 实施规范：提供通知。受保护实体必须应任何人的请求提供本节所要求的通知，并按本节第(c)(1)至(c)(3)段的规定(如适用)向个人提供。

(1) 对健康计划的具体要求。(i) 健康计划必须提供通知：

(A) 不迟于健康计划的合规日期，向当时受该计划覆盖的个人提供；

(B) 此后，在参保时向新参保个人提供。

(ii) 健康计划必须至少每三年一次通知当时受该计划覆盖的个人通知的可获得性以及如何获取通知。

(iii) 如果向保单的记名被保险人提供通知，且该保单为记名被保险人及一名或多名受抚养人提供覆盖，则健康计划满足本节第(c)(1)段的要求。

(iv) 如果健康计划有不止一份通知，则其满足以下要求：通过提供与个人或其他请求通知的人相关的通知，满足本节第(c)(1)段的要求。

(v) 如果通知发生重大变更：

(A) 按本节第(c)(3)(i)段在其网站上发布通知的健康计划，必须在通知重大变更生效日期之前，在其网站上显著发布该变更或其修订通知，并在下一次向当时受该计划覆盖的个人年度邮寄时提供修订通知，或关于重大变更及如何获取修订通知的信息。

(B) 未按本节第(c)(3)(i)段在网站上发布通知的健康计划，必须在通知重大修订后60天内向当时受该计划覆盖的个人提供修订通知，或关于重大变更及如何获取修订通知的信息。

(2) 对某些受保护医疗保健提供者的具体要求。与个人有直接治疗关系的受保护医疗保健提供者必须：

(i) 提供通知：

(A) 不迟于受保护医疗保健提供者合规日期后首次向该个人提供服务(包括以电子方式提供的服务)之日；或

(B) 在紧急治疗情况下，在紧急治疗情况后尽快合理可行时。

(ii) 除紧急治疗情况外，尽善意努力获取按本节第(c)(2)(i)段提供的通知之书面接收确认；如果未获取，记录其获取该确认的善意努力以及未获取确认的原因；

(iii) 如果受保护医疗保健提供者维护实体服务提供场所：

(A) 在服务提供场所备有通知，供个人请求带走；以及

(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

(iv) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.

(3) *Specific requirements for electronic notice.* (i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.

(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

(d) *Implementation specifications: Joint notice by separate covered entities.* Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:

(1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;

(2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and

(i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;

(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

(iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.

(3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.

(4) The permission in paragraph (d) of this section for covered entities that participate in an organized health care arrangement to issue a joint notice may not be construed to remove any obligations or duties of entities creating or maintaining records subject to 42 U.S.C. 290dd-2, or to remove any rights of patients who are the subjects of such records.

(e) *Implementation specifications: Documentation.* A covered entity must document compliance with the notice requirements, as required by §164.530(j), by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such

(B) 将通知张贴在清晰且显著的位置，合理预期寻求受保护医疗保健提供者服务的个人能够阅读该通知；以及

(iv) 每当通知被修订时，在修订生效日期当日或之后应请求提供通知，并及时遵守本节第(c)(2)(iii)段的要求(如适用)。

(3) 对电子通知的具体要求。(i) 维护提供有关受保护实体客户服务或福利信息的网站的受保护实体，必须在其网站上显著发布其通知，并通过网站以电子方式提供通知。

(ii) 如果个人同意电子通知且该同意未被撤回，受保护实体可通过电子邮件向个人提供本节要求的通知。如果受保护实体知道电子邮件传输失败，则必须向个人提供通知的纸质副本。当受保护实体按照本节(c)(1)或(2)段及时提供电子通知时，即满足本节(c)段的提供要求。

(iii) 就本段而言本节第(c)(2)(i)段，如果向个人首次服务交付是以电子方式进行的，受保护医疗保健提供者必须响应个人的首次服务请求，自动并同时提供电子通知。本节第(c)(2)(ii)段的要求适用于电子通知。

(iv) 作为电子通知接收者的个人保留应请求从受保护实体获得通知纸质副本的权利。

(d) 实施规范：由多个独立受保护实体发出的联合通知。参与有组织医疗保健安排的受保护实体可通过联合通知遵守本节规定，前提是：

(1) 参与有组织医疗保健安排的受保护实体同意遵守通知条款，该条款涉及由以下各方创建或接收的受保护健康信息：

受保护实体作为其参与有组织医疗保健安排的一部分；

(2) 联合通知符合本节(b)段的实施规范，但本节要求的声明可作修改，以反映该通知涵盖多个受保护实体的事实；以及

(i) 以合理具体的方式描述联合通知适用的受保护实体或实体类别；

(ii) 以合理具体的方式描述联合通知适用的服务提供场所或服务提供场所类别；以及

(iii) 如适用，声明参与有组织医疗保健安排的受保护实体将相互共享受保护健康信息，以执行与有组织医疗保健安排相关的治疗、付款或医疗保健运营所必需。

(3) 联合通知中包含的受保护实体必须按照本节(c)段适用的实施规范向个人提供通知。联合通知中任一受保护实体向个人提供联合通知，即满足本节(c)段对联合通知涵盖的所有其他实体的提供要求。

(4) 本节(d)段对参与有组织医疗保健安排的受保护实体发布联合通知的许可，不得解释为免除创建或维护受42 U.S.C.290dd-2约束的记录之实体的任何义务或职责，也不得解释为免除作为此类记录对象的患者的任何权利。

(e) 实施规范：文档记录。受保护实体必须按照164.530(j)的要求，通过保留该受保护实体发出的通知副本以及(如适用)任何书面收悉确认或获取该等确认的善意努力文档记录，来记录对通知要求的遵守情况。

written acknowledgment, in accordance with paragraph (c)(2)(ii) of this section.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002; 78 FR 5701, Jan. 25, 2013; 89 FR 33064, Apr. 26, 2024]

§ 164.522 Rights to request privacy protection for protected health information.

(a)(1) *Standard: Right of an individual to request restriction of uses and disclosures.* (i) A covered entity must permit an individual to request that the covered entity restrict:

(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and

(B) Disclosures permitted under §164.510(b).

(ii) Except as provided in paragraph (a)(1)(vi) of this section, a covered entity is not required to agree to a restriction.

(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

(v) A restriction agreed to by a covered entity under paragraph (a) of this section, 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.

(vi) A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if:

(A) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and

(B) The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

(2) *Implementation specifications: Terminating a restriction.* A covered entity may terminate a restriction, if:

(i) The individual agrees to or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented; or

(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is:

(A) Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and

(B) Only effective with respect to protected health information created or received after it has so informed the individual.

(3) *Implementation specification: Documentation.* A covered entity must document a restriction in accordance with §160.530(j) of this subchapter.

(b)(1) *Standard: Confidential communications requirements.* (i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.

