HEALTH PRIVACY PROJECT

INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY
GEORGETOWN UNIVERSITY

COMMENTS

ON PROPOSED MODIFICATIONS TO FEDERAL STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

APRIL 26, 2002

Staff Contacts:
Angela Choy, Field Director
Joanne Hustead, Senior Counsel
Joy Pritts, Senior Counsel

2233 Wisconsin Avenue, NW Suite 525 Washington, DC 20007
phone 202.687.0880 fax 202.784.1265
www.healthprivacy.org

Table of Contents for Health Privacy Project Comments

1. CONSENT FOR TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS
Sec. 164.506

Proposed Modification:
The Department proposes to eliminate the requirement that health care providers obtain an individual's consent prior to using or disclosing protected health information for treatment, payment, and health care operations.

Health Privacy Project Recommendation:
The Health Privacy Project strongly opposes this proposed modification. The Health Privacy Project recommends that the Department retain the Privacy Rule's prior consent requirement and make targeted modifications to address the unintended consequences that result from the consent requirement in some circumstances.

Rationale:
Consent vs. Notice

The Privacy Rule requires that health care providers obtain an individual's consent prior to using or disclosing protected health information for treatment, payment, and health care operations. At the core of the Department's proposed modifications to the Privacy Rule is the elimination of this prior consent requirement. In its place, the Department proposes to substitute a requirement that direct treatment providers make a "good faith effort" to obtain the individual's written acknowledgment that he or she received the provider's privacy notice. (Section 164.520 of the Privacy Rule requires covered entities to provide this notice of privacy practices.) This proposal to eliminate the consent requirement strikes at the very heart of the Privacy Rule and takes away a core privacy protection for consumers. The Privacy Rule's consent requirement is intended to bolster patient trust and confidence in providers and in health care organizations by respecting the patient's central role in making health care decisions. The Department's proposal to eliminate the consent requirement represents a huge step backwards for consumers – and one that will undermine trust in the health care system.

The Health Privacy Project strongly opposes this proposal and urges the Department to retain the consent requirement that is in the Privacy Rule, with targeted modifications to address the unintended consequences that result from the consent requirement in some circumstances.

Criticism of the consent requirement as a "paperwork burden" ignores the underlying values that a consent process seeks to address. Prior consent for the use or disclosure of protected health information seeks to achieve similar goals as those achieved through informed consent for treatment – a process that is now so embedded in our health care culture that few, if any, would criticize it in similar fashion. Obtaining a patient's informed consent prior to surgery or other treatment shows respect for the patient's autonomy, underscores the need to inform the patient fully of the risks and benefits of the proposed treatment, and makes it possible for the patient to make an informed decision. Similarly, obtaining a patient's consent prior to the use or disclosure of protected health information respects the patient's autonomy, underscores the need to inform the patient fully of the risks and benefits of sharing protected health information, and makes it

possible for the patient to make an informed decision about uses or disclosures the individual considers appropriate or finds objectionable.

With these important values at stake, it is clear that this debate is about much more than paperwork, or the label on the piece of paper that a patient signs (consent vs. notice), or even whether a patient is given two pieces of paper (a notice and a consent form) instead of just one (a notice). There are fundamental differences between a consent process and acknowledgment of receipt of a notice. As discussed above, seeking advance permission from a patient before using or disclosing health information acknowledges first and foremost that it is the patient who should decide whether to entrust others with his or her private medical information, under what circumstances, and for what purposes. Asking patients to merely acknowledge receipt of a notice simply takes patients out of the equation altogether.

The Privacy Rule's consent requirement gives individuals *some* control over how their health information is used and disclosed. Patients would certainly have *more* control if consent could be withheld without the provider opting to refuse to provide treatment, but criticism of the consent requirement as "forced" consent misses the mark. The Privacy Rule gives providers the option to refuse to provide treatment, but this is merely an option, not a requirement. It is by no means clear that providers will opt to withhold treatment even though permitted to do so, particularly when the patient consents to some uses or disclosures (treatment and payment uses/disclosures), but withholds consent for others (some of the relatively vast number of "health care operations" permitted by the Privacy Rule). It is clear that *without* a prior consent requirement, patients will have *no* control over how their health care information is used or disclosed beyond the right to *request* a restriction. Asking an individual to acknowledge receiving a privacy notice reinforces that the individual patient has absolutely no say in the matter.

The Privacy Rule's consent requirement is the best way to ensure that patients actually know how their health care information will be used or disclosed and know what their privacy rights are. The process of obtaining consent defines an "initial moment" – as the Department acknowledges – in which patients can raise questions about privacy concerns and learn more about options available to them. Patients are more likely to read the notice, or at least ask questions about how their information will be used or disclosed, when they are being asked to give their consent. Asking a patient to acknowledge receipt of a notice does not provide a comparable "initial moment" – especially when the individual is only asked to acknowledge receipt of a piece of paper, not whether they have read the paper or understood it or have questions about it.

From a practical perspective, the consent form required in the Privacy Rule focuses attention on a new right that is central to the consent process – the right to request a restriction. By all accounts, the consent form is much shorter than the notice of privacy practices. Thus, information that is repeated in the relatively short consent form will be highlighted for patients. The Privacy Rule requires the consent form to state that the individual has the right to request a restriction. *See* § 164.506(c)(4)(i). Including this information in the consent form, as well as in the notice, makes it even more likely that patients will be aware of this important right.

Targeted Modifications Urged

That the Department has chosen radical surgery – total elimination of the consent requirement – when much more targeted, privacy-protective interventions would suffice is especially troublesome. As discussed below, targeted modifications would solve legitimate concerns raised about the operation of the consent requirement.

Segments of the health care industry have been waging an intense campaign to eliminate the consent requirement ever since the final Privacy Rule was issued. To appear primarily, if not solely, motivated by concern for patients and their welfare, this campaign has argued that the consent requirement jeopardizes "timely access to care." As the Department notes in the preamble to the proposal, these concerns were "primarily raised by pharmacists and pharmacies," and they center around a pharmacist's inability to fill the prescription without the patient's written consent. *See* 67 Fed. Reg. 14779.

Pharmacy and First Encounter Issues. The Department could remedy these pharmacy-related problems quite easily, without eliminating the consent requirement for *all* providers. For example, the Department could clarify that pharmacists who receive prescriptions directly from doctors' office are indirect treatment providers and thus not subject to the prior consent requirement. (This could be done through small changes to the definition of "indirect treatment relationship.") Alternatively, the Department could create an exception to the prior consent requirement when obtaining such consent in advance is not practicable under the circumstances. (Such a modification also addresses implementation issues discussed below.) In circumstances where the patient himself or herself is not able to physically go to the pharmacy to pick up the prescription and sign the consent form, or prefers not to do so, consent could be handled through the mail. This second approach would also address the problems that arise when providers need to use a limited amount of protected health information prior to the patient's first encounter, for example, to set up an appointment or schedule surgery after a patient is referred by another provider.

Treatment Not Provided in Person. Similarly, the Department could address any perceived problems when providers do not ever provide treatment in person. *See* 67 Fed. Reg. 14779. Doctors who take phone calls for other doctors could be treated as part of an organized health care arrangement with a joint consent form. Nurses who staff telephone centers that provide advice over the phone usually do so under contract with a health plan, in which case they are functioning as business associates of the health plan, rather than as separate covered entities independently subject to the consent requirement.

Emergency Care. Emergency treatment providers raised concerns about whether the emergency exception encompassed all of the activities in which they engage. *See* 67 Fed. Reg. 14779-80. If any of these concerns are valid (and the Department does not state the precise concerns in the preamble), the Department could propose slight amendments to the emergency exception to address them. We note that the Department's proposed modification to the notice requirement continues to use the same phrase "emergency treatment situation" found in the proposed-to-be-deleted consent section.

Mandated Treatment. Some expressed concern about providers that are required by law to provide treatment having to ask for the patient's consent. *See* 67 Fed. Reg. 14780. This aspect of the consent requirement could be changed without excising the entire requirement.

Minors Who Reach Majority. Some expressed confusion about whether minors who reach the age of majority must sign a new consent form. *See* 67 Fed. Reg. 14780. Again, the Department could address this issue head on.

Tracking Revocation. Finally, some segments of the provider community expressed concerns about the technical difficulty of tracking consent forms and patient revocations. *See* 67 Fed. Reg. 14780. Concerns about revocation focus largely on the perceived need to eliminate all protected health information from data systems designed for health care operations such as quality assurance activities. It is not entirely clear that all protected health information would need to be excised under such circumstances. The Privacy Rule's approach to revocation is tempered; it permits revocation "except to the extent that the covered entity has taken action in reliance thereon." *See* § 164.506(b)(5). Guidance from the Department could certainly clarify, for example, the extent to which covered entities have relied on a patient's consent when they use or disclose data for health care operations activities such as quality assurance studies. We encourage the Department to provide guidance on how to implement a patient's revocation by providing examples to illustrate when a covered entity "has taken action in reliance thereon." To the extent that the concerns expressed in the preamble reflect a lack of existing technology to track revocations and excise protected health information, we are confident that industry will step up to the plate and devise such systems, especially if the Department provides useful guidance on the operational aspects of revocation.

