The Network for Public Health Law

Ideas. Experience. Practical answers.

HIPAA Privacy Rule: Hybrid Entity Regulatory Reference Table

Becoming a Hybrid Entity: As Defined by the HIPAA Privacy Rule

Congress passed the Health Insurance Portability and Accountability Act ("HIPAA"), Public Law 104-191 in 1996, which required the Department of Health and Human Services ("HHS") to adopt national standards for electronic health care transactions and code sets, privacy, security and unique health identifiers. HHS issued its first Privacy Rule in 2000, which spans 367 pages, including the preamble.

HHS recognizes that many organizations, including government agencies, have components that provide covered services, including health care services, lines of health insurance or a health care clearinghouse, as well as other components that do not provide HIPAA regulated services. Reducing compliance burden, HHS offers organizations the option of applying HIPAA to only those components that would be regulated by HIPAA if they were separate legal entities. Becoming a hybrid entity relies upon the careful and precise classification of all organizational components.

The HIPAA Privacy Rule defines the hybrid entity and sets forth the organizational requirements, including standards and implementation specifications. 45 CFR §§ 164.103 and 164.105(a) and (c). The rule provides that the legal entity that is a hybrid entity must implement safeguards and undertake certain responsibilities with respect to its covered entity and business associate components.

Since 2000, HHS has twice amended this rule, including the hybrid entity provisions. The preambles to each of the three rules offer HHS' interpretation of regulatory provisions, analysis, response to comments, rationale for amendments to regulations and background.

This table provides the text and citations to the current Privacy Rule's hybrid entity provisions and relevant portions of all three Privacy Rule preambles, along with brief summaries.

HIPAA Privacy Rule Citation	Regulatory Content	Reference or Summary
Final Omnibus Rule, 78 FR 5566 (January 25, 2013). Strengthening HIPAA's privacy and security protections for health information, this final rule implements provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, and modifies the HIPAA Privacy Rule. 45 CFR Parts 160, 162 and 164. 45 CFR Part 164 This combined official version of HIPAA security and privacy regulatory standards provides a method of viewing the *current and complete* HIPAA Privacy Rule text.		
45 CFR § 164.103.	*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).	**Definitions.**
45 CFR § 164.105(a)(1).	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.	**Organizational requirements**, *Standard: Health care component.*

45 CFR § 164.105(a)(2)(i).	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.	**Organizational requirements**, *Implementation specifications: Application of other provisions.*
45 CFR § 164.105(a)(2)(ii).	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	**Organizational requirements,** *Implementation specifications: Safeguard requirements***.**

	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.	
45 CFR § 164.105(a)(2)(iii).	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 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.	**Organizational requirements,** *Implementation specifications: Responsibilities of the covered entity.*
45 CFR § 164.105(c)(1).	A covered entity must maintain a written or electronic record of a designation as required by paragraphs (a) or (b) of this section.	**Organizational requirements**, *Standard: Documentation.*
45 CFR § 164.105(c)(2).	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.	**Organizational requirements,** *Implementation specification: Retention period.*
Preamble to Final Omnibus Rule, 78 FR 5566 (January 25, 2013). Excerpts from the Final Omnibus Rule's preamble regarding becoming a hybrid entity follow.		
78 FR 5566, 5588, Preamble.	Many covered entities perform both covered and non-covered functions as part of their business operations. For such covered entities, the entire entity is generally required to comply with the Privacy Rule. However, the hybrid entity provisions of the HIPAA Rules permit the entity to limit the application of the Rules to the entity's components that perform	The hybrid entity option gives the legal entity the choice of limiting application of HIPAA to only the covered entity components. (The preamble later discusses the required inclusion of business associate components.)