(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

(2) *Implementation specifications: Conditions on providing confidential communications.* (i) A covered entity may require the individual to make a request

书面确认，依照本节第(c)(2)(ii)款。

[65 FR 82802,2000年12月28日，经67 FR 53271,2002年8月14日；78 FR 5701,2013年1月25日；89 FR 33064,2024年4月26日修订]

164.522 请求隐私的权利

对受保护健康信息的保护。

(a)(1) 标准：个人请求限制使用和披露的权利。(i) 受保护实体必须允许个人请求受保护实体限制：

(A) 为实施治疗、支付或医疗保健运营而使用或披露关于该个人的受保护健康信息；以及

(B) 根据.....允许的披露 164.510(b)。

(ii) 除第款另有规定外本节第(a)(1)(vi)款，受保护实体无需同意限制。

(iii) 同意本节(a)(1)(i)段限制的受保护实体不得违反该限制使用或披露受保护健康信息，但除外情况是，如果请求限制的个人需要紧急治疗，且受限的受保护健康信息是提供紧急治疗所必需的，受保护实体可使用受限的受保护健康信息，或向医疗保健提供者披露此类信息，以为个人提供此类治疗。

(iv) 如果根据本节(a)(1)(iii)段向医疗保健提供者披露受限的受保护健康信息以进行紧急治疗，受保护实体必须要求该医疗保健提供者不得进一步使用或披露该信息。

(v) 受保护实体根据本节(a)段同意的限制，在本子部分下不具有阻止 164.510(a)或164.512允许或要求的使用或披露的效力。

(vi) 在以下情况下，受保护实体必须同意个人提出的限制向健康计划披露关于该个人的受保护健康信息的请求：

(A) 该披露是为了实施支付或医疗保健运营，且法律并无其他要求；以及

(B) 该受保护健康信息仅涉及个人或代表个人的健康计划以外的人已向受保护实体全额支付的医疗保健项目或服务。

(2) 实施规范：终止限制。受保护实体可在以下情况下终止限制：

(i) 个人以书面形式同意或请求终止；

(ii) 个人口头同意终止且该口头同意已记录在案；或

(iii) 受保护实体通知个人其正在终止对限制的同意，但该终止：

(A) 对受段落限制的受保护健康信息无效

(a) (1)(vi) 本节；以及

(B) 仅对在如此通知个人之后创建或接收的受保护健康信息有效。

(3) 实施规范：文档记录。受保护实体必须按照本子章160.530(j)记录限制。

(b)(1) 标准：保密通信要求。(i) 受保护医疗保健提供者必须允许个人提出请求，并必须满足个人通过替代方式或替代地点从该受保护医疗保健提供者接收受保护健康信息通信的合理请求。

(ii) 健康计划必须允许个人提出请求，并且必须满足个人通过替代方式或在替代地点从健康计划接收受保护健康信息通信的合理请求，如果个人明确声明披露全部或部分该信息可能危及该个人。

(2) 实施规范：提供保密通信的条件。(i) 受保护实体可要求个人提出请求

for a confidential communication described in paragraph (b)(1) of this section in writing.

(ii) A covered entity may condition the provision of a reasonable accommodation on:

(A) When appropriate, information as to how payment, if any, will be handled; and

(B) Specification of an alternative address or other method of contact.

(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002; 78 FR 5701, Jan. 25, 2013]

§ 164.524 Access of individuals to protected health information.

(a) *Standard: Access to protected health information*—(1) *Right of access.* Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

(i) Psychotherapy notes; and

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

(2) *Unreviewable grounds for denial.* A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.

(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.

(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(3) *Reviewable grounds for denial.* A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

本节第(b)(1)款所述的保密通信以书面形式。

(ii) 受保护实体可以以以下条件作为提供合理便利的前提：

(A) 在适当情况下，关于如何处理付款(如有)的信息；以及

(B)指定替代地址或其他联系方式。

(iii) 受保护医疗保健提供者不得要求个人解释请求的依据，作为以保密方式提供通信的条件。

(iv) 健康计划可以要求请求中包含一项声明，说明披露该请求所涉全部或部分信息可能危及该个人。

[65 FR 82802,2000年12月28日，经67 FR 53271,2002年8月14日；78 FR 5701,2013年1月25日修订]

164.524 个人获取受保护健康信息

受保护的健康信息。

(a) 标准：获取受保护健康信息 -(1) 访问权。除本节(a)(2)或(a)(3)段另有规定外，个人有权查阅和获取指定记录集中关于该个人的受保护健康信息副本，只要该受保护健康信息保存在指定记录集中，但以下情况除外：

(i) 心理治疗笔记；以及

(ii) 为合理预期或用于民事、刑事或行政诉讼或程序而汇编的信息。

(2) 不可复审的拒绝理由。在以下情况下，受保护实体可拒绝个人访问，且无需向个人提供复审机会。

(i) 该受保护健康信息属于本节(a)(1)段访问权的例外情形。

(ii) 作为惩教机构的受保护实体或在惩教机构指导下行事的受保护医疗服务提供者，可以全部或部分拒绝被监禁者获取受保护健康信息副本的请求，如果获取此类副本将危及该个人或其他被监禁人员的健康、安全、安保、监护或康复，或危及惩教机构内任何官员、雇员或其他人员或负责运送被监禁人员的任何人员的安全。

(iii) 个人对受保护医疗保健提供者在包含治疗的研究过程中创建或获取的受保护健康信息的访问权，可在研究进行期间暂时中止，前提是个人在同意参与包含治疗的研究时已同意拒绝访问，且受保护医疗保健提供者已告知个人，访问权将在研究完成后恢复。

(iv) 个人访问受《隐私法》(5 U.S.C.552a)约束的记录中所含的受保护健康信息，如果根据《隐私法》拒绝访问符合该法律的要求，则可以拒绝。

(v) 如果受保护健康信息是在保密承诺下从非医疗服务提供者处获得的，且所请求的访问合理可能泄露信息来源，则可拒绝个人的访问请求。

(3) 可复审的拒绝理由。在以下情况下，受保护实体可以拒绝个人访问，前提是个人有权按照本节第(a)(4)段的要求对此类拒绝进行复审：

(i) 持证医疗专业人员运用专业判断认定，所请求的访问合理可能危及个人或他人的生命或人身安全；

(ii) 受保护健康信息涉及另一人(除非该另一人为医疗服务提供者)，且持证医疗专业人员运用专业判断认定，所请求的访问合理可能对该另一人造成重大损害；或

(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

(4) *Review of a denial of access.* If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

(b) *Implementation specifications: Requests for access and timely action*—(1) *Individual's request for access.* The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

(2) *Timely action by the covered entity.* (i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.

(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.

(ii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(c) *Implementation specifications: Provision of access.* If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Providing the access requested.* The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

(2) *Form of access requested.* (i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.

(ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

(iii) The covered entity may provide the individual with a summary of the

(iii) 访问请求由个人的个人代表提出，且持证医疗专业人员运用专业判断认定，向该个人代表提供访问合理可能对个人或他人造成重大损害。

(4) 拒绝访问的审查。如果基于本节第(a)(3)段允许的理由拒绝访问，个人有权要求由受保护实体指定作为审查官员且未参与最初拒绝决定的持照医疗保健专业人员对拒绝进行审查。受保护实体必须根据本节第(d)(4)段审查官员的裁定提供或拒绝访问。

(b) 实施规范：访问请求和及时行动-(1) 个人的访问请求。受保护实体必须允许个人请求访问以查阅或获取保存在指定记录集中的关于该个人的受保护健康信息的副本。受保护实体可以要求个人以书面形式提出访问请求，前提是其将此类要求告知个人。

(2) 受保护实体的及时行动。
(i) 除本条(b)(2)(ii)款另有规定外，受保护实体必须在收到请求后不迟于30天内对访问请求采取行动，具体如下。

(A) 如果受保护实体全部或部分批准请求，必须按照本条(c)款告知个人请求已被接受并提供所请求的访问。

(B) 如果受涵盖实体全部或部分拒绝该请求，它必须根据段落向个人提供书面拒绝，

(d) 本节。
(ii) 如果受保护实体无法在本节第(b)(2)(i)段要求的时限内采取本节第(b)(2)(i)(A)或(B)段要求的行动(视情况而定)，受保护实体可将此类行动的时限延长不超过30天，前提是：

(A) 受保护实体在本节第(b)(2)(i)段规定的时限内(视情况而定)，向个人提供书面说明，阐明延迟的原因以及受保护实体将完成对请求行动的日期；以及

(B) 受保护实体对访问请求的行动只能有一次此类延期。

(c) 实施规范：提供访问。如果受保护实体全部或部分向个人提供受保护健康信息的访问，受保护实体必须遵守以下要求。

(1) 提供所请求的访问。受保护实体必须提供个人所请求的访问，包括查阅或获取副本，或两者兼有，涉及指定记录集中关于他们的受保护健康信息。如果作为访问请求对象的同一受保护健康信息保存在多个指定记录集或多个位置，受保护实体只需在响应访问请求时提供一次该受保护健康信息。

(2) 所请求的访问形式。(i) 受保护实体必须以个人请求的形式和格式向个人提供受保护健康信息的访问，如果该信息和格式易于以此种形式和格式生成；否则，以可读的硬拷贝形式或受保护实体与个人约定的其他形式和格式提供。

(ii) 尽管有第
(c)(2)(i) 本节规定，如果访问请求所涉及的受保护健康信息以电子形式保存在一个或多个指定记录集中，且个人请求获取该信息的电子副本，则受保护实体必须以个人请求的电子形式和格式向个人提供受保护健康信息的访问权限(若该信息易于以该形式和格式生成)；若不易生成，则以受保护实体与个人共同商定的可读电子形式和格式提供。

(iii) 受保护实体可向个人提供以下内容的摘要：

protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:

(A) The individual agrees in advance to such a summary or explanation; and

(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(3) *Time and manner of access.* (i) The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

(ii) If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.

(4) *Fees.* If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(i) Labor for copying the protected health information requested by the individual, whether in paper or electronic form;

(ii) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;

(iii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and

(iv) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(iii) of this section.

(d) *Implementation specifications: Denial of access.* If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Making other information accessible.* The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.

(2) *Denial.* The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:

(i) The basis for the denial;

(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and

(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in §164.530(d) or to the Secretary pursuant to the procedures in §160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).

(3) *Other responsibility.* If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

(4) *Review of denial requested.* If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access

所请求的受保护健康信息，以替代提供受保护健康信息的访问权限，或可提供已获访问权限的受保护健康信息的解释，前提是：

(A)个人事先同意此类摘要或解释；以及

(B) 个人事先同意受保护实体为此类摘要或解释收取的费用(如有)。

(3) 访问的时间和方式。(i) 受保护实体必须按照本节第(b)(2)段的要求，及时提供个人所请求的访问，包括与个人安排方便的时间和地点查阅或获取受保护健康信息的副本，或应个人请求邮寄受保护健康信息的副本。受保护实体可以在必要时与个人讨论访问请求的范围、格式和其他方面，以促进及时提供访问。

(ii) 如果个人的访问请求指示受保护实体将受保护健康信息的副本直接传输给个人指定的另一人，受保护实体必须将副本提供给个人指定的人。个人的请求必须为书面形式，由个人签署，并明确标识指定人员以及发送受保护健康信息副本的地点。

(4) 费用。如果个人请求受保护健康信息的副本或同意对此类信息的摘要或解释，受保护实体可以收取合理的、基于成本的费用，前提是该费用仅包括以下成本：

(i) 复制个人请求的受保护健康信息的劳务费用，无论纸质还是电子形式；

(ii) 制作纸质副本或电子介质的用品费用，如果个人请求将电子副本提供在便携式介质上；

(iii) 邮寄费，当个人请求将副本或摘要或解释邮寄时；以及

(iv) 准备受保护健康信息的解释或摘要

经个人同意，按本节第(c)(2)(iii)段的要求。

(d) 实施规范：拒绝访问。若受保护实体全部或部分拒绝访问受保护健康信息，受保护实体必须遵守以下要求。

(1) 使其他信息可访问。
受保护实体必须尽可能向个人提供对任何其他所请求的受保护健康信息的访问权限，但排除受保护实体有理由拒绝访问的受保护健康信息。

(2) 拒绝。受保护实体必须按照本节第(b)(2)段向个人提供及时的书面拒绝。拒绝必须使用通俗语言并包含：

(i) 拒绝的依据；(ii) 如适用，关于个人根据本节第(a)(4)段享有的复审权利的说明，包括个人如何行使此类复审权利的描述；以及

(iii) 关于个人如何根据 160.306的程序向部长投诉的说明。该说明必须包括164.530(a)(1)(ii)中指定的联系人或者办公室的姓名或职务以及电话号码。

(3) 其他责任。如果受保护实体不保存个人访问请求所涉的受保护健康信息，且受保护实体知道所请求信息的保存地点，受保护实体必须告知个人将访问请求指向何处。

(4) 请求的拒绝审查。如果个人已根据本节第(a)(4)段请求对拒绝进行审查，受保护实体必须指定一名未直接参与拒绝的持照医疗保健专业人员来审查拒绝访问的决定。受保护实体必须及时将审查请求转交该指定审查官员。指定审查官员必须在合理时间内确定是否拒绝访问

requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

(e) *Implementation specification: Documentation.* A covered entity must document the following and retain the documentation as required by §164.530(j):

(1) The designated record sets that are subject to access by individuals; and

(2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

[65 FR 82802, Dec. 28, 2000, as amended at 78 FR 5701, Jan. 25, 2013; 78 FR 34266, June 7, 2013; 79 FR 7316, Feb. 6, 2014]

§164.526 Amendment of protected health information.

(a) *Standard: Right to amend.* (1) *Right to amend.* An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) *Denial of amendment.* A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

(i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

(ii) Is not part of the designated record set;

(iii) Would not be available for inspection under §164.524; or

(iv) Is accurate and complete.