What all of these examples share is their amenability to being solved through targeted modifications that leave the consent requirement intact. Instead of taking such a targeted approach to solve these problems, the Department proposes to eliminate the prior consent requirement for *all* providers, under *all* circumstances.

Weakening of Optional Consent

The Department not only proposes to eliminate the consent requirement, it also proposes to delete several provisions that apply when providers or plans *choose* to require consent. The Privacy Rule includes various provisions that govern the content of the consent form (*e.g.*, it must state that the individual has the right to review the privacy notice before signing the consent form) and the right to revoke. *See* § 164.506(b) and (c). Under the Privacy Rule, these provisions apply when consent is required *and* when it is optional. The Department proposes to delete all of these provisions in order to "enhance the flexibility of the consent process for those covered entities that choose to obtain consent." *See* 67 Fed. Reg. 14780. In addition, the Department proposes to delete provisions governing conflicting consents and authorizations; under the Privacy Rule, covered entities must follow the most restrictive. *See* § 164.506(e). The Department also proposes to delete the provisions that govern joint consents by organized health care arrangements. *See* § 164.506(f). By eliminating all of these provisions, the Department takes away important safeguards that should, at the very least, apply when consent is obtained voluntarily.

The proposal includes only one requirement when covered entities choose to obtain consent for treatment, payment, or health care operations purposes: "Consent of an individual under this paragraph shall not be effective to permit a use or disclosure of protected health information that is not otherwise permitted or required by this subpart." *See* proposed § 164.506(b)(2). The preamble states that a consent voluntarily obtained by a provider or plan could not permit a use or disclosure that, according to other parts of the Privacy Rule, requires an authorization, but this is not stated explicitly in the actual text of the proposed modification. *See* 67 Fed. Reg. 14781. This is an important protection. Otherwise a covered entity could substitute a consent form of its own design and choosing for an authorization that must meet certain specifications. To clarify this limit, the Privacy Rule should read: "Consent of an individual under this paragraph shall not be effective to permit a use or disclosure of protected health information *to carry out treatment, payment, or health care operations* that is not otherwise permitted or required by this subpart."

2. MARKETING
Secs. 164.501 and 164.508(a)(3)

Proposed Modifications:
The Department proposes to reduce the Privacy Rule's protections that apply to communications that many consumers consider to be "marketing." Under the Privacy Rule, a covered entity that is paid by a third party to encourage patients to purchase or use a product or service that is health related must adhere to certain conditions. In its first communication, the covered entity must give the patient an opportunity to refuse further marketing materials. The covered entity must inform the patient that it is receiving remuneration for making the communication. Additionally, the marketing materials must identify the covered entity as the party making the communication. The Department proposes to *eliminate* these requirements by removing from the definition of "marketing" all communications that encourage patients to purchase or use products or services that are health related, including communications that a covered entity is paid by a third party to make.

The Department does propose to retain the Privacy Rule's requirement that a covered entity obtain an individual's authorization prior to using or disclosing health information for "marketing." However, because the Department proposes to contract the definition of "marketing," the prior authorization requirement will apply only to a narrow range of communications – those that encourage the purchase or use of a product or service that is *not* health related. The prior authorization requirement will not apply to communications that encourage the use or purchase of a health related product or service because such communications are excluded from the definition of marketing, even if the covered entity is paid to make the communication. The net effect of these proposed changes is to substantially weaken the Privacy Rule.

***Health Privacy Project Recommendations*:**
The Health Privacy Project recommends that the Department:

- Revise the definition of "marketing" to include communications encouraging the purchase or use of a health related product or service where a covered entity receives direct or indirect remuneration from a third party for making the communication.
- Revise the Privacy Rule so that a covered entity must obtain an individual's authorization prior to using or disclosing protected health information for all marketing purposes, including communications encouraging the purchase or use of health related products or services where the covered entity receives direct or indirect remuneration for making the communication.
- Retain the requirement that the authorization notify the individual if the marketing is intended to result in remuneration to the covered entity from a third party.
- Further modify the provisions to require that an authorization for marketing specify whether the protected health information is to be used or disclosed for the marketing of health related services or products or for products and services not related to health.
- Retain the modification that allows oral communications to be "marketing."
- Modify the Privacy Rule to expressly prohibit the selling of lists of patients or enrollees to third parties or from disclosing protected health information to a third party for the

independent marketing activities of the third party, without the express authorization of the individual.

Rationale:
The Privacy Rule classifies communications that encourage patients to purchase or use products and services in three categories: 1) Communications that are clearly treatment oriented and for which the covered entity does not receive remuneration from a third party (such as a doctor recommending a particular medicine to a patient because it is medically indicated); 2) Communications that are related to health but are at least partially financially motivated (such as a pharmacy being paid by a drug company to send patients letters encouraging them to switch their medication to the drug company's brand); and 3) Communications that are clearly marketing because they do not relate to health (such as sending vacation advertisements). *See* § 164.501. Because the first category of communications is clearly treatment related, there is no requirement for prior authorization to use health information to make these communications. *See* § 164.501. At the opposite end of the continuum, when a covered entity is paid to use health information to market a product or service that is totally unrelated to health, the covered entity must obtain the patients' prior authorization before it can use their health information for these marketing purposes. *See* § 164.514(e)(1). The treatment of these two categories of health information remains substantially unchanged under the proposed modifications to the Privacy Rule.

In contrast, the proposed modifications significantly weaken the protections afforded for the second category of communications – those that encourage the use or purchase of a health related product or service and for which the covered entity receives remuneration. Because the Department initially recognized that covered entities face a financial conflict of interest when they are paid to recommend a certain health related product or service, the current Privacy Rule treats these communications as "marketing." The Privacy Rule permits health information to be used without the patient's prior authorization in these circumstances *only* if certain conditions are met. The patient must be given an opportunity to opt out of receiving further marketing materials. Additionally, the patient must be notified that the covered entity is the source of the communication and is being paid to make the recommendation. *See* § 164.514(e)(3).

Health care consumers have recommended that the Department strengthen these protections by requiring covered entities to obtain patient authorization *prior* to using their health information for this second category – communications consumers consider marketing. Rejecting this approach, the Department's proposed modifications do *not* require any prior authorization for this type of activity. Additionally, the Department proposes to *eliminate* the protections that currently exist (*i.e.*, the right to opt out of receiving further similar communications, the requirement that the individual be notified that the covered entity has a financial conflict of interest in making the recommendation, and the requirement that the covered entity be identified as the source of the communication).

The Department accomplishes this through a two-step process. First, it proposes to *remove* from the definition of "marketing" all communications that encourage the use or purchase of a health related product or service, even where the covered entity is paid by a third party to make such a communication. *See* proposed § 164.501. Thus, although the proposed modifications would

require a covered entity to obtain prior authorization for "marketing" (*see* proposed § 164.508(a)(3)), this prior authorization requirement would not apply to this category of communication because it is no longer defined as "marketing." Second, the proposed modifications eliminate all of the consumer protections for this type of communication that currently exist. *See* proposed modifications to § 164.514(e). Taken together, these proposed changes effectively allow covered entities to make this type of paid recommendation without *either* prior authorization *or* a chance to opt out. Additionally, the proposed modifications remove the requirements that covered entities notify consumers of the entity's financial interest in making the recommendation. These proposals significantly weaken the Privacy Rule.

We oppose these proposed changes on a number of grounds. First, we believe that the determination whether prior authorization for a communication is required should not rest on whether a communication is in some way related to health. The proposed exclusion of "health related" communications from the definition of "marketing" is extremely broad. It is hard to conceive of a communication that remotely relates to health that would be considered "marketing." Many activities that health care consumers would consider marketing and find objectionable would be excluded from the definition of marketing under this proposal.

For example, the proposed definition of marketing *excludes* "a communication made to an individual … to direct or recommend alternative treatments, therapies, health care providers, or settings of care." *See* § 164.501 (defining "marketing"). Under this exception, a pharmacy can be paid by a drug company to identify patients based on their health information and to send them material encouraging them to switch their prescriptions to the drug company's particular brand of medicine. This "recommend[ation of] alternative treatment" is primarily motivated by profit and has little to do with what is medically best for the patient. Many patients believe that this financially motivated use of their health information is a violation of their privacy.[1]

Second, because recommending any health related product or service is not considered to be "marketing," there is no requirement that the consumer be informed that the covered entity is receiving remuneration from a third party to make these recommendations. In the above example, patients could receive materials from their pharmacy suggesting that they change their medicine to a different brand without ever being informed that the pharmacy was paid to make the recommendation. This approach encourages providers to engage in practices that are ridden with financial conflicts of interest.[2] In order for patients to make informed decisions, they must be notified of financial conflicts of interest.

