

information.

Solicitation of Comment

The Department is aware of the importance of the activities described by the commenters but is not currently convinced of the need to modify the safe harbor standard for de-identified information. Instead, the Department requests comment on an alternative approach that would permit uses and disclosures of a limited data set which does not include facially identifiable information but in which certain identifiers would remain. The Department is not considering permitting the disclosure of any such limited data set for general purposes, but rather is considering permitting disclosure of such information for research, public health, and health care operations purposes.

The limited data set would not include the following information, which the Department considers direct identifiers: name, street address, telephone and fax numbers, e-mail address, social security number, certificate/license number, vehicle identifiers and serial numbers, URLs and IP addresses, and full face photos and any other comparable images. The limited data set would include the following identifiable information: admission, discharge, and service dates; date of death; age (including age 90 or over); and five-digit zip code. The Department solicits comment on whether another one or more geographic units smaller than State, such as city, county, precinct, neighborhood or other unit, would be needed in addition to, or be preferable to, five-digit zip code.

In addition, to address concerns raised by commenters regarding access to birth date for research or other studies relating to young children or infants, the Department

clarifies that the Privacy Rule does not prohibit age of an individual from being expressed as an age in months, days, or hours. Given that the limited data set would include all ages, including age in months, days, or hours, if preferable, the Department requests comment on whether date of birth is needed and, if so, whether the entire date is needed, or just the month and year.

In addition, to further protect privacy, the Department would propose to condition the disclosure of the limited data set on covered entities obtaining from the recipients a data use or similar agreement, in which the recipient would agree to limit the use of the limited data set to the specified purposes in the Privacy Rule, and limit who can use or receive the data, as well as agree not to re-identify the data or contact the individuals. Commenters seemed to indicate that recipients would be amenable to such conditions.

The Department solicits public comment on the feasibility and acceptability of the above approach for the described purposes, and whether or not the limitations and conditions would be sufficiently protective of patient privacy.

Proposed Modifications

In addition to the solicitation of comment above, the Department proposes a technical modification to the safe harbor provisions. A number of commenters expressed confusion regarding what was believed to be conflicting provisions within the de-identification standard. Commenters argued that, on the one hand, the Privacy Rule treats information as de-identified if all listed identifiers on the information are stripped, including any unique, identifying number, characteristic, or code. Yet, the Privacy Rule

permits a covered entity to assign a code or other record identification to the information so that it may be re-identified by the covered entity at some later date.

The Department did not intend the re-identification code to be considered one of the enumerated identifiers. Therefore, the Department proposes to clarify its intent by explicitly excepting the re-identification code or other means of record identification permitted by § 164.514(c) from the listed identifiers at § 164.514(b)(2)(i)(R).

J. Technical Corrections and Other Clarifications

In addition to the modifications described above, the Department proposes to make the following clarifications:

1. Changes of Legal Ownership. The Privacy Rule's definition of health care operations, at 164.501, includes business management and general administrative activities of the entity, including, due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity.

In the preamble to the Privacy Rule, the Department explained that this language was included to remedy an omission in the 1999 proposed Rule by

add[ing] to the definition of health care operations disclosures of protected health information for due diligence to a covered entity that is a potential successor in interest. This provision includes disclosures pursuant to the sale of a covered entity's business as a going concern, mergers, acquisitions, consolidations, and other similar types of corporate restructuring between covered entities, including a

division of a covered entity, and to an entity that is not a covered entity but will become a covered entity if the reorganization or sale is completed.

65 FR at 82609 (December 28, 2000) (response to comment); see also 65 FR at 82491 (similar language); 65 FR at 82652 (“We clarify in the definition of health care operations that a covered entity may sell or transfer its assets, including protected health information, to a successor in interest that is or will become a covered entity.”)

Despite language in the preamble to the contrary, the definition of health care operations in the Privacy Rule does not expressly provide for the transfer of protected health information upon sale or transfer to a successor in interest. Instead, the definition of “health care operations” only mentions disclosures of protected health information for “due diligence” purposes when a sale or transfer to a successor in interest is contemplated. “Due diligence” is generally understood to mean the “[a] prospective buyer's or broker's investigation and analysis of a target company, a piece of property, or a newly issued security.” Black’s Law Dictionary (7th ed. 1999) *available in* Westlaw, DIBLACK database.

The Department proposes to add language to paragraph (6) of the definition of “health care operations” to clarify the intent to permit the transfer of records to a covered entity upon a sale, transfer, merger, or consolidation. This proposed change would prevent the Privacy Rule from interfering with necessary treatment or payment activities upon the sale of a covered entity or its assets.

The Department also proposes to use the terms “sale, transfer, consolidation or

merger” to eliminate the term “successor in interest” from this paragraph. The Department intended this provision to apply to any sale, transfer, merger or consolidation and believes the current language may not sufficiently accomplish this goal. The proposed language’s use of the terms “sale, transfer, merger and consolidation” is based on language used in model State laws addressing the disclosure of personal or privileged information collected or received in connection with an insurance transaction.

The Department retains the limitation that such disclosures are health care operations only to the extent the entity receiving the protected health information is a covered entity or will become a covered entity as a result of the sale, transfer, merger, or consolidation. In addition, the proposed modification does not affect any responsibility of covered entities either under other law or ethical obligation to notify individuals appropriately of a sale, transfer, merger, or consolidation.

2. Group Health Plan Disclosures of Enrollment and Disenrollment Information to Plan Sponsors. The Department proposes to modify the Privacy Rule to make express the Department’s policy, which was explained in the preamble to the Privacy Rule, that group health plans are permitted to share enrollment and disenrollment information with plan sponsors without amending plan documents. Under the Privacy Rule, a group health plan, as well as a health insurance issuer or HMO providing health insurance or health coverage to the group health plan, are covered entities. Neither employers nor other plan sponsors are defined as covered entities. The Department recognizes the legitimate need of the plan sponsor to have access to health information of these covered entities in certain situations.

Therefore, the Privacy Rule at § 164.504(f) permits a group health plan, and health insurance issuers or HMOs with respect to the group health plan, to disclose protected health information to the plan sponsor provided that, among other requirements, the plan documents are amended to appropriately reflect and restrict the plan sponsor's uses and disclosures of such information.