(b) *Implementation specifications: Requests for amendment and timely action—*(1) *Individual's request for amendment.* The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

(2) *Timely action by the covered entity.* (i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) *Implementation specifications: Accepting the amendment.* If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Making the amendment.* The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) *Informing the individual.* In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to

根据本节(a)(3)段的标准提出请求。受涵盖实体必须及时向个人提供指定审查官员决定的书面通知，并采取本节要求的其他行动来执行指定审查官员的决定。

(e) 实施规范：文档记录。受保护实体必须记录以下内容，并按照164.530(j)的要求保留文档记录：

(1) 受个人访问权约束的指定记录集；以及

(2) 负责接收和处理个人访问请求的人员或办公室的职务名称。

[65 FR 82802,2000年12月28日，经78 FR 5701,2013年1月25日；78 FR 34266,2013年6月7日；79 FR 7316,2014年2月6日修订]

164.526 受保护信息的修正健康信息。

(a) 标准：修改权。(1) 修改权。个人有权要求受保护实体修改指定记录集中关于该个人的受保护健康信息或记录，只要该受保护健康信息保存在指定记录集中。

(2) 拒绝修改。如果受保护实体认定请求所涉的受保护健康信息或记录符合以下情形，可以拒绝个人的修改请求：

(i) 并非由受保护实体创建，除非个人提供合理依据使人相信受保护健康信息的创建者已不再可用来执行所请求的修改；

(ii) 不属于指定记录集；

(iii) 根据164.524 无法供查阅；或

(iv) 准确且完整。(b) 实施规范：修改请求和及时行动-(1) 个人的修改请求。受保护实体必须允许个人请求受保护实体修改保存在指定记录集中的受保护健康信息。受保护实体可以求个人以书面形式提出修正请求并提供支持请求修正的理由，前提是提前告知个人此类要求。

(2) 受保护实体的及时行动。

(i) 受保护实体必须在收到修正请求后不迟于60天内对个人的修正请求采取行动，具体如下。

(A) 如果受保护实体全部或部分批准所请求的修改，必须采取本节第(c)(1)和(2)段要求的行动。

(B) 如果受保护实体全部或部分拒绝所请求的修正，它必须根据本节第(d)(1)段向个人提供书面拒绝。

(ii) 如果受保护实体无法在本节第(b)(2)(i)段要求的时间内对修正采取行动，受保护实体可将此类行动的时间延长不超过30天，前提是：

(A) 受保护实体在本节第(b)(2)(i)段规定的时限内，向个人提供延迟原因的书面说明以及受保护实体将完成对请求行动的日期；以及

(B) 受保护实体对修正请求的行动只能有一次此类时间延长。

(c) 实施规范：接受修正。如果受保护实体全部或部分接受所请求的修正，受保护实体必须遵守以下要求。

(1) 进行修正。受保护实体必须对作为修正请求对象的受保护健康信息或记录进行适当修正，至少应识别指定记录集中受修正影响的记录，并附加或以其他方式提供指向修正位置的链接。

(2) 通知个人。根据本节第(b)段，受保护实体必须及时通知个人修正已被接受，并获得个人对以下内容的确认和同意

have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) *Informing others.* The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) *Implementation specifications: Denying the amendment.* If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Denial.* The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in §164.530(d) or to the Secretary pursuant to the procedures established in §160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).

(2) *Statement of disagreement.* The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) *Rebuttal statement.* The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) *Recordkeeping.* The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) *Future disclosures.* (i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.

(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required

要求受保护实体根据本节第(c)(3)款通知需要共享该修正的相关人员。

(3) 通知他人。受保护实体必须做出合理努力，在合理时间内通知以下各方并提供修正：

(i) 个人指明的已收到关于该个人的受保护健康信息且需要该修正的人员；以及

(ii) 受保护实体所知拥有作为修正对象的受保护健康信息且可能已经依赖或可预见地依赖此类信息从而对个人造成损害的人员，包括业务伙伴。

(d) 实施规范：拒绝修正。如果受保护实体全部或部分拒绝所请求的修正，受保护实体必须遵守以下要求。

(1) 拒绝。受保护实体必须根据本节第(b)(2)段向个人提供及时的书面拒绝。拒绝必须使用通俗语言并包含：

(i) 根据本节第(a)(2)段的拒绝理由；

(ii) 个人提交书面声明表示不同意该拒绝的权利以及个人如何提交此类声明；

(iii) 一项声明，即如果个人未提交不同意声明，个人可请求受保护实体在今后披露作为修正对象的受保护健康信息时一并提供个人的修正请求和拒绝；以及

(iv) 关于个人如何根据 160.306确立的程序向部长投诉的说明。该说明必须包括164.530(a)(1)(ii)中指定的联系人或办公室的姓名或职务以及电话号码。

(2) 不同意声明。受保护实体必须允许个人向受保护实体提交书面声明，表示不同意对全部或部分所请求修正的拒绝以及此类不同意的依据。受保护实体可合理限制不同意声明的长度。

(3) 反驳声明。受保护实体可准备对个人不同意声明的书面反驳。每当准备此类反驳时，受保护实体必须向提交不同意声明的个人提供副本。

(4) 记录保存。受保护实体必须酌情识别指定记录集中作为争议修正对象的记录或受保护健康信息，并将个人的修正请求、受保护实体对请求的拒绝、个人的不同意声明(如有)以及受保护实体的反驳(如有)附加或以其他方式链接到指定记录集。

(5) 未来披露。(i) 如果个人已提交不同意声明，受保护实体必须在随后披露与该不同意相关的受保护健康信息时，一并包含根据本节第(d)(4)段附加的材料，或经受保护实体选择，包含任何此类信息的准确摘要。

(ii) 如果个人未提交书面不同意声明，则仅当个人已根据本节第(d)(1)(iii)段请求此类行动时，受保护实体才必须在随后披露受保护健康信息时一并包含个人的修正请求及其拒绝，或此类信息的准确摘要。

(iii) 当本节第(d)(5)(i)或(ii)款所述的后续披露使用本子章第162部分下的标准交易进行，而该交易不允许在披露中包含附加材料时，受保护实体可以单独传输本节第(d)(5)(i)或(ii)款(如适用)所要求的材料

by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

(e) *Implementation specification: Actions on notices of amendment.* A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.

(f) *Implementation specification: Documentation.* A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by §164.530(j).

§164.528 Accounting of disclosures of protected health information.

(a) *Standard: Right to an accounting of disclosures of protected health information.* (1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

(i) To carry out treatment, payment and health care operations as provided in §164.506;

(ii) To individuals of protected health information about them as provided in §164.502;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in §164.502;

(iv) Pursuant to an authorization as provided in §164.508;

(v) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in §164.510;

(vi) For national security or intelligence purposes as provided in §164.512(k)(2);

(vii) To correctional institutions or law enforcement officials as provided in §164.512(k)(5);

(viii) As part of a limited data set in accordance with §164.514(e); or

(ix) That occurred prior to the compliance date for the covered entity.

