

HIPAA Agreements

Overview, Guidelines, Samples

I. Purpose

The purpose of this document is to provide an overview of the regulatory requirements related to HIPAA trading partner agreements, business associate agreements, and chain of trust agreements, (collectively HIPAA Agreements). The document will also provide guidance on when the respective agreements are necessary or recommended and some samples.

II. Scope

This document provides guidance on what the agreements are, when it must or should be used, and format considerations in a public agency business environment.

There are five primary sections, addressing the following topics:

- ✘ Relationship of HIPAA agreements
- ✘ Trading Partner Agreement
- ✘ Business Associate Contract
- ✘ Data Use Agreement
- ✘ Appendix: Regulation Text and Samples

III. Relationship Among HIPAA Agreements

HIPAA regulations contain requirements for agreements relating to transactions, privacy and (eventually) security. The purpose of this section is to outline how they interact.

Trading Partner Agreements

Trading partner agreements are agreements about how entities accept and process (standardized) transactions. TPAs are needed between the covered entity and those it exchanges transactions with in order to set common expectations about: situational data elements where an element may only be required if required by the payer, or optional functions such as coordination of benefits and batch versus real time processing; connectivity issues and for example, identification of clearinghouses or other third parties used, and for which transactions; whether direct data entry is supported; whether disks or other media, dial-up connectivity, or other electronic connectivity is supported; whether any additional, non-standard communication methods are supported and any restrictions or required formats; and other issues such as testing requirements or timelines.

TPAs are generally needed between all trading partners such as providers, other health plans, any sponsors, and clearinghouses. The format and content are not specified and many organizations are utilizing “companion documents”. The comments to the regulations note that, in general, trading partners are not business associates because each party is acting on their own behalf.

Business Associate Contracts

Business associate contracts (BAC) are required by HIPAA's privacy regulation before health information can be accessed or shared with business associates §160.103 (definition) and §164.504(e)(contract requirement). Generally, the purpose of the contract provisions is to bind the business associate to protect the data and use it only for the contract's specified purposes.

Business associates (with whom the contracts are required) are persons or entities (other than your workforce) that provide or perform services on your behalf that involves the use or disclosure of health information. Examples included: claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, repricing; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, of financial services to the organization.

Generally, except for some clearinghouses, typical state trading partners such as providers, third party payers or other health plans, and CMS are not business associates. Thus, business associate contracts are generally not required with trading partners. However, where your program has another organization conduct or facilitate transactions for you (e.g. clearinghouse), business associate contract language is required. In this case, depending on whether the business associate sends or receives transactions to or from your program, TPA provisions will also be applicable.

Data Use Agreement

A Data Use Agreement is a new contract permitted under the privacy rule, to be used when a covered entity discloses limited data sets with other entities (limited data set recipients).

Limited data sets are generally stripped of all "direct identifiers" but may contain geographic information (city, county, zipcode) and dates (dates of birth, service, etc). Limited data sets may be used or disclosed only for research, public health, or health care operations.

Generally, data use agreements would not be used with trading partners or business associates (except in some cases for health care operations).

IV. Trading Partner Agreement

Summary

Trading partner agreements (TPA) are defined in the HIPAA regulation, but are not required. TPA language is recommended when your program is conducting transactions with other organizations. TPA are used to describe implementation details specific to the organization, transmission requirements, or issues not addressed or left to the discretion of payers by the standard.

The TPA format need not be a typical contract format, consideration should be given to current communication methods about requirements for processing such as billing instructions, formal memorandums or bulletins, addenda, etc. Many entities are issuing "companion documents" that contain TPA information.

Business associate contract provisions, required under Privacy, are not generally needed with trading partners when conducting transactions. Chain of trust provisions, proposed under Security, will generally be needed with TPA.

Regulation

Introduction

The regulation defines “trading partner agreement” and also specifies what cannot be in a TPA. However, the regulation does not require nor outline what should be included in the TPA. On the other hand, the implementation guides for each transaction do recommend trading partner agreements.

It is recognized that there are two levels of scrutiny for electronic transactions: standards compliance, and trading partner specific processing or adjudication requirements. Thus, the regulation makes clear that agreements cannot modify the standards in any way. However, TPAs are appropriate to specify processing requirements that are not in conflict with the standard.

Set forth below is the regulatory definition of a TPA and the items prohibited from inclusion in a TPA.

Regulatory Text

Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.) §160.103.

§162.915 Trading Partner Agreements.

A covered entity must not enter into a trading partner agreement that would do any of the following:

- a) change the definition, data condition, or use of a data element or segment in a standard,
- b) add any data elements or segments to the maximum defined data set,
- c) use any code or data elements that are either marked “not used” in the standard’s implementation specification or are not in the standard’s implementation specification(s).
- d) Change the meaning or intent of the standard’s implementation specification(s).