There are two exceptions where the Privacy Rule permits group health plans (or health insurance issuers or HMOs, as appropriate) to disclose information to a plan sponsor without requiring amendment of plan documents. First, § 164.504(f) permits such disclosures when the information needed by the plan sponsor is summary health information. Second, as explained in the preamble to the Privacy Rule, a plan sponsor is permitted to perform enrollment functions on behalf of its employees without meeting the requirements of § 164.504(f), as such functions are considered outside of the plan administration functions. Therefore, a group health plan is also permitted to disclose enrollment or disenrollment information to the plan sponsor without amending the plan documents as required by § 164.504(f).

However, this policy regarding disclosures of enrollment or disenrollment information was addressed only in the preamble to the Privacy Rule and not explicitly in the regulation itself. As a result, the policy seems to have been overlooked and the absence of a specific provision in the regulation itself has caused misinterpretation within industry. To remedy this misunderstanding and make its policy clear, the Department proposes to add an explicit exception at § 164.504(f)(1)(iii) to clarify that group health plans (or health insurance issuers or HMOs, as appropriate) are permitted to disclose

enrollment or disenrollment information to a plan sponsor without meeting the plan document amendment and other related requirements.

3. Definition of “Individually Identifiable Health Information.” The Department proposes to move the definition of “individually identifiable health information” from § 164.501 to § 160.103 to clarify that the definition is relevant to all of the provisions in Parts 160 through 164.

4. Accounting of Disclosures of Protected Health Information. Under the Privacy Rule at § 164.528, individuals have the right to receive an accounting of disclosures of protected health information made by the covered entity, with certain exceptions. These exceptions, or instances where a covered entity is not required to account for disclosures, include disclosures made by the covered entity to carry out treatment, payment, or health care operations, as well as disclosures to individuals of protected health information about them.

The accounting is required to include the following: (1) disclosures of protected health information that occurred during the six years prior to the date of the request for an accounting, including disclosures to or by a business associate of the covered entity; (2) for each disclosure: the date of the disclosure; the name of the entity or person who received the protected health information; if known, the address of such entity or person; a brief description of the protected health information disclosed; and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the

disclosure, or in lieu of such a statement, a copy of the individual's written authorization pursuant to § 164.508 or a copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512. For multiple disclosures of protected health information to the same person, the Privacy Rule allows covered entities to provide individuals with an accounting that contains only the following information: (1) for the first disclosure, a full accounting, with the elements described in (2) above; (2) the frequency, periodicity, or number of disclosures made during the accounting period; and (3) the date of the last such disclosure made during the accounting period.

A number of commenters raised concerns that the high costs and administrative burdens associated with the accounting requirements would deter covered entities from disclosing protected health information. In response to these concerns, the Department proposes to expand the exceptions to the standard at § 164.528(a)(1) to include disclosures made pursuant to an authorization as provided in § 164.508. Covered entities would no longer be required to account for any disclosures authorized by the individual in accordance with § 164.508. The Department is proposing to alleviate burden in this way because it is believed that an accounting of disclosures made pursuant to such permissions is unnecessary because such disclosures are already known by the individual, in as much as the individual was required to sign the forms authorizing the disclosures.

Accordingly, the Department proposes to make two conforming amendments at §§ 164.528(b)(2)(iv) and (b)(3) to delete references in the accounting content requirements to disclosures made pursuant to an authorization.

5. Uses and Disclosures Regarding FDA-regulated Products and Activities. The Department recognizes the importance of public health activities and, in the Privacy Rule, allows information to be used and disclosed for these purposes without requiring individual consent or authorization. The recent anthrax attacks and the threat of other forms of bio-terrorism have served to underscore the vital necessity of a strong and effective public health system. The Rule allows covered entities to disclose protected health information to public health authorities for a broad array of public health purposes, including reporting of diseases, injuries, vital statistics, and for the conduct of public health surveillance and interventions. The Rule permits public health reporting to private persons who are contractors for or agents of the public health authority. The Rule also recognizes the essential role of manufacturers and other private persons in carrying out the Food and Drug Administration's (FDA) public health mission.

The Privacy Rule, at § 164.512(b)(1)(iii), specifically permits covered entities to disclose protected health information, without individual authorization, to a person who is subject to the jurisdiction of the FDA for the following specified purposes: (1) to report adverse events, defects or problems, or biological product deviations with respect to products regulated by the FDA (if the disclosure is made to the person required or directed to report such information to the FDA), (2) to track products (if the disclosure is made to the person required or directed to report such information to the FDA), (3) for product recalls, repairs, or replacement, and (4) for conducting post-marketing surveillance to comply with FDA requirements or at the direction of the FDA.

The Department received a number of comments on the provisions for public

health activities related to FDA-regulated products. The majority of these commenters were concerned that the Privacy Rule constrains important public health surveillance and reporting activities by impeding the flow of needed information to those subject to the FDA's jurisdiction. In particular, commenters noted that limiting disclosures to those that are "required or directed" by FDA does not reflect the breadth of public health activities that are currently being conducted by the private sector on a voluntary basis or under the general auspices of – but not at the direction of – FDA. In general, commenters were concerned that such limitations would stifle current reporting practices. For example, the FDA currently obtains the vast majority of its information about drugs and devices indirectly from health care providers who voluntarily report known adverse events or problems to the manufacturer of the product. The manufacturer may or may not be required to report such adverse events to FDA. Commenters assert that the present language of the Privacy Rule will have a "chilling effect" on these important communications due to uncertainty over the manufacturer's obligation to report to the FDA.

Some concern was expressed about the potential liability of a covered entity for a disclosure to an employee of the manufacturer who is not "a person subject to the jurisdiction of the FDA" or to the wrong manufacturer. The Department seeks to assure covered entities that use of the term "a person" was not intended to limit reporting to a single individual within an entity, but to allow reporting to flow as it does today between health care providers and representatives of manufacturers or other companies. Moreover, the Department seeks to clarify that covered entities may continue to disclose protected

health information to the companies identified on the product labels as the manufacturer registered with the FDA to distribute the product.