(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in §164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

(A) Document the statement, including the identity of the agency or official making the statement;

(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

(b) *Implementation specifications: Content of the accounting.* The covered entity must provide the individual with a written accounting that meets the following requirements.

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

(2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure:

(i) The date of the disclosure;

(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(iii) A brief description of the protected health information disclosed; and

根据本节(d)(5)(i)或(ii)段（如适用），向标准交易的接收方。

(e) 实施规范：对修正通知的行动。受保护实体在根据本节第(c)(3)段被另一受保护实体告知个人受保护健康信息的修正时，必须按本节第(c)(1)段的规定修正指定记录集中的受保护健康信息。

(f) 实施规范：文档记录。受保护实体必须记录负责接收和处理个人修正请求的人员或办公室的职务，并按164.530(j)的要求保留文档记录。

164.528 披露记录
受保护健康信息。

(a) 标准：获得受保护健康信息披露 *accounting* 的权利。(1) 个人有权获得受保护实体在请求 accounting 之日前六年内所作受保护健康信息披露的 accounting，但以下披露除外：

(i) 按164.506的规定进行治疗、付款和医疗保健运营；

(ii) 按164.502的规定向个人提供关于其本人的受保护健康信息；

(iii) 附随于本子部分另行允许或要求的使用或披露，按164.502的规定；

(iv) 依据164.508 规定的授权；

(v) 用于机构名录或按164.510的规定向参与个人护理的人员或其他通知目的；

(vi) 按164.512(k)(2)的规定用于国家安全或情报目的；

(vii) 按164.512(k)(5)的规定向惩教机构或执法官员披露；

(viii)根据164.514(e)作为有限数据集的一部分；或

(ix) 发生在受保护实体合规日期之前。

(2)(i) 受保护实体必须暂时中止个人获取披露记录的权利，直至

向卫生监督机构或执法官员的披露，如164.512(d)或(f)分别规定，在该机构或官员指定的时间内，如果该机构或官员向受保护实体提供书面声明，说明此类会计记录给个人合理可能导致妨碍该机构的活动，并指明需要此类暂停的时间。

(ii) 如果本节第(a)(2)(i)段所述的机构或官员声明是口头作出的，受保护实体必须：

(A) 记录该声明，包括作出该声明的机构或官员的身份；

(B) 暂时中止个人对受该声明约束的披露进行核算的权利；以及

(C) 将暂时中止的期限限制为自口头声明之日起不超过30天，除非在此期间根据本节第(a)(2)(i)段提交了书面声明。

(3) 个人可以请求对自请求之日起不足六年期间的披露进行核算。

(b) 实施规范：会计记录的内容。受保护实体必须向个人提供符合以下要求的书面会计记录。

(1) 除本节第(a)段另有规定外，核算必须包括在请求核算之日之前六年内(或根据本节第(a)(3)段应个人请求的更短期间内)发生的受保护健康信息的披露，包括向受保护实体的业务伙伴或由受保护实体的业务伙伴进行的披露。

(2) 除本节第(b)(3)或(b)(4)段另有规定外，核算必须就每项披露包括：

(i) 披露日期；
(ii) 接收受保护健康信息的实体或个人的名称，以及(如已知)该实体或个人的地址；

(iii) 对所披露的受保护健康信息的简要说明；以及

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under §164.502(a)(2)(ii) or §164.512, if any.

(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §164.502(a)(2)(ii) or §164.512, the accounting may, with respect to such multiple disclosures, provide:

(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;

(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(iii) The date of the last such disclosure during the accounting period.

(4)(i) If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with §164.512(i) for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:

(A) The name of the protocol or other research activity;

(B) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(C) A brief description of the type of protected health information that was disclosed;

(D) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

(E) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

(F) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

(ii) If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

(c) *Implementation specifications: Provision of the accounting.* (1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.

(i) The covered entity must provide the individual with the accounting requested; or

(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

(B) The covered entity may have only one such extension of time for action on a request for an accounting.

(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

(d) *Implementation specification: Documentation.* A covered entity must document the following and retain the documentation as required by §164.530(j):

(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that

(iv) 对披露目的的简要说明，以合理方式告知个人该披露的依据；或者，代替该说明，提供根据 164.512提出的书面披露请求的副本(如有)。

(3) 如果在核算所涵盖的期间内，受保护实体根据164.512为单一目的向同一人或实体进行了多次受保护健康信息披露，则核算可以就此等多次披露提供：

(i) 本节第(b)(2)段所要求的、关于核算期内首次披露的信息；

(ii) 在核算期间内所作披露的频率、周期性或次数；以及

(iii) 会计期内最后一次此类披露的日期。

(4)(i) 如果在核算所涵盖的期间内，受保护实体根据164.512(i)为特定研究目的对50名或以上个人进行了受保护健康信息披露，则核算可以就此等可能包含该个人受保护健康信息的披露提供：

(A)协议或其他研究活动的名称；

(B) 以通俗语言对研究方案或其他研究活动的描述，包括研究目的和选择特定记录的标准；

(C) 对所披露受保护健康信息类型的简要描述；

(D) 此等披露发生或可能发生的日期或期间，包括核算期间内最后一次此类披露的日期；

(E) 赞助该研究的实体以及接收信息披露的研究人员的名称、地址和电话号码；以及

(F) 一项声明，说明该个人的受保护健康信息可能或可能未被为特定方案或其他研究活动而披露。

(ii) 如果受保护实体根据本节第(b)(4)段提供研究披露的核算，并且合理可能该个人的受保护健康信息已为此等研究方案或活动而披露，则受保护实体应应个人请求，协助联系赞助该研究的实体和研究人员。

(c) 实施规范：提供核算。(1) 受保护实体必须在收到个人核算请求后不迟于 60 天内，按如下方式处理该请求。

(i) 受保护实体必须向个人提供所请求的核算；或

(ii) 如果受保护实体无法在本节第(c)(1)段要求的时间内提供核算，受保护实体可将提供核算的时间延长不超过30天，但须满足：

(A) 受保护实体在本节第(c)(1)段规定的时限内，向个人提供书面声明，说明延迟的原因以及受保护实体将提供核算的日期；以及

(B) 受保护实体对核算请求的处理只能有一次此类延期。

(2) 受保护实体必须在任何12个月期间内免费向个人提供首次账目说明。对于同一人在该12个月期间内提出的每次后续账目说明请求，受保护实体可收取合理的、基于成本的费用，前提是受保护实体事先告知该个人该费用，并为该个人提供撤回或修改后续账目说明请求以避免或减少该费用的机会。

(d) 实施规范：文档记录。受保护实体必须记录以下内容，并按照164.530(j)的要求保留文档记录：

(1) 根据本节第(b)段要求纳入核算的、关于以下受保护健康信息披露的信息：

are subject to an accounting under paragraph (a) of this section;

(2) The written accounting that is provided to the individual under this section; and

(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002]

§ 164.530 Administrative requirements.

(a)(1) *Standard: Personnel designations.* (i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by §164.520.