TPA Considerations

Since the regulation neither requires a TPA nor specifies what it should contain, why is it needed at all, and in what situation is it needed?

When TPAs are Needed

Trading partner agreements are needed when you are conducting administrative transactions with other organizations or businesses. Usually, the provisions of a TPA will contain adjudication or processing information relevant to both electronic transmissions and manual or other non-standard transmissions.

Why TPAs are Needed

As noted above, the transactions standards only cover part of the information that trading partners need in order to transact efficiently, or at all. Generally, the standards mandate the format and elements, but contain no requirements about how the transaction is received, or what is done with the transaction after it is received.

(1) The standards still have flexibility. Many data elements in the standards are “situational” meaning they are required if a given situation is met. Sometimes trading partners must have information from the other party (generally the payer) to know if a situation is met. An example is the provider taxonomy code element. This element is only required if required by the payer. Additionally, some functions are optional or have optional methods. Examples include coordination of benefits and batch versus real time processing. A TPA can specify processing functions and requirements such as this.

(2) The standards do not address some issues at all. While the standards do address format and data content, the standards do not address issues such as connectivity. The method by which trading partners can accept and send transactions (which may be different or multiple ways for some transactions or trading partners) needs to be specified. For example, identification of clearinghouses or other third parties used, and for which transactions; whether direct data entry is supported; whether disks or other media, dial-up connectivity, or other electronic connectivity is supported; whether any additional, non-standard communication methods are supported and any restrictions or required formats, etc.

(3) Other transaction-related issues. Testing requirements or timelines also need to be specified, as well as any telecommunications cost issues.

V. Business Associate Contract

Summary

Both the Business Associate Contract (BAC) and Business Associates (BA) are defined in the HIPAA regulation. BAC are used to require entities that are performing work for you to adhere to the same privacy requirements. BAC language is required prior to disclosing to, or allowing your business associate to collect on your behalf, protected health information.

The BAC format is prescribed by the regulation: it must be a written contract, or if between two governmental entities it may be a written memorandum of understanding. The regulation contains mandatory elements that must be present, but does not require the BAC to be a separate contract.

Business associate contract provisions are not generally needed with trading partner agreement provisions.

Regulation

Introduction

Business associates are entities that perform functions for, or assist the covered entity in activities that involve access to protected health information. Certain functions or services are listed: assistance with claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and repricing, as well as services such as legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. *The full regulatory text is in Appendix A.*

The covered entity must have a written BAC in order to meet the “satisfactory assurance that the business associate will appropriately safeguard the information”

required by the regulation. *The full regulatory text is in Appendix A.* BAC required elements are:

- establish permitted and required uses and disclosures
- provide that the BA will not use or further disclose information other than what is permitted in the contract or required by law
- use appropriate safeguards to prevent use or disclosure of the information other than as allowed by the contract
- report to the covered entity any use or disclosure not provided for under the contract
- ensure that any agents, or subcontractors agree to the same terms for information covered under the contract
- make protected health information available for accounting, amendments, and individual access
- make internal books and practices related to handling of health information available to the Secretary of HHS
- return or destroy all protected health information at termination, or if not feasible, extend the contract protections and limit further use.
- Authorize termination for findings of violation of material terms

New Security related provisions that need to be added:

- 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 covered entity as required by this subpart,
- Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it,
- Report to the covered entity any security incident of which it becomes aware.

BAC Considerations

Designations of BA should be carefully considered because BAC regulatory provisions place requirements on both the covered entity and the business associate. For example, covered entities must be able to include business associate disclosures in an accounting to an individual. On the other hand, business associates must agree to restrict date for purposes related to the contract only, report any other uses or disclosures, and make internal records available to the Secretary of HHS.

An entity must balance the desire for uniformity against the additional legal and regulatory obligations that are acquired when designating an entity a BA. The Covered entity can still place some general requirements to have appropriate safeguards against unauthorized use or disclosure of protected health information in contracts with non-BA.

VI. Data Use Agreement (for the Limited Data Set, LDS)

Summary

The amended privacy rule, published on August 14, 2002, creates a new standard for information that is not completely de-identified for certain uses and disclosures only. In response to requests from researchers and the public health sector specifically, HHS sought to make certain uses and disclosures of information that was not completely de-identified less onerous. Of course, an entity may still de-identify data – using the safe harbor and eliminating the specific identifiers listed in the regulation or by using a statistician to certify that the risk of re-identification is very small and then use or disclose the information for any purpose. Additionally, PHI that is not de-identified can still be disclosed for other purposes allowed in the regulation, like treatment, payment, health care operations, as required by law, and others.