	functions that would make the component a ‘‘covered entity’’ if the component were a separate legal entity. Specifically, this provision allows an entity to designate a health care component by documenting the components of its organization that perform covered entity functions. The effect of such a designation is that most of the requirements of the HIPAA Rules apply only to the designated health care component of the entity and not to the functions the entity performs that are not included in the health care component.	
78 FR 5566, 5588, Preamble.	While most of the HIPAA Rules' requirements apply only to the health care component, the hybrid entity retains certain oversight, compliance, and enforcement obligations.	The legal entity retains oversight, compliance and enforcement obligations.
78 FR 5566, 5588, Preamble.	We explained in the preamble to the 2002 modifications to the Privacy Rule that the Rule provides hybrid entities with discretion as to whether or not to include business associate divisions within the health care component. However, a disclosure of protected health information from the health care component to any other division that is not part of the health care component, including a business associate division, is treated the same as a disclosure outside the covered entity. As a result, because an entity generally cannot have a business associate agreement with itself, a disclosure from the health care component to the business associate division(s) of the entity likely would require individual authorization. See 67 FR 53182, 53205 (Aug. 14, 2002). Importantly, after this final rule, business associates, by definition, are separately and directly liable for violations of the Security Rule and for violations of the Privacy Rule for impermissible uses and disclosures pursuant to their business associate contracts. With respect to a hybrid entity, however, not including business associate functions within the health care component of a hybrid entity could avoid direct liability and compliance obligations for the business associate component. Thus, we agree with the commenters that supported requiring inclusion of business associate functions inside the health care component of a hybrid entity. As such, the final rule requires that the health care component of a hybrid entity include all business associate functions within the entity.	The hybrid entity policy must list business associate components as covered by HIPAA.
78 FR 5566, 5588, Preamble.	*Comment:* One commenter requested that the Department revise the definitions of ‘‘hybrid entity’’ to permit business associates to designate a health care component. *Response:* A business associate performs one or more functions on behalf of a covered entity (or, in this final rule, another business associate). As a business associate is only subject to the HIPAA Rules with respect to the protected health information it maintains, uses, or	If an organization determines that it provides business associate services and no covered entity services, there is no need to become a hybrid entity.

	discloses on behalf of a covered entity (or business associate) and not to other information it may maintain, including health information, there is no need for a business associate to designate one or more health care components.	
78 FR 5566, 5588-89, Preamble.	*Comment:* One commenter asked whether an employer that operates an on-site clinic for the treatment of employees functions as a hybrid entity. *Response:* An entity that maintains an on-site clinic to provide health care to one or more employees may be a HIPAA covered provider to the extent the clinic performs one or more covered transactions electronically, such as billing a health plan for the services provided. If covered, the entity need not become a hybrid entity so as to avoid applying the Privacy Rule to health information the entity holds in its role as employer, such as sick leave requests of its employees. Such information is already excluded from the definition of ''protected health information'' as employment records and thus, the Privacy Rule does not apply to this information. However, the identifiable health information the entity holds as a covered health care provider (e.g., the information the clinic holds about employees who have received treatment) is protected health information and generally may not be shared with the employer for employment purposes without the individual's authorization.	HHS provides guidance regarding on-site health care clinics for employees. Such a clinic need not designate itself as a hybrid entity to avoid application of HIPAA to employer records, as the definition of protected health information already excludes those records.
78 FR 5566, 5589, Preamble.	We proposed to modify this section to re-designate § 164.105(a)(2)(iii)(C) as (D), and to include a new paragraph (C), which makes clear that, with respect to a hybrid entity, the covered entity itself, and not merely the health care component, remains responsible for complying with §§ 164.314 and 164.504 regarding business associate arrangements and other organizational requirements. Hybrid entities may need to execute legal contracts and conduct other organizational matters at the level of the legal entity rather than at the level of the health care component. The final rule adopts this change.	The legal entity is responsible for contract execution and other legal matters.
Preamble to Modifications to the HIPAA Privacy Rule - Final Rule, 67 FR 53182 (August 14, 2002). This August 2002 final rule modifies HHS's first final Privacy Rule, issued in December 2000. Excerpts from this Final Rule's preamble regarding becoming a hybrid entity follow. This table does not include commentary regarding superseded regulatory provisions.		
67 FR 53182, 53205, Preamble.	The final Rule regarding hybrid entities is intended to provide a covered entity with the flexibility to apply the Privacy Rule as best suited to the structure of its organization, while maintaining privacy protections for protected health information within the organization.	HHS' creation of the hybrid entity is intended to give the covered entity flexibility, while still fully covering protected health information.