(2) *Implementation specification: Personnel designations.* A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

(b)(1) *Standard: Training.* A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

(2) *Implementation specifications: Training.* (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

(c)(1) *Standard: Safeguards.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2)(i) *Implementation specification: Safeguards.* A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

(d)(1) *Standard: Complaints to the covered entity.* A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.

(2) *Implementation specification: Documentation of complaints.* As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

(e)(1) *Standard: Sanctions.* A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of §164.502(j) or paragraph (g)(2) of this section.

(2) *Implementation specification: Documentation.* As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

受本节(a)款规定的会计约束；

(2) 根据本节向个人提供的书面核算；以及

(3) 负责接收和处理个人核算请求的人员或办公室的职务名称。

[65 FR 82802,2000年12月28日，经67 FR 53271,2002年8月14日修订]

164.530 行政要求。

(a) (1) 标准：人员指定。

(i) 受保护实体必须指定一名隐私官，负责制定和实施该实体的政策和程序。

(ii) 受保护实体必须指定一名联系人或办公室，负责接收本节下的投诉，并能够就164.520所要求通知涵盖的事项提供进一步信息。

(2) 实施规范：人员指定。受保护实体必须按照本节第(j)段的要求记录本节第(a)(1)段中的人员指定。

(b)(1) 标准：培训。受保护实体必须就本子部分及本部分D子部分所要求的有关受保护健康信息的政策和程序，对所有工作人员成员进行培训，培训程度以工作人员成员在受保护实体内履行其功能所必需和适当者为限。

(2) 实施规范：
培训。(i) 受保护实体必须提供符合本节(b)(1)段要求的培训，具体如下：

(A) 在受保护实体的合规日期之前，向受保护实体工作人员的每一名成员提供；以及

(B) 此后，在该人员加入受保护实体工作人员后的合理期间内，向每一名新工作人员成员提供；以及

(C) 在本子部分或本部分D子部分所要求的政策或程序发生重大变更后的一段合理时间内，向受保护实体工作人员中其功能受该变更影响的每一成员提供；

重大变更根据本节(i)段生效。

(ii) 受保护实体必须按照本节(j)段的要求，记录已提供本节(b)(2)(i)段所述培训的情况。

(c)(1) 标准：保障措施。受保护实体必须制定适当的行政、技术和物理保障措施，以保护受保护健康信息的隐私。

(2) (i) 实施规范：
保障措施。受保护实体必须合理保障受保护健康信息，防止任何违反本子部分标准、实施规范或其他要求的故意或非故意使用或披露。

(ii) 受保护实体必须合理保障受保护健康信息，以限制依据原本允许或要求的使用或披露而发生的附带使用或披露。

(d)(1) 标准：向受保护实体提出的投诉。受保护实体必须为个人提供提出投诉的程序，投诉涉及受保护实体依据本子部分和本部分D子部分所要求的政策和程序，或其对此类政策和程序或本子部分或本部分D子部分要求的遵守情况。

(2) 实施规范：投诉的记录。按照本节(j)段的要求，受保护实体必须记录收到的所有投诉及其处理结果(如有)。

(e)(1) 标准：制裁。受保护实体必须对其工作人员中未能遵守受保护实体的隐私政策和程序或本子部分或本部分D子部分要求的成员制定并实施适当的制裁。本标准不适用于受保护实体工作人员中其行为属于164.502(j)或本节(g)(2)段涵盖范围且符合其条件的成员。

(2) 实施规范：记录。按照本节(j)段的要求，受保护实体必须记录所实施的制裁(如有)。

(f) *Standard: Mitigation.* A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

(g) *Standard: Refraining from intimidating or retaliatory acts.* A covered entity—

(1) May not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this subpart or subpart D of this part, including the filing of a complaint under this section; and

(2) Must refrain from intimidation and retaliation as provided in §160.316 of this subchapter.

(h) *Standard: Waiver of rights.* A covered entity may not require individuals to waive their rights under §160.306 of this subchapter, this subpart, or subpart D of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(i)(1) *Standard: Policies and procedures.* A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

(2) *Standard: Changes to policies and procedures.* (i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart or subpart D of this part.

(ii) When a covered entity changes a privacy practice that is stated in the notice described in §164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with §164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.

(3) *Implementation specification: Changes in law.* Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by §164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with §164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

(4) *Implementation specifications: Changes to privacy practices stated in the notice.* (i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:

(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and

(C) Revise the notice as required by §164.520(b)(3) to state the changed practice and make the revised notice available as required by §164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

(f) 标准：缓解。受保护实体必须在切实可行的范围内，缓解受保护实体已知的、因受保护实体或其业务伙伴违反其政策和程序或本子部分要求而使用或披露受保护健康信息所造成的任何有害影响。

(g) 标准：禁止恐吓或报复行为。受保护实体--

(1) 不得因任何个人行使本子部分或本部分D子部分确立的任何权利，或参与本子部分或本部分D子部分规定的任何程序(包括根据本节提出投诉)，而对该个人进行恐吓、威胁、胁迫、歧视或采取其他报复行动；以及

(2) 必须避免本子章160.316规定的恐吓和报复行为。

(h) 标准：权利放弃。受保护实体不得要求个人放弃其在本子章160.306、本子部分或本部分D子部分下的权利，作为提供治疗、付款、加入健康计划或获得福利资格的条件。

(i)(1) 标准：政策和程序。受保护实体必须针对受保护健康信息实施旨在遵守本子部分及本部分D子部分的标准、实施规范或其他要求的政策和程序。这些政策和程序必须合理设计，考虑到受保护实体所开展的与受保护健康信息相关的活动的规模和类型，以确保此类合规。本标准不得被解释为允许或免除违反本子部分任何其他标准、实施规范或其他要求的行为。

(2) 标准：政策和程序的变更。(i) 受保护实体必须视必要和适当变更其政策和程序，以遵守法律的变化，包括本子部分或本部分D子部分的标准、要求和实施规范。

(ii) 当受涵盖实体更改 164.520(b)(1)(v)(C)在通知中包含一项声明，保留其在隐私实践中进行此类更改的权利；或

(iii) 受保护实体可随时对政策和程序作出任何其他变更，但该变更须按照第(j)段的要求记录和实施

(i) (5) 本节之规定。

(3) 实施规范：

法律变更。每当法律发生变更而需要对受保护实体的政策或程序进行变更时，受保护实体必须及时记录并实施修订后的政策或程序。如果法律变更实质性影响 164.520(b)(3)及时对通知作出适当修订。本款中的任何内容不得被受保护实体用来免除未能遵守法律的责任。

(4) 实施规范：对通知中载明的隐私实践的变更。(i) 为实施本节(i)(2)(ii)段规定的变更，受保护实体必须：

(A) 确保为反映其通知中载明的受保护实体隐私实践变更而修订的政策或程序符合本子部分的标准、要求和实施规范；

(B) 按照本节(j)段的要求记录经修订的政策或程序；以及

(C) 依据 164.520(c)的要求提供修订后的通知。受保护实体不得在修订后通知的生效日期之前实施政策或程序的变更。

(ii) If a covered entity has not reserved its right under §164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

(A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)–(C) of this section; and

(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

(5) *Implementation specification: Changes to other policies or procedures.* A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by §164.520, provided that:

(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and

(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.