Regulation

The amended rule allows the additional ability to use or disclose slightly more information than the de-identified set in a "limited data set," for the purpose of research, public health or health care operations. The limited data set must exclude 16 specified identifiers that are listed in the rule, and the covered entity must enter into a data use agreement with the recipient of the limited data set. 164.514(e)

A limited data set is PHI that excludes specific, readily identifiable information, not only about the individuals themselves, but also their relatives, employers, and members of their households. The final rule specifies the 16 identifiers which must be excluded. (What would be allowed in the limited data set but not in the de-identified data is geographic information including town, city, county, state, zip-code though not street address, and dates such as date of birth and date of service).

To use or disclosure the limited data set, for the purpose of research, public health or health care operations only, a covered entity must enter into a data use agreement with the recipient of the information. 164.514(e)(4). The agreement must:

- Establish the permitted uses and disclosures of the limited data set by the recipient and consistent with the regulatory limitations
- Establish who is permitted to use or receive the limited data set
- Provide that the recipient will not use or further disclose the information other than as provided in the agreement or as required by law, use appropriate safeguards to prevent uses and disclosures not permitted; report use or disclosure not provided for in the agreement; ensure that any agents and subcontractors who receive the information agree to the same conditions; and
- Not identify the information or contact the individuals.

The covered entity must also take reasonable steps to cure any breaches by recipients that it becomes aware of. 164.514(e)(4)(iii). The covered entity can use PHI to create the limited data set or disclose PHI to a business associate, for the purpose of creating a limited data set. 164.512(e)(3). Finally, the disclosure of PHI in a limited data set need not be included in any accounting of disclosures provided to the individual. 164.528.

LDS Considerations

While the above elements must be included, the form of the agreement is not specified. Thus, theoretically oral agreements, workforce confidentiality agreements for some internal uses, and less formal memorandums of understanding or other arrangements are sufficient. However, a formal, written, signed, and dated contract would be the most conservative approach. It is recommended that the agreement be in writing so that compliance, but all elements of a contract may or may not be present.

LDS agreements will only be necessary where the covered entity is using or disclosing information:

- That is not fully de-identified, and
- That is not otherwise allowed by the regulation, and
- For the purpose of research, public health, or health care operations

Generally, then, limited data set agreements will not be needed to for data exchanges with business associates or with trading partners.

APPENDIX A

Trading Partner Agreement Issues

Due to the individual nature of TPA, guidance on the content of a trading partner agreement is not addressed in the document, except as it relates to requirements and usage considerations. However, a good place to look at sample documents that include TPA content is the Medicare website that has instructions to its carriers and companion documents, as well as other communications about HIPAA at: <http://www.hcfa.gov/medicare/edi/hipaadoc.htm>.

The format of a trading partner agreement is not regulated. It can be part of a larger agreement or stand alone. Further, since it is not required nor format prescribed, there are no limitations on the form of the provisions. This gives agencies much needed flexibility. Trading partner agreement provisions might take the form of a formal agreement, a provider agreement addenda, an informational guide or companion document, an agency memorandum or bulletin, billing instructions, agency regulations, or some combination.

Currently many public agencies provide instructions to trading partners regarding how to bill for services (what codes, when, cycles), inquire about eligibility, what communication methods to use, managed care transaction requirements, etc. Agencies should give thought to their current method and approach to communicating such details. If that method is workable and familiar, change appears unnecessary. Consider the following issues when deciding on format:

- Current communication method advantages and disadvantages
- Amount of resources to maintain additional formats or agreements
- Time and resources required to change or update when new transaction requirements or communication methods require it
- Binding effect on trading partners
- Desirability of combining with other agreements or with other HIPAA requirements

Business Associate Regulatory Provisions

§160.103 Business associate: (1) Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in Sec. 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in Sec. 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such

organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.

(3) A covered entity may be a business associate of another covered entity.

§164.308(b)(1) [Security] Standard: Business associate contracts and other arrangements. A covered entity, in accordance with § 164.306, 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.

(2) This standard does not apply with respect to—

(i) The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual.

(ii) The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met; or

(iii) The transmission of electronic protected health information from or to other agencies providing the services at § 164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)(C) are met.

(3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).

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

(a)(1) *Standard: Business associate contracts or other arrangements.*

(i) The contract or other arrangement between the covered entity and its business associate required by 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an 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—

(A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.

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

(A) 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 covered entity as required by this subpart;

(B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) 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.

(ii) *Other arrangements.* (A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if—

(1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or (2) 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 (a)(2)(i) of this section.

(B) 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 as specified in § 160.103 of this subchapter

to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit

electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained.