To eliminate the “chilling effect” of the Rule, some commenters requested that the Department include in the Rule a “good-faith” safe harbor to protect covered entities from enforcement actions arising from unintentional violations of the Privacy Rule. For example, a health care provider would not have violated the Rule if the disclosure was made in the good faith belief that the entity to whom the adverse event was report was responsible for the FDA-regulated product, even if it turned out to be the wrong manufacturer.

Finally, a number of commenters, including some that are subject to the FDA’s jurisdiction, suggested that: identifiable health information is not necessary for some or all of these public health reporting purposes; that identifiable health information is not reported to FDA; and that for purposes of post-marketing surveillance, information without direct identifiers (such as name, mailing address, phone number, social security number, and email address) should suffice. The Department recognizes that there must be a balance between the need for public health activities that benefit every individual by safeguarding the effectiveness, safety, and quality of the products regulated by the FDA, and the privacy interests of specific individuals. However, the comments did not offer a consensus as to which activities could be performed without identifiable information or which identifiers, if any, were needed. In Section III.I of this preamble regarding De-identification issues, the Department is soliciting comments on a limited data set for use for specific purposes, including public health. The Department also requests comments as

to whether this limited data set should be required or permitted for some or all public health purposes or if a special rule should be developed for public health reporting.

The Department did not intend the Privacy Rule to discourage or prevent the reporting of adverse events or otherwise disrupt the flow of essential information that FDA and persons subject to the jurisdiction of FDA need in order to carry out their important public health activities. Therefore, the Department proposes a number of changes to eliminate uncertainties identified by the commenters, and, thereby, encourage covered entities to continue to report and cooperate in these essential public health activities. The proposed modifications attempt to recognize and preserve current public health activities of persons subject to the jurisdiction of the FDA while not diminishing the health information privacy protections for individuals.

Specifically, the Department proposes to remove from §§ 164.512(b)(1)(iii)(A) and (B) the phrase “if the disclosure is made to a person required or directed to report such information to the Food and Drug Administration” and to remove from subparagraph (D) the phrase “to comply with requirements or at the direction of the Food and Drug Administration.” In lieu of this language, HHS proposes to describe at the outset the public health purposes for which disclosures may be made. The proposed language reads: “A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity.”

The Department proposes to retain the listing of specific activities identified in

paragraphs (A), (B), (C), and (D), to give covered entities additional assurance that public health disclosures for these activities are permissible under the Privacy Rule. The listing, however, is no longer an exclusive list of FDA-related public health activities, but rather is a list of examples of the most common activities. Additionally, language has been added to paragraph (C) to include “lookback” activities which are necessary for tracking blood and plasma products, as well as quarantining tainted blood or plasma and notifying recipients of such tainted products.

The privacy of individuals’ health information would continue to be protected through the limitations placed on the permissible disclosures for FDA purposes. Specifically, such disclosures must relate to FDA-regulated products or activities for which the person using or receiving the information has responsibility, and for activities related to the safety, effectiveness, or quality of such FDA-regulated product or activity.

The Department is not proposing a good-faith safe harbor at this time because it believes that these proposed modifications will adequately address the concerns and uncertainties facing covered entities. However, the Department is interested in hearing from affected parties as to whether the proposed modifications are adequate or if additional measures are necessary for health care providers or others to continue to report this vital information about FDA-regulated products or activities.

6. Hybrid Entities. The Privacy Rule defines covered entities that primarily engage in activities that are not covered functions—i.e., functions that relate to the entity’s operation as a health plan, health care provider, or health care clearinghouse—as hybrid

entities. See § 164.504(a). In order to limit the burden on such entities, most of the requirements of the Privacy Rule only apply to the health care component(s) of the hybrid entity and not to the parts of the entity that do not engage in covered functions. The health care component(s) include those components of the entity that perform covered functions and other components of the entity that support those covered functions, in the same way such support may be provided by a business associate. A covered entity that is a hybrid entity is required to define and designate those parts of the entity that engage in the covered functions and “business associate” functions and that are, therefore, part of the health care component(s). The health care component is designed to include components that engage in “business associate” functions because it is impossible for the entity to contract with itself and the authorization requirement would limit the ability to engage in necessary health care operations functions.

The hybrid entity is also required to create adequate separation (i.e., fire walls) between the health care component(s) and other components of the entity. Transfer of protected health information held by the health care component to other components of the hybrid entity is a disclosure under the Privacy Rule and is only allowed to the same extent as such disclosure would be permitted to a separate entity.

Examples of hybrid entities are: (1) corporations that are not in the health care industry, but that operate on-site health clinics, and (2) insurance carriers that have multiple lines of business which include both health insurance and other insurance lines such as general liability or property and casualty insurance.

A “hybrid entity” is defined in the Privacy Rule as an entity “whose covered

functions are not its primary functions.” (emphasis added). In the preamble to the Privacy Rule, the Department explained that the use of the term “primary” in the definition of a “hybrid entity” was not intended to operate with mathematical precision. The Department intended a common sense evaluation of whether the covered entity mostly operates as a health plan, health care provider, or health care clearinghouse. If an entity’s primary activity was engaging in covered functions, then the whole entity would be a covered entity and the hybrid entity provisions would not apply. However, if the covered entity primarily conducted non-health activities, it would qualify as a hybrid entity and would be required to comply with the Privacy Rule with respect to its health care component(s). Commenters expressed concern that the policy guidance in the preamble was insufficient as long as the Privacy Rule itself limited the hybrid entity provisions to entities that primarily conducted non-health related activities. There were particular concerns in cases in which the health plan line of business was the primary business, and the line of business that is one of the excepted benefits, e.g., workers’ compensation insurance, was only a small portion of the business. There were also concerns about what “primary” meant if not a mathematical calculation and how the entity would know whether or not it was a hybrid entity based on the guidance in the preamble.

As a result of these comments, the Department proposes to delete the term “primary” from the definition of “hybrid entity” in § 164.504(a). In order to avoid the problem of line drawing, the Department proposes to permit any covered entity to be a hybrid entity if it is a single legal entity that performs both covered and non-covered functions, regardless of whether the non-covered functions represent that entity’s primary

function, a substantial function, or even a small portion of the entity's activities.