Third, and perhaps most importantly, the proposed modification eliminates any control that individuals may have over the use of their protected health information for making this type of recommendation. Because these communications are not "marketing" there is no requirement that the covered entity obtain prior authorization to use the information in this manner. Furthermore, there is no mechanism by which an individual can remove his or her name from the

[1] *See e.g.*, Robert O'Harrow, Jr., *Prescription Fear, Privacy Sales*, WASH. POST, February 15, 1998 at A1; Henry l. Davis, *More Eckerd Questions*, ST. PETERSBURG TIMES, March 5, 2002 at 1E.

[2] *See* Bernard Lo and Ann Alpers, *Uses and Abuses of Prescription Drug Information in Pharmacy Benefits Management Programs*, 283 JAMA 801, 809 (February 9, 2000).

covered entity's mailing list for these "recommendations." This approach does not respect health care consumers and leaves them powerless.

Expanding the definition of marketing can cure these faults. We believe that marketing should include communications about a product or service to encourage recipients of the communication to purchase or use the product or service where the covered entity receives direct or indirect remuneration for making the communication. We would apply this standard to both health related and non-health related communications. Using this definition presents a bright line test. If a covered entity receives payment for a communication, the communication is marketing.

In conjunction with this recommendation, we urge the Department to retain the proposed modification that would require covered entities to obtain an individual's authorization prior to using his or her health information for these marketing purposes. The Privacy Rule's delayed opt-out approach is insufficient to protect privacy. Health care consumers should have meaningful control over whether their health information is used for these profit-making purposes.

Appointment reminders and prescription refill notices

A number of concerns have been raised about communications, such as appointment reminders and prescription refill notices, which may potentially fall in the gray area of what should be considered to be marketing. We would expect that the vast majority of covered entities do not receive remuneration for sending their patients appointment reminders. Therefore, this type of communication would not be marketing. Likewise, where a pharmacy on its own volition sends a prescription refill notice or advises a patient of a potential adverse drug reaction and suggests an alternative it would not be marketing. However, where a pharmacy receives payment for encouraging patients to refill prescriptions or switch medicine brands, the communication would be marketing.

We recognize that at times this definition may encompass some communications that provide useful information to health care consumers. However, when a covered entity receives payment from a third party for making a communication, it is acting significantly in its self-interest, as opposed to the interest of the patient. In such a circumstance, the individual should be informed in advance that the covered entity receives remuneration for its communications and should have control over whether his or her health information is used in this manner.

Oral communications

In conjunction with the above changes, we urge the Department to retain the proposed modification that removes oral communications from the type of health care related communication that is excluded from the definition of marketing. Under the current Privacy Rule, oral communications related to health care are not considered to be marketing. This exclusion would allow covered entities to telephone individuals to recommend alternative treatments – essentially permitting telemarketing – *without* the individual's authorization. The proposed modifications to the marketing provisions delete this exclusion. We urge the Department to adopt this modification while expanding the definition of marketing to include

communications made pursuant to remuneration in order to ensure that this type of activity is only engaged in with individuals' permission.

Simplification language

In addition to these substantive proposals, the Department has also modified the language of the exclusions to "simplify the language," such as using the phrase "treatment of that individual" in lieu of "made by a health care provider to an individual as part of the treatment of the individual, and for the purpose of furthering the treatment of that individual" in the definition of marketing. *Compare* proposed modification and current version of section 164.501. We request the Department to clarify that these proposed changes do not expand the type of communications excluded from the definition of "marketing."

Assessment standard

The Department has also indicated that the assessment whether a communication is marketing should be made from the effect the communication has on the recipient—if the effect of the communication is to encourage recipients to purchase or use the product or service, the communication would be marketing. *See* 67 Fed. Reg. 14790. We do not believe that the proposed modifications to the text of the Privacy Rule clearly reflect this policy. Furthermore, we believe that a slightly more objective standard would be appropriate. Accordingly, we encourage the Department to modify the Privacy Rule to include an express, objective standard for assessing whether a communication is "marketing."

Sale of Patient or Enrollee Lists/Disclosing Protected Health Information to Third Parties

In the preamble to the proposed modifications, the Department makes the following statement:

> [T]he Privacy Rule prohibits a covered entity from selling lists of patients or enrollees to third parties, or from disclosing protected health information to a third party for the independent marketing activities of the third party, without the express authorization of the individual. *See* 67 Fed. Reg. 14789.

These are important limitations, but they are not expressly stated in the Privacy Rule itself or in the proposed changes to the regulatory text. Indeed, based on media commentary since the proposed modifications were issued, it is clear that there is much confusion on these exact points. We recommend that the Department include express language in the Privacy Rule itself to clarify these points.

3. HYBRID ENTITIES
Sec. 164.504

Proposed Modifications:
The Department proposes to modify the hybrid entity provisions in order to allow *any* covered entity that performs a mixture of covered and non-covered functions to have the option of being designated a hybrid entity or having the entire organization treated as a covered entity. Additionally, the Department would require that a covered entity that elects hybrid status include in its designated health care component(s) any component that would meet the definition of covered entity if it were a separate legal entity.

The modifications would permit, but not require, the hybrid entity to designate a component that performs: (1) covered functions; and (2) activities that would make such a component a business associate of a component that performs covered functions if the two components were separate legal entities.

Health Privacy Project Recommendations:

- Reject the proposal that any covered entity can elect to be a hybrid entity, and *require* those covered entities whose primary functions are not covered functions to be hybrid entities and to erect firewalls between their health care components and other components.
- Modify the implementation specifications of the proposed modified hybrid provisions to *require* that, at a minimum, a hybrid entity must designate a component that performs covered functions as a health care component.
- Clarify that a health care provider (including a component of a hybrid entity that provides health care) cannot avoid being deemed a "covered entity" if it relies on a third party to conduct its standard electronic transactions. Clarify that with respect to hybrid entities, a health care provider cannot avoid having its treatment component considered a health care component by relying on a billing department to conduct its standard electronic transactions.
- Reconsider the circumstances under which a covered entity whose primary function is health care can designate itself a hybrid entity.

Rationale:
Currently, the Privacy Rule deems a covered entity whose *primary* functions are *not* covered functions to be a "hybrid entity." For example, a manufacturing employer who self-administers a health plan or that operates an on-site clinic could be a hybrid entity. *See* 65 Fed. Reg. 82502 (preamble to final Privacy Rule). Under the Privacy Rule, the hybrid entity must designate components that are to be considered "health care components." In general, only the health care component is treated as being the covered entity and subject to the requirements of the Privacy Rule (although the hybrid entity remains ultimately responsible for any violations). A transfer of protected health care information from the health care component to a non-health care component of the entity would be considered to be a disclosure and subject to all of the restrictions on disclosure contained in the Privacy Rule. A hybrid entity must establish firewalls to ensure that protected health information does not flow improperly between the health care component and the other components of the entity.

We believe that the current proposal to allow *any* covered entity that has both covered and non-covered functions to have the option of being treated as a hybrid entity is misdirected. Its potential impact is both under and over inclusive of entities that properly should be considered hybrid entities. The modification is under inclusive because an organization that has only a small component that is related to health care may avoid creating firewalls between the health care component and the rest of the organization by electing *not* to be a hybrid entity. Yet it is also over inclusive because ambiguities may allow a covered entity that primarily (and even overwhelmingly) performs health care functions to circumvent the requirements of the Privacy Rule for a large part of its operations by designating itself as a hybrid entity. We will address these concerns below.

Optional vs. Mandatory Hybrid Entity Status

We believe that the proposed modification that would allow hybrid entities that have only minimal health care functions to elect to have the entire organization treated as a covered entity is inappropriate. In originally drafting the Privacy Rule's hybrid entity provisions, the Department voiced two concerns:

- That companies that only had a small component should not be overly burdened with the entire entity's having to be deemed a covered entity; and
- That in an organization whose primary functions are not health care related "the lack of corporate boundaries increases the risk that protected health information will be used in a manner that would not otherwise be permitted by these rules. Thus, we require that the covered entity erect firewalls to protect against the improper use or disclosure within or by the organization." *See* 65 Fed. Reg. 82502.

By imposing firewall protections, the Department clearly believed that the general safeguard requirements imposed on all covered entities were insufficient to protect health information in an environment where the primary function of the organization is not health care. This is the correct approach. Unlike a health care organization, a company that is only tangentially involved in health care does not necessarily approach health information with the ingrained perspective that health care information should be treated confidentially.

We believe that organizations whose primary functions are not health care should be deemed to be hybrid organizations and required to institute firewall protections between their health care and other components. Allowing these organizations to choose to be considered a single covered entity merely permits them to avoid these extra protections. For example, under the proposed modification, an insurance company primarily engaged in selling life insurance, but that also sells health insurance, could elect to be treated as a single covered entity and *not* erect firewalls between the health and life insurance components. This approach reduces the protections afforded under the current Privacy Rule which deems such a company a hybrid and requires the erection of firewalls.

Standards for Designating Health Care Components

The provisions governing which components are to be designated as health care components are ambiguous. We are concerned that some covered entities may take advantage of this ambiguity to largely circumvent the application of the Privacy Rule.

The proposed modifications provide as follows:

> The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation as required by § 164.530(j), provided that if the covered entity designates a health care component or components, it must include any component *that would meet the definition of covered entity if it were a separate legal entity*. Health care components *may* include a component that performs:
>
> (A) covered functions; and
>
> (B) activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.