(C) The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph (a)(2)(i)(D) of this section if such authorization is inconsistent with the statutory obligations of the covered entity or its 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, including a subcontractor, 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.

§164.502(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 or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

(ii) This standard does not apply: (A) With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual; (B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of Sec. 164.504(f) apply and are met; or (C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

(iii) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and Sec. 164.504(e).

(2) *Implementation specification: documentation.* A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of Sec. 164.504(e).

§164.504(e)(1) Standard: Business associate contracts. (i) The contract or other arrangement between the covered entity and the business associate required by Sec. 164.502(e)(2) must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in Sec. 164.502(e) and paragraph (e) of this section, 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: (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.

(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 such 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 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; (D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees 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 Sec. 164.524; (F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with Sec. 164.526; (G) Make available the information required to provide an accounting of disclosures in accordance with Sec. 164.528; (H) 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 (I) 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 paragraph (e) of this section 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. (B) The covered entity may comply with paragraph (e) of this section, 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.

(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 Sec. 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 (e), provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(3)(i) of this section, 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.

(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 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 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 used or further disclosed only as required by law or for the purpose 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.

Privacy NPRM: Model Business Associate Contract

Appendix to the Preamble—Model Business Associate Contract Provisions

Introduction

The Department of Health and Human Services provides these model business associate contract provisions in response to numerous requests for guidance. This is only model language. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these model provisions is not required for compliance with the Privacy Rule. The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate. These or similar provisions may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate business associate agreement. These provisions only address concepts and requirements set forth in the Privacy Rule and alone are not sufficient to result in a binding contract under State law and do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this model is not sufficient for compliance with state law and does not replace consultation with a lawyer or negotiations between the parties to the contract. Furthermore, a covered entity may want to include other provisions that are related to the Privacy Rule but that are not required by the Privacy Rule. For example, a covered entity may want to add provisions in a business associate contract in order for the covered entity to be able to rely on the business associate to help the covered entity meet its obligations under the Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically addressed in these model provisions. For example, the Privacy Rule does not preclude a business associate from disclosing protected health information to report unlawful conduct in accordance with § 164.502(j). However, there is not a specific model provision related to this permissive disclosure. These and other types of issues will need to be worked out between the parties.

Model Business Associate Contract Provisions I

Definitions (alternative approaches)

Catch-all definition: Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 CFR 160.103 and 164.501.

Examples of specific definitions: (a) *Business Associate.* “Business Associate” shall mean [Insert Name of Business Associate]. (b) *Covered Entity.* “Covered Entity” shall mean [Insert Name of Covered Entity]. (c) *Individual.* “Individual” shall have the same meaning as the term “individual” in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g). (d) *Privacy Rule.* “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E. (e) *Protected Health Information.* “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity. (f) *Required By Law.* “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR 164.501. (g) *Secretary.* “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.

Obligations and Activities of Business Associate

- (a) Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.
- (b) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
- (c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement. [This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages by a Business Associate.]
- (d) Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement.
- (e) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
- (f) Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner designated by Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]
- (g) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity. [Not necessary if business associate does not have protected health information in a designated record set.]
- (h) Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity to the Secretary, in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
- (i) Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.
- (j) Business Associate agrees to provide to Covered Entity or an Individual, in time and manner designated by Covered Entity, information collected in accordance with Section [Insert Section Number in Contract Where Provision (i) Appears] of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

Permitted Uses and Disclosures by Business Associate

General Use and Disclosure Provisions (alternative approaches)

Specify purposes:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity: [List Purposes].

Refer to underlying services agreement:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of Services Agreement], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity.

Specific Use and Disclosure Provisions [only necessary if parties wish to allow Business Associate to engage in such activities]

- (a) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(b) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(c) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR 164.504(e)(2)(i)(B).

Obligations of Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement] (a) Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

(b) Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522. Permissible Requests by Covered Entity Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate].

Term and Termination

(a) *Term.* The Term of this Agreement shall be effective as of [Insert Effective Date], and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

(b) *Termination for Cause.* Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the II Agreement/sections II of the II Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, or immediately terminate this Agreement [and the II Agreement/sections II of the II Agreement] if Business associate has breached a material term of this Agreement and cure is not possible. [Bracketed language in this provision may be necessary if there is an underlying services agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

(c) *Effect of Termination.* (1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(2) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such protected Health Information.

Miscellaneous

(a) *Regulatory References.* A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended, and for which compliance is required.

(b) *Amendment.* The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act, Public Law 104–191.

(c) *Survival.* The respective rights and obligations of Business Associate under Section [Insert Section Number Related to “Effect of Termination”] of this Agreement shall survive the termination of this Agreement.

(d) *Interpretation.* Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rule.