The Department proposes to permit covered entities that could qualify as hybrid entities to choose whether or not they want to be hybrid entities. Elimination of the requirement in the definition of "hybrid entity" that covered functions not be the "primary" functions of the covered entity would greatly increase the proportion of covered entities that are hybrid entities. In order to avoid the burden of requiring many more covered entities to designate the health care components and create fire walls within their entity when it is administratively simpler to treat the entire entity as a covered entity, the proposal would allow the covered entity to choose whether it will be a hybrid entity or not. To accomplish this objective, the proposed definition of "hybrid entity" would require that in order to be a hybrid entity, a covered entity that otherwise qualifies must designate health care components. If a covered entity does not designate health care components, the entire entity would be a covered entity.

There are advantages and disadvantages to being a hybrid entity. Whether or not the advantages outweigh the disadvantages will be a decision of each covered entity that may qualify as a hybrid entity and will be influenced by factors such as how the entity is organized and the proportion of the entity that must be included in the health care component. Where the non-covered functions of the entity are only a small portion of the entity, it will likely be more efficient to simply consider the entire entity as a covered entity. Nonetheless, the Department is proposing to permit flexibility for covered entities to choose whether or not to be treated as a covered entity entirely or as a hybrid entity.

The Department also proposes to simplify the definition of "health care

component” in § 164.504(a) to make clear that a health care component is whatever the covered entity designates as the health care component, consistent with the provisions regarding designation in § 164.504(c)(3)(iii). The specific language regarding which components make up a health care component would be in the implementation specification that addresses designation of health care components. The Department proposes to move this specific language because it provides requirements and directions that are more appropriately placed in an implementation specification. The Department proposes that health care components may include: (1) components of the covered entity that engage in covered functions, and (2) any component that engages in activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.

With respect to the components that perform covered functions, the Department also clarifies that a hybrid entity must include in its health care component(s) any component that would meet the definition of “covered entity” if it were a separate legal entity. “Covered functions” are those functions of a covered entity that make the entity a health plan, health care provider, or health care clearinghouse. However, there was some ambiguity as to whether a component of a covered entity that is a health care provider, but that does not conduct standard electronic transactions, must be included in the health care component. The proposed language would clarify that any component that would be a covered entity if it were a separate legal entity must be included in the health care component.

Under these proposed changes, a component that is a health care provider and that

engages in standard electronic transactions must be included in the health care component, but a component that is a health care provider but that does not engage in standard electronic transactions may, but would not be required to, be included in the health care component of the hybrid entity. The decision would be left to the covered entity in the second case. For example, in a university setting, the single legal entity may operate hospital facilities that bill electronically and research laboratories that do not engage in any electronic billing. The modification would clarify that the university as a hybrid entity need only include the hospital facilities that bill electronically in the health care component. The modification also would make clear that the university has the option to include the components, such as the research laboratory, that function as a health care provider, but not as a covered health care provider. A covered entity that chooses to include a non-covered health care provider in their health care component would be 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.

There is also a conforming change in the proposed language in § 164.504(c)(1)(ii) to make it clear that a reference to a “covered health care provider” in the Privacy Rule could include the functions of a health care provider who does not engage in electronic transactions, if the covered entity chooses to include such functions in the health care component.

With respect to the language regarding components that engage in “business associate” functions, the Department does not make any substantive change. The components of a hybrid that may provide services to the component that performs covered

functions, such as a portion of the legal or accounting departments of the entity, may be included in the health care component so protected health information can be shared with such components of the entity without requiring business associate agreements or individual authorizations. The related language in paragraph (2)(ii) of the definition of “health care component” in the Privacy Rule that requires the “business associate” functions include the use of protected health information is not included in this proposed Rule because it is redundant.

It is important to note that a covered entity may include components that engage in “business associate” functions in its health care component or not. It is not a violation of the Privacy Rule to fail to include such a component in the health care component designation. However, a disclosure of protected health information from the health care component to such other component if it is not part of the health care component is the same as a disclosure outside the covered entity and is a violation unless it is permitted by the Privacy Rule. Because an entity cannot have a business associate contract with itself, such a disclosure likely would require individual authorization.

Finally, to avoid needless application of the hybrid entity provisions to a covered entity’s activities as an employer, rather than as a health plan, health care provider, or health care clearinghouse, the Department proposes to modify the definition of “protected health information” in § 164.501. The preamble to the Privacy Rule makes clear that the Privacy Rule does not treat employment records as protected health information. To avoid any confusion or misinterpretation on this point, the Department proposes to expressly exclude employment records held by a covered entity in its role as employer

from the definition of “protected health information.” In that way, employment records will be treated in the same manner as student medical records covered by FERPA, which the Privacy Rule excludes from the definition of “protected health information.” This change will limit the need for a covered entity, whose primary activities are covered functions, to designate itself as a hybrid entity simply to carve out employment records.

It is important to note that the exception from the definition of “protected health information” for employment records only applies to individually identifiable health information in those records that are held by a covered entity in its role as employer. The exception does not apply to individually identifiable health information held by a covered entity when carrying out its health plan or health care provider functions. Such information would be protected health information. The Department specifically is soliciting comments on whether the term “employment records” is clear or whether it needs to be more fully explained. It would be particularly helpful if commenters could identify certain types of records that should be included or excluded from “employment records.”

7. Technical Corrections. The Privacy Rule contained some technical and typographical errors. Therefore, the Department proposes to make the following corrections:

a. In § 160.102(b), beginning in the second line, “section 201(a)(5) of the Health Insurance Portability Act of 1996, (Pub. L. 104-191),” is replaced with “42 U.S.C. § 1320a-7c(a)(5)”.