67 FR 53182, 53205, Preamble.	Most of the requirements of the Privacy Rule continue to apply only to the health care component(s) of a hybrid entity. Covered entities that choose not to designate health care component(s) are subject to the Privacy Rule in their entirety.	Most HIPAA Privacy Rule requirements only apply to covered entity and business associate components. Absent a hybrid entity policy, HIPAA Privacy Rule requirements apply to the entire legal entity.
67 FR 53182, 53205, Preamble.	The final Rule adopts the proposal's simplified definition of “health care component,” which makes clear that a health care component is what the covered entity designates as the health care component. The Department makes a conforming change in Sec. 164.504(c)(2)(ii) to reflect the changes to the definition of “health care component.” The final Rule at Sec. 164.504(c)(3)(iii) requires a health care component to include a component that would meet the definition of a “covered entity” if it were a separate legal entity. The Department also modifies the language of the final Rule at Sec. 164.504(c)(3)(iii) to clarify that only a component that performs covered functions, and a component to the extent that it performs covered functions or activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities, may be included in the health care component. “Covered functions” are defined at Sec. 164.501 as “those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.”	HHS gives covered entities the discretion to define their covered entity and business associate components. The covered entity component must include any component that, if it were a separate legal entity, would be a covered entity. A hybrid entity may only list its covered entity components and business associate components as covered in its hybrid entity policy.
67 FR 53182, 53205, Preamble.	As in the proposal, the Department provides a hybrid entity with some discretion as to what functions may be included in the health care component in two ways. First, the final Rule clarifies that a hybrid entity may include in its health care component a non-covered health care provider component. Accordingly, the Department adopts the proposed conforming change to Sec. 164.504(c)(1)(ii) to make clear that a reference to a “covered health care provider” in the Privacy Rule may include the functions of a health care provider who does not engage in electronic transactions for which the Secretary has adopted standards, if the covered entity chooses to include such functions in the health care component. A hybrid entity that chooses to include a non-covered health care provider in its health care component is required to ensure that the non-covered health care provider, as well as the rest of the health care component, is in compliance with the Privacy Rule.	HHS clarifies that a non-covered health care provider may be included in the covered entity component.
67 FR 53182, 53205, Preamble.	However, a disclosure of protected health information from the health care component to such other division that is not part of the health care component is the same as a disclosure outside the covered entity.	A covered entity component’s disclosure of protected health information to a non-covered component within the same legal entity is the equivalent of a disclosure outside the hybrid entity.

67 FR 53182, 53205-06, Preamble.	Also in response to comments, the Department clarifies that even if a covered entity does not choose to be a hybrid entity, and therefore is not required to erect firewalls around its health care functions, the entity still only is allowed to use protected health information as permitted by the Privacy Rule, for example, for treatment, payment, and health care operations. Additionally, the covered entity is still subject to minimum necessary restrictions under Secs. 164.502 and 164.514(d), and, thus, must have policies and procedures that describe who within the entity may have access to the protected health information. Under these provisions, workforce members may be permitted access to protected health information only as necessary to carry out their duties with respect to the entity's covered functions. For example, the health insurance line of a multi-line insurer is not permitted to share protected health information with the life insurance line for purposes of determining eligibility for life insurance benefits or any other life insurance purposes absent an individual's written authorization. However, the health insurance line of a multi- line insurer may share protected health information with another line of business pursuant to Sec. 164.512(a), if, for example, State law requires an insurer that receives a claim under one policy to share that information with other lines of insurance to determine if the event also may be payable under another insurance policy. Furthermore, the health plan may share information with another line of business if necessary for the health plan's coordination of benefits activities, which would be a payment activity of the health plan.	Even where a covered entity does not become a hybrid entity which requires firewalls, it must ensure that its protected health information is only used and shared in compliance with the HIPAA Privacy Rule.
67 FR 53182, 53206, Preamble.	Further, the Department does not believe that allowing a covered entity to exclude a non-covered health care provider component from its health care component will be subject to abuse. Excluding health care functions from the health care component has significant implications under the Rule. Specifically, the Privacy Rule treats the sharing of protected health information from a health care component to a non-covered component as a disclosure, subject to the same restrictions as a disclosure between two legally separate entities. For example, if a covered entity decides to exclude from its health care component a non-covered provider, the health care component is then restricted from disclosing protected health information to that provider for any of the non-covered provider's health care operations, absent an individual's authorization. See Sec. 164.506(c). If, however, the non-covered health care provider function is not excluded, it would be part of the health care component and that information could be used for its operations without the individual's authorization.	Inclusion of a non-covered provider in the covered entity component is necessary for information sharing to occur without patient authorization.