(j)(1) *Standard: Documentation.* A covered entity must:

(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;

(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and

(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.

(iv) Maintain documentation sufficient to meet its burden of proof under §164.414(b).

(2) *Implementation specification: Retention period.* A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

(k) *Standard: Group health plans.* (1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:

(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and

(ii) The group health plan does not create or receive protected health information, except for:

(A) Summary health information as defined in §164.504(a); or

(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with §164.504(f).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53272, Aug. 14, 2002; 71 FR 8433, Feb. 16, 2006; 74 FR 42769, Aug. 24, 2009]

§164.532 Transition provisions.

(a) *Standard: Effect of prior authorizations.* Notwithstanding §§164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, a waiver of informed consent by an IRB, or a waiver of authorization in accordance with §164.512(i)(1)(i).

(b) *Implementation specification: Effect of prior authorization for purposes other than research.* Notwithstanding any provisions in §164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of

(ii) 如果受保护实体未根据164.520(b)(1)(v)(C)保留其更改通知中所述隐私实践的权利，则受保护实体在该通知有效期间创建或接收的受保护健康信息方面受通知中所述隐私实践的约束。受保护实体可以更改通知中所述的隐私实践及相关政策和程序，而无需保留这样做的权利，前提是：

(A) 此类变更符合以下各款中的实施规范

(4) (i)(A) -(C) 本节；以及

(i)

(B) 该变更仅对通知生效日期之后创建或收到的受保护健康信息生效。

(5) 实施规范：对其他政策或程序的变更。受保护实体可随时变更不实质性影响164.520所要求通知内容的政策或程序，前提是：

(i) 经修订的政策或程序符合本子部分的标准、要求和实施规范；以及

(ii) 在变更生效日期之前，经修订的政策或程序已按照本节(j)段的要求记录。

(j)(1) 标准：文档记录。受保护实体必须：

(i) 以书面或电子形式保存本节(i)段规定的政策和程序；

(ii) 如果本子部分要求某项通信采用书面形式，则保存该书面文件或电子副本作为记录；以及

(iii) 如果本子部分要求对某项行动、活动或指定进行记录，则应保存该行动、活动或指定的书面或电子记录。

(iv) 保存足以满足其在164.414(b)下举证责任的记录。

(2) 实施规范：保存期限。受保护实体必须自本节(j)(1)段所要求记录的创建之日起保存六年，或最后生效的日期，以较晚者为准。

(k) 标准：团体健康计划。(1) 团体健康计划在以下范围内不受本节(a)至(f)段和(i)段的标准或实施规范约束：

(i) 团体健康计划仅通过与健康保险发行机构或HMO的保险合同提供健康福利；以及

(ii) 团体健康计划不创建或接收受保护健康信息，但以下信息除外：

(A)164.504(a) 所定义的摘要健康信息；或

(B) 关于个人是否参加团体健康计划，或是否加入或已退出该计划所提供的健康保险发行机构或HMO的信息。

(2) 本节(k)(1)段所述的团体健康计划仅就按照164.504(f)修订的计划文件受本节(j)段的标准和实施规范约束。

[65 FR 82802,2000年12月28日，经67 FR 53272,2002年8月14日；71 FR 8433,2006年2月16日；74 FR 42769,2009年8月24日修订]

164.532 过渡条款。

(a) 标准：先前授权的影响。尽管有 164.508和164.512(i)的规定，受保护实体可以依照本节(b)和(c)段，根据从个人获得的授权或其他明确的法律许可，允许使用或披露受保护健康信息、个人参与研究的知情同意、IRB对知情同意的豁免，或根据164.512(i)(1)(i)对授权的豁免，使用或披露受保护健康信息。

(b) 实施规范：先前授权用于研究以外目的的效果。尽管164.508中有任何规定，受保护实体可以使用或披露其在本子部分适用合规日期之前创建的或收到的受保护健康信息，前提是依据在该适用合规日期之前从个人处获得的授权或其他明示法律许可，

this subpart, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with §164.522(a).

(c) *Implementation specification: Effect of prior permission for research.* Notwithstanding any provisions in §§164.508 and 164.512(i), a covered entity may, to the extent allowed by one of the following permissions, use or disclose, for research, protected health information that it created or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with §164.522(a), and the covered entity has obtained, prior to the applicable compliance date, either:

(1) An authorization or other express legal permission from an individual to use or disclose protected health information for the research;

(2) The informed consent of the individual to participate in the research;

(3) A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with §164.508 if, after the compliance date, informed consent is sought from an individual participating in the research; or

(4) A waiver of authorization in accordance with §164.512(i)(1)(i).

(d) *Standard: Effect of prior contracts or other arrangements with business associates.* Notwithstanding any other provisions of this part, a covered entity, or business associate with respect to a subcontractor, may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§164.308(b), 164.314(a), 164.502(e), and 164.504(e), only in accordance with paragraph (e) of this section.

(e) *Implementation specification: Deemed compliance*—(1) *Qualification.* Notwithstanding other sections of this part, a covered entity, or business associate with respect to a subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§164.308(b), 164.314(a), 164.502(e), and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:

(i) Prior to January 25, 2013, such covered entity, or business associate with respect to a subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the business associate that complies with the applicable provisions of §164.314(a) or §164.504(e) that were in effect on such date; and

(ii) The contract or other arrangement is not renewed or modified from March 26, 2013, until September 23, 2013.

(2) *Limited deemed compliance period.* A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section shall be deemed compliant until the earlier of:

(i) The date such contract or other arrangement is renewed or modified on or after September 23, 2013; or

(ii) September 22, 2014.

(3) *Covered entity responsibilities.* Nothing in this section shall alter the requirements of a covered entity to comply with part 160, subpart C of this subchapter and §§164.524, 164.526, 164.528, and 164.530(f) with respect to protected health information held by a business associate.