- b. In § 160.203(b), in the second line, “health information” is replaced with “individually identifiable health information”.
- c. In § 164.102, “implementation standards” is corrected to read “implementation specifications.”
- d. In § 164.501, in the definition of “protected health information”, “Family Educational Right and Privacy Act” is corrected to read “Family Educational Rights and Privacy Act.”
- e. In § 164.508(b)(1)(ii), in the fifth line, the word “be” is deleted.
- f. In § 164.508(b)(3)(iii), a comma is added after the words “psychotherapy notes”.
- g. In § 164.510(b)(3), in the third line, the word “for” is deleted.
- h. In § 164.512(b)(1)(v)(A), in the fourth line, the word “a” is deleted.
- i. In § 164.512(b)(1)(v)(C), in the eighth line, the word “and” is added after the semicolon.
- j. In § 164.512(f)(3), paragraphs (ii) and (iii) are redesignated as (i) and (ii), respectively.
- k. In § 164.512(g)(2), in the seventh line, the word “to” is added after the word “directors.”
- l. In § 164.512(i)(1)(iii)(A), in the second line, the word “is” after the word “sought” is deleted.
- m. In § 164.522(a)(1)(v), in the sixth line, “§§164.502(a)(2)(i)” is corrected to read “§§164.502(a)(2)(ii)”.

n. In § 164.530(i)(4)(ii)(A), in the second line, “the requirements” is replaced with the word “specifications”.

IV. Preliminary Regulatory Impact Analysis

Federal law (5 U.S.C. 804(2), as added by section 251 of P. L. 104-21), specifies that a “major rule” is any rule that the Office of Management and Budget finds is likely to result in:

- An annual effect on the economy of \$100 million or more;
- A major increase in costs or prices for consumers, individual industries, federal, State, or local government agencies, or geographic regions; or
- Significant adverse effects in competition, employment, investment productivity, innovation, or on the ability of United States based enterprises to compete with foreign-based enterprises in domestic and export markets.

The impact of the modifications proposed in this rulemaking would be a net reduction of costs associated with the Privacy Rule of approximately \$100 million. Therefore, this Rule is a major rule as defined in 5 U.S.C. 804(2).

Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects; distributive impacts; and equity). According to Executive Order 12866, a regulatory action is “significant” if it meets any one of a number of specified conditions, including having an annual effect on the economy of \$100 million or more, adversely

affecting in a material way a sector of the economy, competition, or jobs, or if it raises novel legal or policy issues. The purpose of the regulatory impact analysis is to assist decision-makers in understanding the potential ramifications of a regulation as it is being developed. The analysis is also intended to assist the public in understanding the general economic ramifications of the regulatory changes.

The Privacy Rule included a regulatory impact analysis (RIA), which estimated the cost of the Privacy Rule at \$17.6 billion over ten years. 65 FR 82462, 82758. The changes to the Privacy Rule proposed by this notice of proposed rulemaking are a result of comment by the industry and the public at large identifying a number of unintended consequences of the Privacy Rule that could adversely affect access to, or the quality of health care delivery. These proposed changes should facilitate implementation and compliance with the Privacy Rule, and lower the costs and burdens associated with the Privacy Rule while maintaining the confidentiality of protected health information.

The proposed changes would affect five areas of the Privacy Rule that will have an economic impact: 1) consent; 2) notice; 3) marketing; 4) research; and 5) business associates. In addition, the proposal contains a number of changes that, though important, can be categorized as clarifications of intended policy. For example, the modifications would permit certain uses and disclosures of protected health information that are incidental to an otherwise permitted use or disclosure. This change would recognize such practices as the need for physicians to talk to patients in semi-private hospital rooms or nurses to communicate with others in public areas, and avoids the costs covered entities might have incurred to reconfigure facilities as necessary to ensure absolute privacy for

these common treatment-related communications. This and other modifications in this proposal (other than those described below) clarify the intent of the standards in the Privacy Rule and, as such, do not change or alter the associated costs that were estimated for the Privacy Rule. There are no new costs or savings by these changes, and therefore, there is no cost estimate made here for them.

A. Summary of Costs and Benefits in Final Regulatory Impact Statement

The Privacy Rule was estimated to produce net costs of \$17.6 billion, with net present value costs of \$11.8 billion (2003 dollars) over ten years (2003-2012). The Department estimates the modifications in this proposal would lower the net cost of the Privacy Rule by approximately \$100 million over ten years.

Measuring both the economic costs and benefits of health information privacy was recognized as a difficult task. The paucity of data and incomplete information on current industry privacy and information system practices made cost estimation a challenge. Benefits were difficult to measure because they are, for the most part, inherently intangible. Therefore, the regulatory impact analysis in the Privacy Rule focused on the key policy areas addressed by the privacy standards, some of which would be affected by the proposed modifications in this rulemaking.

B. Proposed Modifications to Prevent Barriers to Access to or Quality of Health Care

The changes proposed in this rulemaking are intended to address the possible adverse effects of the final privacy standards on an individual's access to, or the quality of,

health care. The modifications touch on five of the key policy areas addressed by the final regulatory impact analysis, including consent, research, marketing, notice, and business associates.

Consent

Under the Privacy Rule, a covered health care provider with a direct treatment relationship with an individual must obtain the individual's prior written consent for use or disclosure of protected health information for treatment, payment, or health care operations, subject to a limited number of exceptions. Other covered health care providers and health plans may obtain such a consent if they so choose. The initial cost of the consent requirement was estimated to be \$42 million. Based on assumptions for growth in the number of patients, the total costs for ten years was estimated to be \$103 million. See 65 FR 82771 (December 28, 2000).²

The proposed modifications would eliminate the consent requirement. The consent requirement posed many difficulties for an individual's access to health care, and was problematic for operations essential for the quality of the health care delivery system. However, any health care provider or health plan may choose to obtain an individual's consent for treatment, payment, and health care operations. The elimination of the consent requirement reduces the initial cost of the privacy standards by \$42 million in the

²The total cost for consent in the regulatory impact analysis showed an initial cost of \$166 million and \$227 million over ten years. Included in these total numbers is the cost of tracking patient requests to restrict the disclosure of their health information. This right is not changed in these modifications. The numbers here represent the costs associated with the consent functions that are proposed to be repealed.

first year and by \$103 million over ten years.