Proposed § 164.504(c)(3)(iii) (emphasis added).

This provision is ambiguous. Because the provision uses the term "may" it can potentially be construed as allowing, but not requiring, a hybrid entity to include a component that performs covered functions as part of their health care component. In other words, it may permit a covered entity to designate only a component that performs business associate type functions as the "health care component." Even the Department recognizes that there is ambiguity as to what components must be included as the health care component if a covered entity elects hybrid entity status. *See* 67 Fed. Reg. 14803. This is a critical issue because *only* the health care component of a hybrid entity must adhere to the requirements of the Privacy Rule.

Specifically, the question was raised "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." *Id.* The Department attempted to clarify this ambiguity by proposing to modify the rule by requiring that a hybrid entity include in its health care components(s) *any component that would meet the definition of covered entity if it were a separate legal entity*. *See* proposed §164.504(c)(3)(iii), emphasis added.

Yet this clarifying requirement remains ambiguous and may be interpreted in a manner that fails to take into account the nuances of the definition of "covered entity." A provider is not a covered entity under the Privacy Rule unless it conducts standard electronic transactions. Therefore, if a component of a provider does not conduct standard electronic transactions, it appears that this component need not be designated as a health care component of the covered entity.

In fact, the example used by the Department supports this conclusion. *See* 67 Fed. Reg. 14803. In its example, the Department reasoned that a university that is a single legal entity with a hospital that bills electronically and a research center that does not would only have to include the

hospital facilities that bill electronically in the health care component since, if the hospital were a separate legal entity it would be a covered entity. *See* 67 Fed. Reg. 14803.

While this clarification may be adequate for the particular situation cited, it does not address many other possible arrangements of health care providers, such as a single covered health care facility. For example, it might be argued that a hospital could designate only its billing office which engages in electronic billing as the "health care component," and *exclude* its treatment component from the "health care component" designation because the treating component does not electronically bill and, therefore, would not meet the definition of a covered entity if it were a separate legal entity. This would allow the hospital to only adhere to the Privacy Rule in its billing department. The treatment component would not be covered by the Privacy Rule. This interpretation would stand the Privacy Rule on its head.

We believe that such an assertion would be erroneous since the Department has indicated in the past that a provider cannot avoid being a covered entity by having a third party file claims electronically on its behalf. *See* 65 Fed. Reg. 82568. Under this approach, a provider could not avoid the application of the Privacy Rule to its treatment component by designating only its billing function as the "health care component." However, this position is not expressly incorporated in the Privacy Rule.

We believe that the Privacy Rule should expressly clarify that a covered entity may not avoid being covered by having another party perform its electronic billing functions to avoid these potential types of ambiguities. Additionally, the language detailing the types of functions that need to be included in a designation of health care component(s) needs to be clarified.

Covered Entities Primarily Engaged in Health Care

Assuming that the above ambiguities can be suitably resolved, there are still problems with permitting covered entities that are primarily engaged in health care to elect hybrid entity status. We recognize that there may be some circumstances that warrant a covered entity whose primary function is health care being able to designate itself a hybrid entity. However, we are concerned that in many circumstances this approach may create a false sense of security and confusion among the public. For example, most health care consumers would assume that a hospital in its entirety is a covered entity. If the hospital were to designate itself a hybrid entity there may be some functions that would not be covered. A hospital, for instance, could operate a free nurse advice line as a community service and a marketing tool and not designate it a health care component since it does not bill electronically. The advice line would clearly be associated with the hospital and most people using such a line would assume their information was protected. Because the component receiving the information would not be designated a "health care component," however, it would not be covered by the Privacy Rule. We recommend that covered entities whose primary function is health care be permitted to elect hybrid entity status only where the separate components are readily identifiable to the outside public, such as having separate facilities and different names.

4. DISCLOSURES OF PROTECTED HEALTH INFORMATION RELATED TO FDA-REGULATED PRODUCTS OR ACTIVITIES Sec. 164.512(b)

Proposed Modifications:

The Department proposes to amend the public health provisions of the Privacy Rule to permit disclosures of protected health information to private entities as part of any data-gathering activity that can be termed "related to the quality, safety, or effectiveness of such FDA-regulated product or activity," without patient authorization or any other limitations. Under the proposed modifications, disclosures would no longer be limited to achieving four specific objectives. In addition, the private person or entity requesting or receiving protected health information from the covered entity need no longer be required or directed by the Food and Drug Administration (FDA) to report such information to the FDA or to track the product at issue.

HPP Recommendation:

The Health Privacy Project strongly opposes the Department's proposal and urges the Department to retain the existing approach in the Privacy Rule of limiting permissive disclosures to four precise activities. The final Privacy Rule provides a specific list of public health exceptions to the authorization requirement. The proposed modifications, however, would create a vague and general exception, under the rubric of "public health," that would open the door to the release of protected health information to pharmaceutical companies, device manufacturers, food suppliers, and a range of their contractors and subcontractors (and arguably even to tobacco companies as well). For instance, a drug company could – with neither authorization nor an ethics committee review – gather a list of names and diagnoses of patients taking an existing product to assess "patient satisfaction" under the amorphous "quality" exception. Having gathered these names and diagnoses, the company could then use the same list to market new products for the same diagnosis. Indeed, given the vagueness of the proposed modifications, a pharmaceutical company could simply gather protected health information to assess the "effectiveness" of its direct-to-consumer TV ads since the promotion of drugs is itself an "FDA-regulated activity." We do not see a genuine public health need that justifies such a significant loophole in the Privacy Rule.

Rationale:

Under section 164.512(b)(1)(iii) of the Privacy Rule, a covered entity may disclose protected health information to a private entity ("a person subject to the jurisdiction of the Food and Drug Administration") without individual authorization if the disclosure is for one of the four specific purposes described in this section (reporting adverse events, tracking FDA-regulated products, enabling product recalls, and conducting post-marketing surveillance). For activities related to an FDA-regulated product (other than product recalls), this section also requires that the disclosures be made *only* "to a person required or directed by the Food and Drug Administration" to conduct such activities or report such information to the FDA, or in the case of post-marketing surveillance, "to comply with requirements or at the direction of the Food and Drug Administration." In other words, the section specifically permits, without authorization, disclosures "for purposes that the FDA has, in effect, identified as national priorities by issuing regulations or express directions requiring such disclosure; or if such disclosure is necessary for a product recall." *See* 65 Fed. Reg. 82669 (preamble to final Privacy Rule).

We strongly oppose the Department's proposed "technical corrections" to section 164.512(b)(1)(iii). The proposed modifications are substantive and significant, not technical. They sweep far too broadly and create a wholesale exemption to the Privacy Rule that has not been justified by the comments received or issues raised. They would create a large loophole for data collection and use for inappropriate purposes under the guise of "public health." Pharmaceutical and medical device manufacturers as well as food processors would be given general license to collect protected health information that goes far beyond that even permitted to biomedical research institutions with human subjects protections review or to legally responsible public health officials. Such a transfer by proxy of authority over protected health information places the data desires of these industries over the privacy interests of millions of Americans.

The most troubling aspect of the proposed modifications is the creation of a vague and general standard for the release of protected health information to manufacturers of FDA-regulated products in place of a provision that permits disclosures for a finite list of activities. Under the proposed modifications, virtually any activity related to the manufacture, storage, distribution, or marketing of FDA-regulated products can be "related" to the quality, safety, or effectiveness of the product. The general term "activity" further expands the types of functions that may be permitted without individual authorization. The gathering of patient information to perform a mass survey on the product's flavoring, for example, is arguably "related" to the quality of pharmaceuticals, but such an activity would not be a widely supported basis for the nonconsensual release of protected health information. Likewise, the tracking of an FDA-regulated product (an activity explicitly permitted by section 164.512(b)(1)(iii)(B)) could be used to compile names, addresses, and Social Security numbers solely to conduct patient-satisfaction studies under the rubric of "quality" or "effectiveness," although few if any patients would be happy to know that their records were used for such a purpose.

The proposed modifications also open protected health information to a wide range of disclosures not generally thought of as being part of public health. The proposed modifications would permit disclosures related to any FDA-regulated product(s) or activities. Because of the history of the Food, Drug, and Cosmetic Act, and because of the careful scientific and regulatory balancing that is done in permitting the commercialization of products only for demonstrated purposes, FDA is often intimately involved in the promotion, marketing, and advertising of products under its jurisdiction. Thus, the proposed modifications would allow the use of protected health information to assess the "effectiveness" of promotion, marketing, and advertising. While both manufacturers and advertisers alike would, no doubt, be delighted to be privy to such information, its release is not and cannot be justified. For example, the FDA has been involved in the regulation and review of tobacco products, and may again in the future; but no one would argue for nonconsensual release of protected health information to tobacco manufacturers, although the terms of the proposed modifications would allow exactly that. In some manner, all food products are under the jurisdiction of the FDA as well. With the possible exception of the need for a recall due to food contamination, it is difficult to imagine a situation that would warrant the nonconsensual release of protected information to food manufacturers.