(f) *Effect of prior data use agreements.* If, prior to January 25, 2013, a covered entity has entered into and is operating pursuant to a data use agreement with a recipient of a limited data set that complies with §164.514(e), notwithstanding §164.502(a)(5)(ii), the covered entity may continue to disclose a limited data set pursuant to such agreement in exchange for remuneration from or on behalf of the recipient of the protected health information until the earlier of:

(1) The date such agreement is renewed or modified on or after September 23, 2013; or

本子部分，前提是该授权或其他明示法律许可明确允许此类使用或披露，且不存在依据164.522(a)达成的限制。

(c) 实施规范：先前研究许可的效力。尽管有 164.508和164.512(i)中的任何规定，受保护实体可以在以下许可之一允许的范围内，为研究目的使用或披露其在本子部分适用合规日期之前或之后创建或接收的受保护健康信息，前提是根据164.522(a)不存在已达成一致的限制，且受保护实体在适用合规日期之前已获得以下之一：

(1) 个人为研究而使用或披露受保护健康信息的授权或其他明示法律许可；

(2) 个人参与研究的知情同意；

(3) 研究审查委员会(IRB)根据 7 CFR 1c.116(d)、10 CFR 745.116(d)、14 CFR 1230.116(d)、15 CFR 27.116(d)、16 CFR 1028.116(d)、21 CFR 50.24、22 CFR 225.116(d)、24 CFR 60.116(d)、28 CFR 豁免研究知情同意

46.116 (d)、32 CFR 219.116(d)、34 CFR
97.116 (d)、38 CFR 16.116(d)、40 CFR
26.116 (d)、45 CFR 46.116(d)、45 CFR
690.116(d)或49 CFR 11.116(d)获得的研究同意，前提是如果在合规日期之后寻求参与研究的个人的知情同意，受保护实体必须依据164.508获得授权；或

(4) (3) 根据164.512(i)(1)(i) 豁免授权。

(d) 标准：先前与业务伙伴的合同或其他安排的效力。尽管有本部分的任何其他规定，受保护实体，或业务伙伴就分包商而言，可以依据与业务伙伴签订的书面合同或其他书面安排，向业务伙伴披露受保护健康信息，并允许业务伙伴代表其创建、接收、维护或传输受保护健康信息，但该合同或安排不符合 164.308(b)、164.314(a)、164.502(e)和164.504(e)的规定，且仅依照本节(e)款进行。

(e) 实施规范：
视为合规 -(1) 资格。尽管本部分其他条款有规定，受保护实体，或业务伙伴就分包商而言，在下列情况下，就特定业务伙伴关系而言，在本节(e)(2)款规定的期限内，视为符合 164.308(b)、164.314(a)、164.502(e)和164.504(e)的文件和合同要求：

(i) 在2013年1月25日之前，该受保护实体，或就分包商而言的业务伙伴，已与该业务伙伴签订书面合同或其他书面安排，并正依据该合同或安排运营，且该合同或安排符合在该日期生效的 164.504(e)的适用条款；以及

(ii) 合同或其他安排自2013年3月26日起至2013年9月23日止未续签或修改。

(2) 有限视为合规期。符合本节第(e)款资格要求的先前合同或其他安排，应视为合规，直至以下日期中较早者：

(i) 该合同或其他安排于2013年9月23日或之后续签或修改的日期；或

(ii) 2014年9月22日。

(3) 受保护实体的责任。
本节任何内容均不得改变受保护实体就业务伙伴持有的受保护健康信息遵守本子章第160部分C子部分以及164.524、164.526、164.528和164.530(f)的要求。

(f) 先前数据使用协议的效力。
如果在2013年1月25日之前，受保护实体已与符合164.502(a)(5)(ii)的规定，受保护实体可以继续依据该协议披露有限数据集，以换取来自受保护健康信息接收方或代表其提供的报酬，直至以下日期中较早者：

(1) 该协议于2013年9月23日或之后续签或修改的日期；或

(2) September 22, 2014.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53272, Aug. 14, 2002; 78 FR 5702, Jan. 25, 2013; 78 FR 34266, June 7, 2013]

§ 164.534 Compliance dates for initial implementation of the privacy standards.

(a) *Health care providers.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 14, 2003.

(b) *Health plans.* A health plan must comply with the applicable requirements of this subpart no later than the following as applicable:

(1) *Health plans other than small health plans.* April 14, 2003.

(2) *Small health plans.* April 14, 2004.

(c) *Health clearinghouses.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 14, 2003.

[66 FR 12434, Feb. 26, 2001]

§ 164.535 Severability.

If any provision of the HIPAA Privacy Rule to Support Reproductive Health Care Privacy is held to be invalid or unenforceable facially, or as applied to any person, plaintiff, or circumstance, it shall be construed to give maximum effect to the provision permitted by law, unless such holding shall be one of utter invalidity or unenforceability, in which case the provision shall be severable from this part and shall not affect the remainder thereof or the application of the provision to other persons not similarly situated or to other dissimilar circumstances.

[89 FR 33066, Apr. 26, 2024]

PARTS 165–169 [RESERVED]

(2) 2014年9月22日。

[65 FR 82802,2000年12月28日，经67 FR 53272,2002年8月14日；78 FR 5702,2013年1月25日；78 FR 34266,2013年6月7日修订]

164.534 初始合规日期

隐私标准的实施。

(a) 医疗保健提供者。受保护医疗保健提供者必须不迟于2003年4月14日遵守本子部分的适用要求。

(b) 健康计划。健康计划必须不迟于以下适用日期遵守本子部分的适用要求：

(1) (3)小型健康计划以外的健康计划。2003年4月14日。

(2) 小型健康计划。 2004年4月14日。(c) 健康信息交换中心。医疗保健信息交换中心必须不迟于2003年4月14日遵守本子部分的适用要求。

[66 FR 12434，2001年2月26日]

164.535 可分割性。

如果《HIPAA隐私规则--支持生殖健康保健隐私》的任何条款被认定为表面上无效或不可执行，或在适用于任何人、原告或情形时无效或不可执行，则应将其解释为在法律允许的范围内给予该条款最大效力，除非该认定属于完全无效或不可执行，在此情况下该条款应可从本部分中分割，且不影响本部分的其余内容或该条款对非类似处境的其他人的适用或对其他不同情形的适用。

[89 FR 33066，2024年4月26日]

第165-169部分[保留]

How this file was made

This is a complete Chinese translation of the HIPAA Security Rule. Tables, captions, headers, footers and numbering all keep their original positions. Nothing has been cut.

If you have documents of your own

- Contracts, tenders, standards, patents, reports: original layout kept, CNY 0.15/page
- PDF to Word: free up to 100 pages, CNY 0.10/page beyond that
- Scanned or image-only PDFs: OCR to Word, free
- No sign-up, no login: upload and download

Open the address below and try it with your own file:

https://www.ivyivy.com.cn/hipaa-security-rule-zh

On-premise deployment available (subject to model and compliance review)

Machine translation, provided for reading reference only. For professional judgement and compliance citation, please refer to the original English source.

This page is a translator's note; it is not part of the original document.

这份文件是怎么做出来的

本译本是《HIPAA 安全规则》的中文全译本，共 64 页。表格、图注、页眉页脚、编号层级都按原文位置一一还原，未做任何删节。

你手上如果也有英文文件要处理

- 合同、标书、标准、专利、报告：翻译后保留原版式，0.15 元/页
- PDF 转 Word：100 页内免费，超出 0.1 元/页
- 扫描件、图片版 PDF：先 OCR 再转 Word，免费
- 不用注册、不用登录，传上去直接下载

打开下面这个地址，把你自己的文件传上去试试：

https://www.ivyivy.com.cn/hipaa-security-rule-zh

支持私有化部署（需按贵方模型与合规要求评估）

本译本由机器翻译生成，仅供阅读参考；专业技术判断与合规引用，请以英文原文为准。

本页为译制说明，不属于原文件内容。