

provided that they meet the requirements of the Privacy Rule.

Comment: Another commenter indicated that the sample language should not require the return or destruction of protected health information in the possession of subcontractors or agents of the business associate.

Response: We have retained this language as this is consistent with the Privacy Rule. Section 164.504(e)(2)(ii)(D) requires that the business associate contract include a provision that the business associate ensures that any agents, including subcontractors, agree to the same restrictions and conditions as the business associate. Generally, the contract must require the business associate to return or destroy protected health information; therefore, the contract also must require the business associate to have agents and subcontractors to do the same. This is reflected in the sample contract language.

Comment: One commenter requested that the sample language include a provision that the covered entity may impose monetary damages on a business associate for violation of its privacy policies.

Response: We have not included such a provision because the Privacy Rule does not address this issue. The Privacy Rule would not prohibit a monetary damages provision from being included in the contract. This, again, is a matter to be negotiated between covered entities and their business associates.

Comment: One commenter suggested that specific references to sections in the Rule be deleted and either replaced by a general statement that the contract shall be interpreted in a manner consistent with the Rule or supplemented with clarifying language with examples.

Response: We believe that using section reference is a valid and expeditious approach as it incorporates changes as modifications are made to the Privacy Rule. A business associate contract may take a different approach than using section references to the Privacy Rule.

Comment: One commenter asked that the sample business associate contract provisions be included in the Rule rather than published as an appendix to the preamble so that it will be in the Code of Federal Regulations.

Response: We have published the sample business associate contract provisions as an appendix to the preamble because they are meant as guidance. The sample language shall be available on the Office for Civil Rights

web site at www.hhs.gov/ocr/hipaa; and may be updated or revised as necessary.

Appendix to the Preamble—Sample Business Associate Contract Provisions

Statement of Intent

The Department provides these sample business associate contract provisions in response to numerous requests for guidance. This is only sample 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 sample 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. They do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this sample 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 sample provisions, for example having a business associate create a limited data set. These and other types of issues will need to be worked out between the parties.

Sample Business Associate Contract Provisions³

Definitions (Alternative Approaches)

Catch-all definition:

³ Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions and are not intended to be included in the contractual provisions.

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

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 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 to 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 of which it becomes aware.

(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 [Insert negotiated terms], 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 [Insert negotiated terms]. [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, including policies and procedures and Protected Health Information, 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] to the Secretary, in a time and manner [Insert negotiated terms] or designated by 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 [Insert negotiated terms], 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 [(a) and (b) are alternative approaches]

(a) *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 or the minimum necessary policies and procedures of the Covered Entity: [List Purposes].

(b) *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 or the minimum necessary policies and procedures of the 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).

(d) Business Associate may use Protected Health Information to report violations of law to appropriate Federal

and State authorities, consistent with § 164.502(j)(1).

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 notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

(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, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

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. [Term may differ.]

(b) *Termination for Cause.* Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

(1) Provide an opportunity for Business Associate to cure the breach or

end the violation and terminate this Agreement [and the ___ Agreement/ sections ___ of the ___ Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

(2) Immediately terminate this Agreement [and the ___ Agreement/ sections ___ of the ___ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible; or

(3) If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary. [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 [Insert negotiated terms] 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.

(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 of 1996, Pub. L. No. 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 to permit Covered Entity to comply with the Privacy Rule.

List of Subjects

45 CFR Part 160

Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Medicaid, Medical research, Medicare, Privacy, Reporting and record keeping requirements.

45 CFR Part 164

Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Medicaid, Medical research, Medicare, Privacy, Reporting and record keeping requirements.

Dated: August 6, 2002.

Tommy G. Thompson,
Secretary.

For the reasons set forth in the preamble, the Department amends 45 CFR subtitle A, subchapter C, as follows:

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

1. The authority citation for part 160 continues to read as follows:

Authority: Sec. 1171 through 1179 of the Social Security Act (42 U.S.C. 1320d-1329d-8), as added by sec. 262 of Pub. L. No. 104-191, 110 Stat. 2021-2031 and sec. 264 of Pub. L. No. 104-191 (42 U.S.C. 1320d-2(note)).

2. Amend § 160.102(b), by removing the phrase "section 201(a)(5) of the Health Insurance Portability Act of 1996, (Pub. L. No. 104-191)" and adding in its place the phrase "the Social Security Act, 42 U.S.C. 1320a-7c(a)(5)".

3. In § 160.103 add the definition of "individually identifiable health information" in alphabetical order to read as follows:

§ 160.103 Definitions.

* * * * *

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or

condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

- (i) That identifies the individual; or
- (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

* * * * *

4. In § 160.202 revise paragraphs (2) and (4) of the definition of "more stringent" to read as follows:

§ 160.202 Definitions.

* * * * *

More stringent means * * *

(2) With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable.

* * * * *

(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

* * * * *

5. Amend § 160.203(b) by adding the words "individually identifiable" before the word "health".

PART 164—SECURITY AND PRIVACY

Subpart E—Privacy of Individually Identifiable Health Information

1. The authority citation for part 164 continues to read as follows:

Authority: 42 U.S.C. 1320d-2 and 1320d-4, sec. 264 of Pub. L. No. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2(note)).

2. Amend § 164.102 by removing the words "implementation standards" and adding in its place the words "implementation specifications."

3. In § 164.500, remove "consent," from paragraph (b)(1)(v).

4. Amend § 164.501 as follows:

a. In the definition of "health care operations" remove from the introductory text of the definition " , and any of the following activities of an