Preamble to HIPAA Privacy Rule – Final Rule, 65 FR 82462 (December 28, 2000).		
HHS issued its first final Privacy Rule in December 2000, implementing the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996. 45 CFR Parts 160 and 164. Excerpts from this Final Rule's preamble regarding becoming a hybrid entity follow. This table does not include commentary regarding superseded regulatory provisions.		
65 FR 82462, 82502, Preamble.	In the final rule we address the issue of differentiating health plan, covered health care provider and health care clearinghouse activities from other functions carried out by a single legal entity in paragraphs (a)-(c) of Sec. 164.504. We have created a new term, ``hybrid entity'', to describe the situation where a health plan, health care provider, or health care clearinghouse is part of a larger legal entity; under the definition, a ``hybrid entity'' is ``a single legal entity that is a covered entity . . . '' The term ``covered functions'' is discussed above under Sec. 164.501. By ``single legal entity'' we mean a legal entity, such as a corporation or partnership, that cannot be further differentiated into units with their own legal identities. For example, for purposes of this rule a multinational corporation composed of multiple subsidiary companies would not be a single legal entity, but a small manufacturing firm and its health clinic, if not separately incorporated, could be a single legal entity.	A hybrid entity is a single legal entity that cannot be further legally subdivided and includes a health plan, health care provider or health care clearinghouse.
65 FR 82462, 82503, Preamble.	With respect to excepted benefits, the rules below operate as follows. (Excepted benefits include accident, disability income, liability, workers' compensation and automobile medical payment insurance.) Excepted benefit programs are excluded from the health care component (or components) through the definition of ``health plan.'' If a particular organizational unit performs both excepted benefits functions and covered functions, the activities associated with the excepted benefits program may not be part of the health care component. For example, an accountant who works for a covered entity with both a health plan and a life insurer would have his or her accounting functions performed for the health plan as part of the component, but not the life insurance accounting function. See Sec. 164.504(c)(2)(iii). We require this segregation of excepted benefits because HIPAA does not cover such programs, policies and plans, and we do not permit any use or disclosure of protected health information for the purposes of operating or performing the functions of the excepted benefits without authorization from the individual, except as otherwise permitted in this rule.	The HIPAA Privacy Rule excludes excepted benefit programs from the covered component and generally requires patient authorization for information sharing with these programs.
65 FR 82462, 82503, Preamble.	In Sec. 164.504(c)(2) we require covered entities with a health care component to establish safeguard policies and procedures to prevent any access to protected health information by its other organizational units that would not be otherwise permitted by this rule. We note that	Hybrid entities must establish policies and procedures to safeguard the protected health information and only allow access as allowed by HIPAA.