The Department is claiming that the proposed modifications are intended to address concerns about barriers to the flow of information for "public health" purposes, but some of the same

concerns were raised by private entities during the comment period on the proposed rule, and the Department explained then that the concerns did not justify a modification to broaden access to protected health information without individual authorization. In fact, the preamble to the final Privacy Rule states that the Department believes that:

> modifying the proposed rule to allow disclosure of protected health information to private entities as part of any data-gathering activity related to a drug, device, or biological product or its use, or for any activity that is consistent with, or that appears to promote objectives specified, in FDA regulation would represent an inappropriately broad exception to the general requirement to obtain authorization prior to disclosure. Such a change could allow, for example, drug companies to collect protected health information without authorization to use for the purpose of marketing pharmaceuticals. We do not agree that all activities taken to promote compliance with FDA regulations represent public health activities as that term is defined in this rule. *See* 65 Fed. Reg. 82669.

There may be private entities engaged in data collection activities that benefit individuals affected by a particular condition, and these activities may even contribute to public health, but there must be some nexus to a government authority or other underlying legal requirement beyond being "related to" an FDA-regulated product or activity. The nexus to a government authority is especially important because once the protected health information is transferred to a private entity, the information is no longer protected by the Privacy Rule. Thus, we oppose the proposed elimination of such a government nexus (deleting the phrases "to a person required or directed by the Food and Drug Administration…" and "to comply with requirements or at the direction of the Food and Drug Administration").

We strongly urge the Department *not* to adopt the proposal to expand the list of permitted disclosures of protected health information, without authorization, to any activity that might be related to the quality, safety, or effectiveness of an FDA-regulated product or activity. We believe that the four specific activities in the final Privacy Rule sufficiently encompass the "public health" activities carried out by private entities subject to the jurisdiction of the FDA. We acknowledge that with respect to adverse events reporting, there may be a need to address the practical implications of restricting permitted disclosures only "to the person required or directed to report such information to the Food and Drug Administration." However, the proposed modification would have broad adverse unintended consequences. We believe that this issue can be addressed in a more targeted fashion.

5. DE-IDENTIFICATION
Sec. 164.514

Proposed Modification:
The Department is not proposing any substantive modifications to the de-identification provisions of the Privacy Rule at this time, but is considering the creation of a limited data set that would not include "facially" identifiable health information. This data set would be available for research, public health, and health care operations purposes presumably without authorization. In addition, the Department is considering the requirement that covered entities obtain data use or similar agreements from recipients that limit the use and disclosure of the data set and prohibit the recipients from re-identifying or contacting individuals.

Health Privacy Project Recommendations:
The Health Privacy Project supports the Department's decision to maintain the de-identification provisions. Before proposing an approach for the use or disclosure of a limited data set, the Department must carefully consider what identifiers can safely be included and the adequacy of privacy protections for the data set. We have specific concerns about the ease with which identifiable information that does not include direct identifiers can be combined with other data to directly identify an individual, as well as concerns about the enforceability of data use agreements.

Rationale:
We commend the Department for not proposing changes to the de-identification provisions of the Privacy Rule, recognizing that advances in information technology offer both promise and peril to patients. We urge the Department to continue to maintain these provisions in the Privacy Rule as they currently exist.

We support the continuation of research initiatives that would improve the quality of and access to health care, and recognize that some researchers, for example, may need to maintain a few identifiers to conduct their research. However, the Department must be very careful that, in its attempt to create flexible standards so "de-identified" databases remain useful, it does not also authorize the free flow of identifiable data for a myriad of other purposes under the guise of research, public health, and health care operations.

If the Department decides to adopt an alternative approach to de-identification that would permit uses and disclosures of a limited data set, it is important, first of all, that the Department make it very clear that this new approach is not another method for de-identifying data. The limited data set should be considered identifiable information. Second, we urge the Department to carefully consider the types of identifiers that may safely be included in the limited data set since the use and disclosure of such data set may not require individual authorization.

Advances in information technology have made it easier for entities to link data elements from various sources, as the Department acknowledges in its preamble to the proposed modifications. *See* 67 Fed. Reg. 14798. The Department's release of the final rule on national standards for electronic transactions further facilitates data linkage, the creation of large databases, and the re-

identification of "de-identified" data, simply because it promotes the standardization of data transmitted for health care transactions.

Most data that move through health information systems end up in databases.[3] While many of the databases currently are not fully standardized nor organized optimally for research, they provide a great deal of information about individuals. Standardization creates the potential for data linkage within and between data sets, and thus within and between many different health care entities, such as hospitals, health plans, public health departments, pharmacists and others. Even if identifiable data were not required for a specific function or research project, the existence of large standardized databases – especially those that are public databases – raise significant concerns. The more data that can be linked from different sources, the more likely it is that individual people or particular groups of people can be identified. Data could be aggregated from several sources, without individual knowledge or consent and accessed by parties outside the health care treatment environment.

Latanya Sweeney, Assistant Professor of Public Policy and of Computer Science at Carnegie Mellon University, has demonstrated both in her writings and at a policy briefing on Medical and Genetic Privacy on July 14, 2000, that "nonidentifiable" data can be combined with publicly available data to easily identify people.[4] For example, most cities sell locally collected census data or voter registration lists, which include the date of birth, name and address of their residents. These data may be linked to medical data, containing dates of birth and zip codes, to re-identify individuals, particularly in smaller communities.[5] One does not have to surf long on the Internet to find these publicly available databases. On anybirthday.com (www.anybirthday.com), for example, one can search for a person's birth date and address by entering a last name and zip code. For a small fee, the site will search for all individuals in its database with a specific birth date or provide a person's recent addresses.

The Department's distinction between facially and not facially identifiable information rests on a false premise, given the ease with which identifiable information that does not include direct identifiers can be combined with other data to directly identify an individual. Birth date and/or zip code, as explained above, are sufficient to identify an individual when linked to another database with overlapping data elements; therefore, we would oppose the expansion of the limited data set to include birth date. We recommend that the Department also consider excluding the full zip code and using only the first three digits of the zip code, especially when the full zip code along with the other data elements of the limited data set could reveal information about a specific individual (such as in a rural community) or a specific population (such as in a predominantly minority community).

We anticipate that supporters of a limited data set that includes zip code and/or birth date would comment that privacy will be adequately protected because only entities that enter into a data use

[3] William W. Lowrance, *Privacy and Secondary Use of Data in Health Research*, Proceedings of the Inaugural Robert H. Levi Leadership Symposium 13, 14 (April 2000).
[4] Alliance for Health Reform and The Forum on Technology & Innovation, *Policy Briefing: Medical & Genetic Privacy* (Washington, DC July 14, 2000); *See also*, Latanya Sweeney, *Controlling Inference and Protecting Privacy by Constructing an Anonymous Data System*, Carnegie Mellon University, unpublished paper, November 1998.
[5] Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*, 25 J.L. MED. & ETHICS 98, 100 (1997).

agreement with a covered entity would be permitted access to the data set. First of all, we are concerned that the Department is not suggesting that data use agreements limit the use of the data for the purpose for which the data was received. Second, if the Department makes the limited data set available for research purposes without authorization or waiver of authorization by an IRB or privacy board, the Department creates a loophole for the collection and use of identifiable health information by privately funded researchers. This would be inconsistent with the way the Privacy Rule currently treats the disclosure of protected health information for research. Under the Privacy Rule, research protocols involving the use and disclosure of protected health information, regardless of funding, require an authorization or a waiver of authorization before covered entities may disclose protected health information to researchers. However, while federally funded research would continue to undergo IRB review for research protocols involving identifiable information, including a limited data set, privately funded research would be permitted to circumvent the review process.

Finally, we are also extremely concerned about the enforceability of data use or similar agreements. According to Professor Sweeney, even if the original data holder imposes privacy and confidentiality requirements on a third party requesting access to the data, once the data are disclosed to the third party, the third party is in a position to redisclose the data to others without restrictions.[6] While the Department is suggesting that access to a limited data set would be conditioned on covered entities obtaining a data use or similar agreement from recipients, what happens when a recipient violates the agreement? Who is held accountable? Will the agreement function like a business associate contract so that if the covered entity is aware of a violation yet does nothing to remedy it, the covered entity will be held liable? These are questions we believe the Department must consider before making a decision to adopt an approach for the use or disclosure of a limited data set. We look forward to providing comments to the Department if and when the Department releases a specific proposal for the use and disclosure of a limited data set.

[6] Alliance for Health Reform and The Forum on Technology & Innovation, *Policy Briefing: Medical & Genetic Privacy* (Washington, DC July 14, 2000).

6. RESEARCH
Secs. 164.512(i), 164.508(f), 164.508(c)(1), 164.532

Proposed Modifications:
The Department proposes to:

(1) modify the waiver of authorization provisions.
(2) clarify that the Privacy Rule's provisions for IRBs and privacy boards would encompass a partial waiver of authorization for purposes of recruiting research participants.
(3) maintain an individual's right to revoke an authorization.
(4) permit research authorizations to be combined with other legal permission to participate in a research study.
(5) permit an authorization to use or disclose protected health information for the creation and maintenance of a research database without an expiration date or event, but limit it to the purpose of creating or maintaining that database.
(6) permit the use of individually identifiable health information after the compliance date for research protocols that received a waiver of authorization from an IRB prior to the compliance date.