As explained in detail in section III.A.1. above, many comments that the Department received in March 2001 and testimony before the NCVHS revealed that the consent requirements in the Privacy Rule create unintended barriers to timely provision of care, particularly with respect to use and disclosure of health information prior to a health care provider's first face-to-face contact with the individual. These and other barriers discussed above would have entailed costs not anticipated in the economic analyses in the Privacy Rule. These comments also revealed that the consent requirements create administrative burdens, for example, with respect to tracking the status and revocation of consents, that were not foreseen and thus not included in that economic analysis. Therefore, while the estimated costs of the consent provisions were \$103 million, comments have suggested that the costs were likely to be much higher. If these comments are accurate, the cost savings associated with retracting the consent provisions would, therefore, also be significantly higher than \$103 million.

Notice

In eliminating the consent requirement, the Department proposes to preserve the opportunity for a covered health care provider with a direct treatment relationship with an individual to engage in a meaningful communication about the provider's privacy practices and the individual's rights by strengthening the notice requirements. Under the Privacy Rule, these health care providers are required to distribute to individuals their notice of privacy practices no later than the date of the first service delivery after the compliance

date. The modifications would not change this distribution requirement, but would add a new documentation requirement. A covered health care provider with a direct treatment relationship would be required to make a good faith effort to obtain the individual's acknowledgment of receipt of the notice provided at the first service delivery. The form of the acknowledgment is not prescribed and can be as unintrusive as retaining a copy of the notice initialed by the individual. If the provider's good faith effort fails, documentation of the attempt is all that would be required. Since the modification would not require any change in the form of the notice or its distribution, the ten-year cost estimate of \$391 million for these areas in the Privacy Rule's impact analysis remains the same. See 65 FR 82770 (December 28, 2000).

However, the additional effort by direct treatment providers in obtaining and documenting the individual's acknowledgment of receipt of the notice would add costs. This new requirement would attach only to the initial provision of notice by a direct treatment provider to an individual after the compliance date. Under the proposed modification, providers would have considerable flexibility on how to achieve this. Some providers could choose to obtain the required written acknowledgment on a separate piece of paper, while others could take different approaches, such as an initialed check-off sheet or a signature line on the notice itself with the provider keeping a copy.

In the original analysis, the Department estimated that the consent cost would be \$0.05 per page based on the fact that the consent had to be a stand alone document requiring a signature. This proposed modification to the notice requirement would provide greater flexibility and, therefore, greater opportunity to reduce costs compared to

the consent requirement. The Department estimates that the additional cost of the signature requirement, on average, would be \$0.03 per notice. Based on data obtained from the Medical Expenditure Panel Survey (MEPS), which estimate the number of patient visits in a year, the Department estimates that in the first year there would be 816 million notices distributed, including the new additional information needed to acknowledge receipt of the notice. Over the next nine years, the Department estimates, again based on MEPS data, that there would be 5.3 billion visits to health care providers by new patients (established patients will not need to receive another copy of the notice). At \$0.03 per document, the first year cost would be \$24 million and the total cost over ten years would be \$184 million.

Business Associates

The Privacy Rule requires a covered entity to have a written contract, or other arrangement that documents satisfactory assurances that a business associates will appropriately safeguard protected health information in order to disclose protected health information to the business associate. The regulatory impact analysis for the Privacy Rule provided cost estimates for two aspects of this requirement. In the Privacy Rule, \$103 million in first-year costs was estimated for development of a standard business associate contract language. (There were additional costs associated with these requirements related to the technical implementation of new data transfer protocols, but these are not affected by the changes being proposed here.) In addition, \$197 million in first-year costs and \$697 million in total costs over ten years were estimated in the Privacy Rule for the review

and oversight of existing business associate contracts.

The modifications do not change the standards for business associate contracts or the implementation specifications with respect to the covered entity's responsibilities for managing the contracts. However, as part of this proposal, the Department is including model business associate contract language. This model is only suggested language and is not a complete contract. The model language is designed to be adapted to the business arrangement between the covered entity and the business associate and to be incorporated into a contract drafted by the parties. The final regulatory impact analysis assumed the development of such standard language by trade and professional associations. While this has, in fact, been occurring, the Department continues to receive requests for model contract language, particularly from small health care providers. The Department expects that trade and professional associations will continue to provide assistance to their members. However, the model contract language in this proposal will simplify their efforts by providing a base from which they can develop language. The Department had estimated \$103 million in initial year costs for this activity based on the assumption it would require one hour per non-hospital provider and two hours for hospitals and health plans to develop contract language and to tailor the language to the particular needs of the covered entity. The additional time for hospitals and health plans reflected the likelihood that these covered entities would have a more extensive number of business associate relationships. Because there will be less effort expended than originally estimated in the Privacy Rule, the Department estimates a reduction in contract development time by one-third because of the availability of the model language. Thus, the Department now

estimates that this activity will take 40 minutes for non-hospital providers and 80 minutes for hospitals and health plans. The Department estimates that the savings from the proposed business associate contract language would be approximately \$35 million in the first year.

The Department is also proposing in this rulemaking to give covered entities additional time to review their existing business associate contracts and to conform written contracts to the privacy standards. Under the proposal, a covered entity's written business associate contracts, existing at the time the modifications become effective, would be deemed to comply with the privacy standards until such time as the contracts are renewed or modified or until April 14, 2004, whichever is earlier. The effect of this proposal would be to spread first year costs over an additional year, with a corresponding postponement of the costs estimated for the out years. However, the Department has no reliable information as to the number of contracts potentially affected by the modification or how long a delay may occur. Therefore, the Department does not compute any cost savings to this modification.

Marketing

Under §164.514(e) of the Privacy Rule, certain health-related communications are subject to special conditions on marketing communications, if they also serve to promote the use or sale of a product or service. These marketing conditions require that particular disclosures be made as part of the marketing materials sent to individuals. Absent these disclosures, protected health information can only be used or disclosed in connection with

such marketing communications with the individual's authorization. The Department is aware that the Privacy Rule's §164.514(e) conditions for health-related communications create a potential burden on covered entities to make difficult assessments regarding many of their communications. The proposed modifications to the marketing provisions would relieve the burden on covered entities by making most marketing subject to an authorization requirement and eliminating the §164.514(e) conditions on marketing communications.