	section 1173(d)(1)(B) of HIPAA requires policies and procedures to isolate the activities of a health care clearinghouse from a ``larger organization'' to prevent unauthorized access by the larger organization. This safeguard provision is consistent with the statutory requirement and extends to any covered entity that performs ``non-covered entity functions'' or operates or conducts functions of more than one type of covered entity.	
65 FR 82462, 82503, Preamble.	Because, as noted, the covered entity in the hybrid entity situation is the legal entity itself, we state explicitly what is implicitly the case, that the covered entity (legal entity) remains responsible for compliance vis-a-vis subpart C of part 160. See Sec. 164.504(c)(3)(i). We do this simply to make these responsibilities clear and to avoid confusion on this point. Also, in the hybrid entity situation the covered entity/legal entity has control over the entire workforce, not just the workforce of the health care component. Thus, the covered entity is in a position to implement policies and procedures to ensure that the part of its workforce that is doing mixed or non-covered functions does not impermissibly use or disclose protected health information. Its responsibility to do so is clarified in Sec. 164.504(c)(3)(ii).	The legal entity is responsible for HIPAA compliance. The legal entity must ensure that its workforce performing mixed or non-covered functions does not impermissibly use or disclose protected health information.
65 FR 82462, 82639, Preamble.	Comment: A commenter representing a government agency recommended that only the component of the agency that runs the program be considered a covered entity, not the agency itself. In addition, this commenter stated that often subsets of other government agencies work in partnership with the agency that runs the program to provide certain services. For example, one state agency may provide maternity support services to the Medicaid program which is run by a separate agency. The commenter read the rule to mean that the agency providing the maternity support services would be a business associate of the Medicaid agency, but was unclear as to whether it would also constitute a health care component within its own agency. Response: We generally agree. We expect that in most cases, government agencies that run health plans or provide health care services would typically meet the definition of a ``hybrid entity'' under Sec. 164.504(a), so that such an agency would be required to designate the health care component or components that run the program or programs in question under Sec. 164.504(c)(3), and the rules would not apply to the remainder of the agency's operations, under Sec. 164.504(b).	Generally, government agencies that run health plans or provide health care services meet the definition of a hybrid entity.

65 FR 82462, 82639, Preamble.	Comment: One commenter representing an insurance company stated that different product lines should be treated separately under the rule. For example, the commenter argued, because an insurance company offers both life insurance and health insurance, it does not mean that the insurance company itself is a covered entity, rather only the health insurance component is a covered entity. Another commenter requested clarification of the use of the term ``product line'' in the proposed rule. This commenter stated that product line should differentiate between different lines of coverage such as life vs. health insurance, not different variations of the same coverage, such as HMO vs. PPO. Finally, one commenter stated that any distinction among product lines is unworkable because insurance companies need to share information across product lines for coordinating benefits. This sharing of information, the commenter urged, should be able to take place whether or not all product lines are covered under the rule. Response: We agree that many forms of insurance do not and should not come within the definition of ``health plan,'' and we have excepted them from the definition of this term in Sec. 160.103 applies. This point is more fully discussed in connection with that definition. Although we do not agree that the covered entity is only the specific product line, as this comment suggests, the hybrid entity rules in Sec. 164.504 address the substance of this concern. Under Sec. 164.504(c)(3), an entity may create a health plan component which would include all its health insurance lines of business or separate health care components for each health plan product line. Finally, the sharing of protected health information across lines of business is allowed if it meets the permissive or required disclosures under the rule. The commenter's example of coordination of benefits would be allowed under the rule as payment.	An entity may place all of its lines of health insurance in separate covered components or within one covered component. A covered entity may not include excepted lines of insurance in the covered component. Sharing of protected health information across business lines is allowed to the extent permitted or required by HIPAA.

SUPPORTERS

Robert Wood Johnson Foundation

The Network for Public Health Law is a national initiative of the Robert Wood Johnson Foundation.

This document was developed by Sallie Milam, JD, CIPP/US/G, Deputy Director, Network for Public Health Law – Mid-States Region Office, and reviewed by Denise Chrysler, JD, Director, Network for Public Health Law – Mid-States Region Office. The Network for Public Health Law provides information and technical assistance on issues related to public health. The legal information and assistance provided in this document does not constitute legal advice or legal representation. For legal advice, please consult specific legal counsel.