Health Privacy Project Recommendations:
The Health Privacy Project:

(1) is pleased that research protocols will still be required to meet waiver criteria that are more narrowly focused on the privacy interests of the research participants.
(2) is pleased that the Department is ***not*** proposing modifications that would allow researchers to remove protected health information from a covered entity's premises for recruitment purposes prior to the approval of their research protocols.
(3) commends the Department for retaining an individual's right to revoke a research authorization, and recommends further guidance on how to implement the revocation requirement.
(4) urges the Department not to permit research authorizations to be combined with an informed consent to participate in a study.
(5) strongly agrees with the Department that the expiration date exception for the creation and maintenance of databases should not be extended to authorizations for further research or any other purpose.
(6) recommends that a research study that receives a waiver of authorization from an IRB prior to the compliance date, but begins after the compliance date, be re-evaluated to ensure that adequate privacy protections are in place.

Rationale:
We strongly support the continuation of initiatives that would improve access to and the quality of health care. In fact, the Health Privacy Project believes that protecting privacy and confidentiality and promoting research are values that go hand-in-hand. Rather than prevent the flow of health information for research purposes, the Privacy Rule will build public trust in research and help ensure that researchers receive complete and accurate health information for their studies. If people withdraw from full participation in their own care because of fear that their personal health information will be used against them, the health data from medical files

and patient databases that researchers may rely on to recruit subjects and/or conduct records-based studies will be inaccurate and incomplete.

Waiver Criteria
Sec. 164.512(i)(2)

We commend the Department for retaining most of the research provisions in the Privacy Rule so that all research regardless of funding that involves protected health information must satisfy the waiver criteria before such information can be used or disclosed without patient authorization. This is a significant step in helping to close the gap in standards adhered to by federally and privately funded research.

In addition, we are pleased that research protocols will still be required to meet waiver criteria that are more narrowly focused on the privacy interests of the research participants. As cited in the Department's preamble to the proposed modifications, there are only two references to privacy and confidentiality in human subjects protection regulations. The Common Rule and the FDA's regulations require an informed consent form to include "a statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained" (Common Rule § .116(a)(5), 21 CFR § 50.25(a)(5)); and to approve a study an IRB must determine that "when appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data." (Common Rule § .111(a)(7), 21 CFR § 56.111(a)(7)) Requiring IRBs and privacy boards to evaluate whether protocols meet the privacy-specific waiver criteria in the Privacy Rule will better ensure that adequate safeguards are in place to respect individuals' privacy and protect the confidentiality of the data when protected health information about individuals is used for research without their authorization.

Recruitment
Secs. 164.512(i)(1)(ii) and 164.512(i)(2)

We are pleased that the Department is ***not*** proposing to allow the release of protected health information for recruitment purposes without first obtaining an authorization or an IRB or privacy board waiver of authorization. Section 164. 512(i)(1)(ii) currently allows researchers to review protected health information necessary to prepare research protocols, but does not permit researchers to remove the information from the covered entity's premises. The purpose of this section is to give researchers access to protected health information to develop a research protocol, and to determine whether a covered entity has protected health information about patients who might meet the eligibility criteria for enrollment in a research study. At this stage, a research project has yet to be designed.

Some commenters at an August 2001 National Committee on Vital and Health Statistics (NCVHS) hearing claimed that it would be burdensome to go back to a covered entity to review the records to identify potential participants after already reviewing the records to prepare a research protocol. During the initial review of the records, however, researchers may identify possible recruits to participate in a research protocol. What the Privacy Rule prohibits is the removal of protected health information from the covered entity's premises and the contacting of potential recruits without first going through an IRB or privacy board. This is an important

provision because it protects against the release of protected health information to a researcher whose research protocol may subsequently be rejected by an IRB or privacy board.

We believe that the privacy interests of the patients significantly outweigh the inconvenience of returning to a covered entity for a list of potential recruits and that weakening the Privacy Rule to create an exception for recruitment purposes would be absolutely unwarranted. Hence, we support the Department's clarification that the Privacy Rule's provisions for IRBs and privacy boards would "encompass a partial waiver of authorization for purposes of allowing a researcher to obtain protected health information necessary to recruit potential research participants." *See* 67 Fed. Reg. 14794. The Department's clarification would ensure that, at a minimum, an IRB or privacy board has considered the researcher's proposal for recruitment of research participants before covered entities may release protected health information without authorization.

Research Authorization
Sec. 164.508(f)

Revocation. We applaud the Department for retaining an individual's right to revoke his or her authorization for disclosure of his or her information for research purposes. We strongly agree with the Department's argument that "if covered entities were permitted to continue using or disclosing protected health information for the research project even after an individual had revoked his or her authorization, this would undermine the primary objective of the authorization requirements to be a voluntary, informed choice of the individual." *See* 67 Fed. Reg. 14794. If an individual determines that an authorized use or disclosure is no longer in his or her best interest, he or she should be able to withdraw the authorization and prevent any further uses or disclosures.

We are also pleased that the Department is making an effort to clarify the Privacy Rule's approach to revocation. The Privacy Rule permits revocation "except to the extent that the covered entity has taken action in reliance thereon." *See* § 164.506(b)(5). Some commenters are concerned, however, about how to implement a revocation of an authorization for the use or disclosure of protected health information for research. In response to these concerns, the Department states in the preamble that it "believes that limiting uses and disclosures following revocation of an authorization to those necessary to preserve the integrity of the research appropriately balances the individual's right of choice and the researcher's reliance on the authorization." *See* 67 Fed. Reg. 14794. While we applaud the Department for this attempt to explain the revocation requirement, we believe further guidance is necessary. We also encourage the Department to provide examples to illustrate when a covered entity "has taken action in reliance thereon."

Separate Authorizations. The Department is proposing to permit authorizations for the use or disclosure of protected health information for a specific research study to be combined with any other legal permission related to that study, including a consent to participate in the study. *See* 67 Fed. Reg. 14796; proposed § 164.508(b)(3). We understand the desire to simplify the authorization process not only for researchers but also for the individuals who will be signing these forms, however, this proposed modification is problematic. Submitting a request for disclosure of protected health information pursuant to an authorization that is combined with the

consent to participate in a study, for example, might reveal information about the individual that the individual may want to keep confidential, such as possible treatments or an agreement to take a genetic test. A consent to participate in a study may also reveal more information than a covered entity needs to know. Therefore, we urge the Department not to permit research authorizations to be combined with an informed consent to participate in a study.

Expiration Date
Sec. 164.508(c)(1)

We are pleased that the Department's proposal specifically limits authorizations for the use or disclosure of protected health information to create and maintain a research database without an expiration date or event to the purpose of creating or maintaining that database. *See* 67 Fed. Reg. 14796. We strongly agree that this exception should not extend to authorizations for further research or any other purpose. Authorizations for the use or disclosure of data maintained in the database should explicitly provide an expiration date or event.

Transition Provisions
Sec. 164.532

We recognize that the Department had to make a decision about where best to draw the line for compliance with the Privacy Rule and where to draw that line is not always obvious. However, we urge the Department to reconsider its proposal to permit the use of individually identifiable health information after the compliance date for all research protocols that received a waiver of authorization from an IRB prior to the compliance date. For studies that have not begun, entities should be required to re-evaluate their research protocols to ensure that there are adequate privacy protections in place as specified in the Privacy Rule.

Along with several other waiver criteria, the Privacy Rule requires IRBs and privacy boards to examine protocols to determine whether there are adequate written assurances that protected health information will not be reused or disclosed to any other person or entity before granting a waiver of authorization. This criterion is an important element of protecting individually identifiable health information in research because it extends privacy protections beyond the initial point of data collection and provides some assurance that protected health information used or obtained without authorization will not be misused by researchers.

Investigators of a study that does not begin until after the compliance date should be bound by the same redisclosure restrictions and other privacy protections that researchers who obtain a waiver of authorization after the compliance date must observe. We believe that the privacy interests of the subjects of the information outweigh the potential burden of re-evaluating protocols to ensure that they satisfy the Privacy Rule's waiver criteria.

While we also believe that a covered entity should obtain a new authorization for a research study if the authorization was obtained before the compliance date and before the study has begun, we do recognize that it may not be practicable to do so. Moreover, since an authorization was obtained from the research participant, the individual at least is aware that his or her information is being used or disclosed for the purpose of the research project.

7. INDIVIDUAL AUTHORIZATION
Sec. 164.508

Proposed Modification:
The Department proposes to:

(1) streamline the authorization process by consolidating the different authorizations in the Privacy Rule under a single set of criteria and removing some core elements from the authorization requirement.
(2) tighten provisions on the use and disclosure of psychotherapy notes so that psychotherapy notes cannot be used or disclosed without individual authorization for another entity's treatment, payment, and health care operations purposes.
(3) add clarifying language so that an individual who initiates an authorization would not be required to reveal the purpose of his or her request.
(4) maintain the individual's right to revoke an authorization.