In developing the final impact analysis for the Privacy Rule, the Department was unable to estimate the cost of the marketing provisions. There was too little data and too much variation in current practice to estimate how the Privacy Rule might affect marketing. The same remains true today. However, the proposed modifications would relieve burden on the covered entities in making communications for treatment and certain health care operations relative to the requirements in the Privacy Rule. Although the Department cannot provide a quantifiable estimate, the effect of these proposed changes will be to lower costs relative to the Privacy Rule.

Research

In the final impact analysis for the Privacy Rule, the Department estimated the total cost of the provisions requiring documentation of an Institutional Review Board (IRB) or Privacy Board waiver of individual authorization for the use or disclosure of protected health information for a research purpose as \$40 million for the first year and \$585 million for the ten-year period. The costs were estimated based on the time that an IRB or

privacy board would need to consider a request for a waiver under the criteria provided in the Privacy Rule. See 65 FR 82770-82771 (December 28, 2000).

The proposed modification would simplify and reduce the number of criteria required for an IRB or Privacy Board to approve a waiver of authorization in three ways. First, the proposal would simplify the criteria for waivers to better conform to the Common Rule's waiver criteria for informed consent to participate in the research study. Second, the proposal would simplify the accounting procedures for research by eliminating the need to account for disclosures based on individual authorization. Third, the proposal would simplify the authorization process for research to facilitate the combining of the informed consent for participation in the research itself with all authorizations required under the Privacy Rule. Therefore, the Department estimates that the net effect of these modifications would be to reduce the time necessary to assemble the necessary waivers and for an IRB or Privacy Board to consider and act on waiver requests by one quarter. The Department estimates these simplifications would reduce the expected costs first year costs by \$10 million and the ten year costs by \$146 million, relative to the Privacy Rule. Since this initial estimate is based on limited information available to the Department, the Department requests information to better assess this cost savings.

| Privacy Rule Modifications - Ten-Year Cost Estimates | | | |
|---|----------------------|---------------------|-----------------------------------|
| Policy | Original Cost | Modification | Change due to Modification |
| Consent | \$103 million | Provision removed | -\$103 million ¹ |

| | | | |
|---|--|---|---|
| Notice | \$391 million | Good faith effort to obtain acknowledgment of receipt | +\$184 million |
| Marketing | Not scored due to lack of data | Fewer activities constitute marketing | Reduction in cost but magnitude cannot be estimated |
| Business Associates | \$103 million for contract modifications | Model language provided | -\$35 million |
| Research | \$585 million | Waiver requirements simplified | -\$146 million |
| Net Change | | | -\$100 million |
| <p>¹As noted above in the discussion on consent, while the estimated costs of the consent provisions were \$103 million, comments have suggested that the costs were likely to be much higher. If these comments are accurate, the cost savings associated with retracting the consent provisions would, therefore, also be significantly higher than \$103 million.</p> | | | |

C. Costs to the Federal Government

The proposed changes in this Rule will result in small savings to the federal government relative to the costs that would have occurred under the Privacy Rule. Although there will be some increase in costs for the new requirements for obtaining acknowledgment for receipt of the notice, these costs are partially offset by the savings in the elimination of the consent. As discussed above, to the extent comments are accurate that the costs for the consent provisions are much higher than estimated, the cost savings associated with the retraction of these provisions would, therefore, be significantly higher. The Department does not believe the federal government engages in significant marketing as defined in the Privacy Rule. The federal government will have business associates

under the Privacy Rule, and therefore, the model language proposed in this rulemaking will be of benefit to federal departments and agencies. The Department has not estimated the federal government's portion of the \$35 million savings it estimated for this change. Similarly, the federal government, which conducts and sponsors a significant amount of research that is subject to IRBs, will realize some savings as a result of the research modifications proposed in this rulemaking. The Department does not have sufficient information, however, to estimate the federal government's portion of the total \$146 million savings with respect to research modifications.

D. Costs to State and Local Government

The proposed changes also may affect the costs to state and local governments. However, these effects likely will be small. As with the federal government, state and local governments will have any costs of the additional notice requirement offset by the savings realized by the elimination of the consent requirement. As discussed above, to the extent comments are accurate that the costs for the consent provisions are much higher than estimated, the cost savings associated with the retraction of these provisions would, therefore, be significantly higher. State and local governments could realize savings from the model language for business associates and the changes in research, but the savings are likely to be small. The Department does not have sufficient information to estimate the state and local government's share of the net savings from the proposed changes.

E. Benefits

The benefits of these modifications would be lower costs, and enhanced implementation and compliance with the Privacy Rule without compromising the protection of individually identifiable health information or access to quality health care.

F. Alternatives

In July 2001, the Department clarified the Privacy Rule in guidance, where feasible, to resolve some of the issues raised by commenters. Issues that could not adequately be addressed through guidance because of the need for a regulatory change are addressed in this proposed Rule. The Department examined a number of alternatives to these proposed provisions. One alternative was to not make any changes to the Privacy Rule, but this option was rejected for the reasons explained throughout the preamble. The Department also considered various alternatives to specific provisions in the development of this proposed Rule. These alternatives are generally discussed above, where appropriate.

V. Preliminary Regulatory Flexibility Analysis

The Department also examined the impact of this proposed Rule as required by the Small Business Regulatory Enforcement and Fairness Act (SBREFA) (5 U.S.C. 601, *et seq.*). SBREFA requires agencies to determine whether a rule will have a significant economic impact on a substantial number of small entities.

The law does not define the thresholds to use in implementing the law and the Small Business Administration discourages establishing quantitative criteria. However,

the Department has long used two criteria--the number of entities affected and the impact on revenue and costs-- for assessing whether a regulatory flexibility analysis is necessary. Department guidelines state that an impact of three to five percent should be considered a significant economic impact. Based on these criteria, the Department has determined that a regulatory flexibility analysis is not required.