Health Privacy Project Recommendation:
The Health Privacy Project applauds the Department's proposal under numbers (2), (3) and (4) above. However, while we support the Department's effort to simplify the authorization provisions, we strongly urge the Department to: (a) retain the core elements required for research authorizations involving treatment of an individual; (b) require remuneration disclosures in all authorizations, not only in authorizations for marketing; and (c) retain the plain language requirement as a core element of a valid authorization. It is critical that individuals know how their information will and will not be used or disclosed so that they can make an informed decision about giving authorization. Furthermore, any request for individual authorization to use or disclose information must be communicated in a manner that can be understood by the average reader so that people know what they are authorizing.

***Rationale*:**
We commend the Department for tightening the provisions on the use and disclosure of psychotherapy notes without authorization to carry out treatment, payment, and health care operations. *See* proposed § 164.508(a)(2)(i)(A), (B), and (C). We strongly support the Department's proposal to clarify that psychotherapy notes may not be used or disclosed without individual authorization for another entity's treatment, payment, and health care operations purposes. *See* 67 Fed. Reg. 14798. We also welcome the proposal to add language clarifying that an individual who initiates an authorization would not be required to reveal the purpose of the request. Finally, we commend the Department for maintaining an individual's right to revoke an authorization for disclosure of protected health information. The right to revoke is essential to ensuring that an individual's authorization is truly voluntary.

However, we are extremely concerned that in an effort to streamline the authorization process the Department is proposing to remove some critical elements from the authorization requirement. As the Department states in the preamble, the core elements of the authorization are intended to provide individuals with information they need to make an informed decision about giving authorization. *See* 67 Fed. Reg. 14797.

The Privacy Rule currently requires an authorization to include information on what information will be used or disclosed, by whom, to whom, the purpose of the use or disclosure, an expiration date or event, and the individual's signature and date. There are additional elements, such as information about revocation and notice of the potential for redisclosure, that also must be included in the authorization. These important elements will remain in the Privacy Rule under the Department's proposal. However, under the final Privacy Rule, there are also other requirements specifically for three types of authorizations – authorizations requested by a covered entity for its own uses and disclosures (§164.508(d)); authorizations requested by a covered entity for disclosures by others (§164.508(e)); and authorizations for research that includes treatment of the individual (§ 164.508(f)). The Department proposes to consolidate these authorizations under one set of criteria.

While we support the Department's effort to simplify the authorization provisions, we urge the Department to: (1) retain the additional elements required for authorizations for research involving treatment as specified under section 164.508(f)(1)(ii); (2) require all authorizations to include any remuneration that a covered entity may receive from obtaining an individual's authorization; and (3) retain the plain language requirement as a core element of a valid authorization.

Research Authorizations. Section 164.508(f)(1)(ii) requires authorizations for research involving treatment to include a description of the extent to which protected health information created for research would be used to carry out treatment, payment, or health care operations. It also requires a description of any protected health information that will not be used or disclosed for purposes permitted in sections 164.510 and 164.512. (Section 164.510 governs uses and disclosures that require an opportunity for the individual to agree or object. Section 164.512 covers the uses and disclosures that do not require consent, authorization or an opportunity for the individual to agree or object (*e.g.*, disclosures to public health authorities).)

It is critical that individuals know how their research related information will and will not be used or disclosed so that they can make an informed decision about giving authorization. For example, an individual's insurer may cover some of the treatment services provided in the course of the research study, but the individual may not want the insurer to know about his or her participation in the study or about the treatment(s) to be received. Unless it is clearly stated in the authorization form what information will be used or disclosed for payment purposes, this potential research participant cannot make an informed decision about participating in the study and authorizing disclosure of his or her information. The risk here is that people may be afraid to participate in research studies for fear that their information will be used against them to deny them and/or their family members health insurance coverage.

Remuneration. We urge the Department to require that all authorizations include any remuneration that a covered entity may receive from obtaining an individual's authorization. The Department's proposal to limit the remuneration disclosure only to authorizations for marketing purposes ignores the growing problem of financial conflict of interest. Conflicts of interest do not exist only in the marketing context. Research, for example, is another area where it is imperative that individuals are informed of a provider/researcher's monetary interests in obtaining the individual's authorization. The disclosure of financial gain is critical to informing

individuals about how and why protected health information about them will be used or disclosed. For example, it should be made clear to an individual when a provider is being paid for each patient recruited to a study to be conducted by a drug company.

Plain Language. The Privacy Rule requires that an authorization be written in plain language as a core element of a valid authorization. The Department drew on established laws and guidelines, including the July 1977 Report of the Privacy Protection Study Commission, to develop the list of required elements in a "valid" authorization currently specified in the Privacy Rule. The Department's proposal, however, would remove the plain language requirement from this list of core elements. The plain language requirement is critical to ensuring that an individual's authorization is informed and voluntary. Any request for individual authorization to use or disclose information must be communicated in a manner that can be understood by the average reader so that people know what they are authorizing. Therefore, we urge the Department to retain the plain language requirement as a core element of a valid authorization by adding a reference to section 164.508(c)(3) under section 164.508(b)(1)(i). The provision should read as follows: "A valid authorization is a document that meets the requirements in paragraphs (c)(1), (2) and (3) of this section."

8. ACCOUNTING OF DISCLOSURES
Sec. 164.528

Proposed Modification:
The Department proposes to expand the list of exceptions to the accounting of disclosures requirement so that it no longer requires covered entities to account for any disclosures made pursuant to an individual authorization.

Health Privacy Project Recommendation:
The Health Privacy Project opposes the Department's proposal and urges the Department to retain the requirement that disclosures of protected health information made pursuant to an authorization be included in an accounting of disclosures. Removing authorized disclosures from the accounting takes away the individual's means of verifying that his or her information was disclosed as specified in the authorization. Such a modification would also hinder an individual's ability to detect authorizations that have been fraudulently submitted or altered.

Rationale:
We commend the Department for maintaining an individual's right to obtain an accounting of disclosures of protected health information. However, we oppose the Department's proposal to expand the number of exceptions to the accounting of disclosures requirement under section 164.528(a)(1) by removing disclosures made pursuant to an authorization from the list of information to be provided in an accounting. We believe that the Department should make changes to strengthen this provision by providing a full audit trail where one exists. Instead, the Department is proposing to weaken this right in response to claims of administrative burden by some in the health care industry.

An accounting of disclosures is useful in detecting alleged violations of confidentiality. It documents for individuals to whom certain information has been released, even information that the individual authorized for disclosure. It also allows individuals to monitor how covered entities are complying with the Privacy Rule. Covered entities that deliberately make disclosures in violation of the rule might not note such a violation, but the accounting may document inappropriate disclosures, enabling individuals to raise their concerns about these disclosures with the covered entity. Removing authorized disclosures from the accounting takes away the individual's means of verifying that his or her information was disclosed as specified in the authorization. As the Department stated in its preamble to the final Privacy Rule in response to comments about the accounting provisions, "We do not agree that individuals should be required to track these disclosures themselves. In many cases, an authorization may authorize a disclosure by more than one entity, or by a class of entities, such as all physicians who have provided medical treatment to the individual. Absent the accounting, the individual cannot know whether a particular covered entity has acted on the authorization." *See* 65 Fed. Reg. 82743.

A case currently being investigated by the Florida Attorney General's office provides a good example of the danger of excluding "authorized" disclosures from the accounting. When customers of Eckerd Drug Company pick up their prescriptions, they sign a log to indicate that they do not want the counseling of the pharmacist. According to press accounts, Eckerd then takes this signature, which is written on a gum-backed sticker, and puts it on a form authorizing

the chain drug store to use the customer's prescription record for promotions and discounts financed by drug companies.[7] If the Department adopts its proposed modification to the Privacy Rule, a company that engaged in such conduct would not have to include such a disclosure in a requested accounting – even though the disclosure was made pursuant to an erroneous, perhaps fraudulent, authorization.

[7] Mark Albright, *More Eckerd Questions*, ST. PETERSBURG TIMES, March 5, 2002, 1E.

9. BALANCING THE RIGHTS OF MINORS AND PARENTS Sec. 164.502(g)(3)

***Proposed Modification**:*
The Department proposes to modify the Privacy Rule's approach to balancing the rights of minors and parents by permitting covered entities to decide when to disclose protected health information about a minor to a parent in cases where State or other applicable law is silent or unclear.

***Health Privacy Project Recommendation**:*
The Health Privacy Project opposes the proposed modifications because they would deter minors from obtaining critical health services, such as mental health care, substance abuse treatment, and testing and treatment for sexually transmitted diseases. We recommend that the Department retain the approach in the current Privacy Rule, except its approach to non-preemption of State laws that are less protective of a minor's privacy. Specifically, we recommend that the Department apply the same preemption rules to State laws pertaining to minors and disclosures to parents that the Department applies to other State laws, as HIPAA requires.