As described in the Regulatory Flexibility Analysis for the Privacy Rule, most covered entities are small businesses--approximately 465,000. See Table A, 65 FR 82780 (December 28, 2000). Lessening the burden for small entities, consistent with the intent of protecting privacy, was an important consideration in developing these modifications. However, as discussed in the Preliminary Regulatory Impact Analysis, above, the net affect of the proposed changes is an overall savings of approximately \$100 million over ten years. Even if all of this savings were to accrue to small entities (an over estimation), the impact per small entity would be de minimis.

VI. Collection of Information Requirements

Under the Paperwork Reduction Act (PRA) of 1995, the Department is required to provide 60-day notice in the Federal Register and solicit public comment before a collection of information requirement is submitted to the Office of Management and Budget (OMB) for review and approval. In order to fairly evaluate whether an information collection should be approved by OMB, section 3506(c)(2)(A) of the PRA requires that the Department solicit comment on the following issues:

- The need for the information collection and its usefulness in carrying out the

proper functions of the agency.

- The accuracy of the estimate of the information collection burden.
- The quality, utility, and clarity of the information to be collected.
- Recommendations to minimize the information collection burden on the affected

public, including automated collection techniques.

In accordance with these requirements, the Department is soliciting public comments on the model business associate contract language displayed in the Appendix to this proposed Rule. The Department provides these model business associate contract provisions in response to numerous requests for guidance. 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. Nor is the model language a complete contract. Rather, the model language is designed to be adapted to the business arrangement between the covered entity and the business associate and to be incorporated into a contract drafted by the parties.

Section 164.506—Consent for Treatment, Payment, and Health Care Operations

Under the Privacy Rule, a covered health care provider that has a direct treatment relationship with individuals must, except in certain circumstances, obtain an individual's consent to use or disclose protected health information to carry out treatment, payment, and health care operations. The modifications would eliminate this requirement. While the consent requirement is subject to the PRA, the Department believes that the burden

associated with the requirement is exempt from the PRA as stipulated under 5 CFR 1320.3(b)(2). Therefore, the modification does not affect the paperwork burden associated with the Privacy Rule.

Section 164.520—Notice of Privacy Practices for Protected Health Information

The modifications would impose a good faith effort on direct treatment providers to obtain an individual's acknowledgment of receipt of the notice of privacy practices for protected health information and to document such acknowledgment or, in the absence of such acknowledgment, the entity's good faith efforts to obtain it. In addition, a covered entity would have to retain the acknowledgment or documentation of the good faith effort as required by § 164.530(j). The Department is continuing to work on estimating the burden imposed by the Privacy Rule. The estimate for the acknowledgment of receipt of the notice will be reflected in the paperwork reduction package to be submitted to OMB as required by the PRA.

The Department has submitted a copy of this proposed Rule to OMB for its review of the information collection requirements described above. These requirements are not effective until they have been approved by OMB.

If you comment on any of these information collection and record keeping requirements, please mail copies directly to the following:

Center for Medicaid and Medicare Services

Information Technology Investment Management Group

Division of CMS Enterprise Standards

Room C2-26-17
7500 Security Boulevard
Baltimore, MD 21244-1850.
ATTN: John Burke, HIPAA Privacy

and

Office of Information and Regulatory Affairs,
Office of Management and Budget,
Room 10235, New Executive Office Building,
Washington, DC 20503,
ATTN: Allison Herron Eydt, CMS Desk Officer

VII. Unfunded Mandates

Section 202 of the Unfunded Mandates Reform Act of 1995 also requires that agencies assess anticipated costs and benefits before issuing any rule that may result in an expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of \$110 million in a single year. A final cost-benefit analysis was published in the Privacy Rule of December 28, 2000 (65 FR 82462, 82794). In developing the final Privacy Rule, the Department adopted the least burdensome alternatives, consistent with achieving the Rule's goals. The Department does not believe that the modifications in the proposed Rule would qualify as an unfunded mandate under the statute.

VIII. Environmental Impact

The Department has determined under 21 CFR 25.30(k) that this action is of a type that does not individually or cumulatively have a significant effect on the human environment. Therefore, neither an environmental assessment nor an environmental impact statement is required.

IX. Executive Order 13132: Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent Privacy Rule) that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has Federalism implications. The federalism implications of the Privacy Rule were assessed as required by Executive Order 13132 and published in the Privacy Rule of December 28, 2000 (65 FR 82462, 82797). The proposed change with the most direct effect on federalism principles concerns the clarifications regarding the rights of parents and minors under State law. The modifications would make clear the intent of the Department to defer to State law with respect to such rights. Therefore, the Department believes that the modifications in this proposed Rule would not significantly affect the rights, roles and responsibilities of States.

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 Provisions¹

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

¹Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these model provisions and are not intended to be included in the contractual provisions.

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 _____ Agreement/ sections _____ of the _____ 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 _____ Agreement/ sections ____ of the _____ 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.

List of Subjects

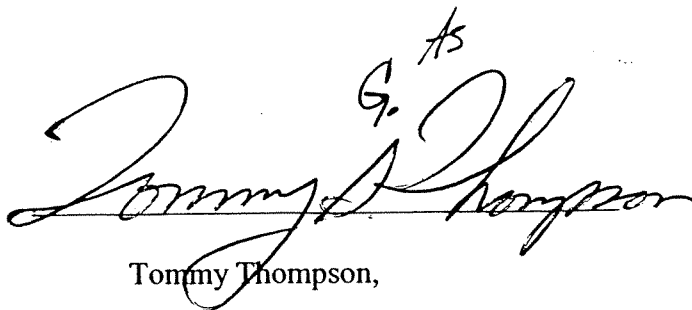
45 CFR Part 160

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: 3-12-02

^{G. AS}


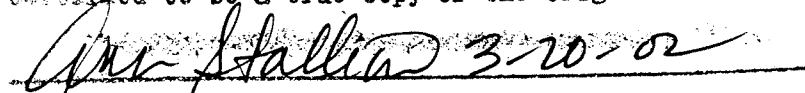
Tommy Thompson,

Secretary

For the reasons set forth in the preamble, the Department proposes to amend 45 CFR

Subtitle A, Subchapter C, as follows:

Certified to be a true copy of the Original Document


Ann Stallion 3-20-02