***Rationale**:*
As currently written, the Privacy Rule strikes a careful balance between the need for parents to have access to their children's health information and the need for adolescents to feel secure that their health information will be kept private in certain limited circumstances. Thus, under the Privacy Rule, parents are generally treated as the personal representatives of their unemancipated minor children and given control over and access to their children's health information. Based upon significant research and standard medical practice, however, the Privacy Rule contains narrow exceptions to this general rule.

One of these exceptions gives a minor control over and access to information related to health services that the minor lawfully obtains based on his or her own consent. *See* § 164.502(g)(3)(i). Numerous studies have found that confidentiality is one of the prime determinants of whether an adolescent seeks and obtains timely health care related to sensitive topics such as mental health, substance abuse, and sexuality. For example, studies show that somewhere between eight and thirty-one percent of teens delay or entirely forego health care because of concerns that their private information will be revealed to parents or others.[8] In addition, research confirms that teens who believe that their health care provider will maintain their confidentiality are more likely to discuss sensitive health topics, such as sexually transmitted diseases, pregnancy prevention, and substance abuse, with their provider. In recognition of these facts and in pursuit of the lifesaving goal of ensuring that minors get the health care they need, the overwhelming majority of States have enacted laws that allow minors to consent on their own to specific

[8] *See, e.g.*, Jeannie S. Thrall et al., *Confidentiality and Adolescents' Use of Providers for Health Information and Pelvic Examinations*, 154 ARCH. PEDIATR. & ADOLESC. MED. 885 (2000); Carol A. Ford et al., *Foregone Health Care Among Adolescents*, 282 JAMA 2227 (1999); T.L. Cheng et al., *Confidentiality in Health Care: A Survey of Knowledge, Perceptions, and Attitudes Among High School Students*, 269 JAMA 1404 (1993); Laurie S. Zabin et al., *Reasons for Delay in Contraceptive Clinic Utilization: Adolescent Clinic and Nonclinic Populations Compared*, 12 J. ADOLESC. MED. 225 (1991).

services such as prenatal care, family planning services, testing and treatment for sexually transmitted diseases, mental health counseling, and treatment for alcohol and/or drug abuse.

Because laws allowing minors to self-consent to certain services were enacted precisely to ensure that confidentiality concerns did not keep adolescents from obtaining critical care, the Privacy Rule wisely linked the right to consent to a service to the right to control the information related to that service. Thus, under the existing Privacy Rule, in those limited circumstances where a minor lawfully obtains a service without a parent's consent, the minor (and not the parent) exercises the rights of control over and access to the information related to that service.

The proposed modifications to the Privacy Rule would sever the fundamental link between the minor's right to consent to a health service and the minor's need for confidentiality. Under the proposed modifications, a minor who lawfully obtains a service based on his or her own consent would no longer have a right to deny his or her parent access to the information related to that service. Rather, the proposed modifications would give the covered entity discretion to decide, within the bounds of State and other applicable law, whether or not to provide the minor's parent access to the information. *See* proposed § 164.502(g)(3)(iii).[9]

By failing to guarantee minors' confidentiality, the proposed modifications undermine the goal of the minors' consent laws – to encourage minors to get critical health care they would otherwise forego because of confidentiality concerns. Because the proposed modifications would deter adolescents from seeking essential health care, we urge the Department to retain the current version of section 164.502(g)(3).

What we believe was an oversight in the language of the proposed modifications to section 164.502(g)(3)(iii) makes this broad discretion over minors' health information even more problematic. Although the preamble speaks in terms of a "provider" exercising this discretion (*see* 67 Fed. Reg. 14792), the text of the proposed modifications does not limit the individuals who may exercise this discretion to the minor's treating provider. Rather, it confers upon *all* covered entities the discretion to decide whether to give a parent access to a minor's health information (so long as the decision is consistent with State and other applicable law). Thus, not only would physicians, nurses, and counselors who know the minor (and in some instances the parent) be vested with such discretion, but so would a wide range of others, including employees of health insurance plans and hospital records rooms who have never met the minor. We believe this to be an unintended consequence of the proposed modifications. We urge the Department to narrow the scope of individuals who are given such discretion to licensed health care professionals who have provided the health care service to the minor. To accomplish this goal, we recommend replacing "covered entity" in proposed section 164.502(g)(3)(iii) with the phrase "covered health care provider who is a licensed, treating health care professional."

The proposed modifications also restate and reinforce the Privacy Rule's inappropriate deference to State law in determining who shall have access to protected health information about minors.

[9] Because another section of the proposed modifications (§ 164.502(g)(3)(ii)) deals with State and other applicable law that explicitly requires, permits, or forbids disclosure of a minor's protected health information to a parent, section 164.502(g)(3)(iii) pertains only to a covered entity's decision whether to allow a parent access to such information when State or other applicable law is silent or ambiguous.

Under the proposed modifications, even in those limited circumstances where the minor is authorized to act as the individual, section 164.502(g)(3)(ii)(A) would permit a covered entity to disclose protected health information about the minor to a parent if State law expressly required or permitted such disclosure.

We continue to object to deference to State laws that are less protective of an individual's privacy than is the Privacy Rule. The Privacy Rule generally preempts State laws that are contrary to the regulation and less protective of an individual's privacy, but lets stand those State laws that provide more protections. This rule not only makes good sense but is also required by HIPAA. *See* 42 U.S.C. § 1320d-7. Yet minors' health information is subject to a special rule of non-preemption that allows all State laws regarding disclosures to parents – even those that are contrary to the Privacy Rule and provide less protection for privacy – to stand. This approach is misguided. A State law authorizing, or worse, mandating disclosure of protected health information about a minor to a parent in a case where the minor has lawfully obtained health care services on his or her own is contrary to the policy that underlies the Privacy Rule and provides less protection for a minor's privacy. Such a State law should be preempted.

10. DISCLOSURES FOR TREATMENT, PAYMENT, OR HEALTH CARE OPERATIONS OF ANOTHER ENTITY
Proposed Sec. 164.506(c)

Proposed Modification:
The Department proposes several modifications to clarify how covered entities may use or disclose protected health information for treatment, payment, or health care operations, and to permit covered entities to disclose protected health information to other entities (including non-covered entities) for the second entity's treatment, payment, or health care operations activities.

Health Privacy Project Recommendation:
Most troubling is the Department's proposal to permit covered entities to disclose protected health information to other covered entities for the recipient's health care operations. This constitutes a significant alteration of the structure of the Privacy Rule, and the Department is proposing it without adequate justification. The Health Privacy Project recommends that the Department reconsider the necessity for such a change and assess whether the concept of "organized health care arrangement," which already is part of the Privacy Rule, addresses the quality assurance issues raised in the preamble. If the Department pursues modifications along these lines, the Department should craft narrow language that addresses actual problems – and only the problems identified in the preamble.

Rationale:
The Department's proposed modifications add the following statements to the proposed optional consent section (in proposed § 164.506(c)(1)-(5)), two of which significantly alter the approach taken in the Privacy Rule:

> (1) <u>One covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.</u> This merely states the obvious and does not change the Privacy Rule. (The Privacy Rule permits *providers* – as distinct from other covered entities – to engage in such activities only after obtaining consent of the individual. As discussed elsewhere in these comments, the proposal makes obtaining such consent optional.)
>
> (2) <u>One covered entity may disclose protected health information for treatment activities of another health care provider.</u> As the preamble notes, this is permitted under the Privacy Rule because of the breadth of the definition of the term "treatment." Thus, this statement merely clarifies what the Privacy Rule permits.
>
> (3) <u>One covered entity may disclose protected health information to another covered entity or another health care provider for the payment activities of the recipient.</u> As discussed below, the Department should craft more narrow language that addresses the actual problems explained in the preamble. At the very least, covered entities should be required to obtain assurances from non-covered providers, prior to disclosure of protected health information, that the recipient will not use protected health information for any other purpose or disclose it to others.

(4) One covered entity may disclose protected health information to another covered entity for specified health care operations activities of the recipient, if both entities have a relationship with the individual who is the subject of the protected health information. As discussed below, this proposal is extremely problematic due to its unnecessary breadth and the possibility of unforeseen consequences.

(5) One covered entity participating in an organized health care arrangement may disclose protected health information to another participant for any health care operations activities of the organized health care arrangement. This was implicit in the very concept of an organized health care arrangement in the Privacy Rule. Thus, adding this explicitly does not alter the Privacy Rule. We suggest, however, that such disclosures among the participants in an organized health care arrangement be permitted only when their privacy notices (or any joint notice they issue) informs individuals of this possibility.

Item 3 (from above list): One covered entity may disclose protected health information to another covered entity or another health care provider for the payment activities of the recipient.

The preamble to the proposed modifications states that such disclosures are necessary to permit ambulance service providers to receive the payment information they need directly from the hospital to which they transported the patient. *See* 67 Fed. Reg. 14781-2. The preamble also states that the proposal would permit collection agencies to use a patient's demographic information received from one provider to facilitate collection of another provider's bill. *See* 67 Fed. Reg. 14782. In these specific contexts, this makes sense. But the approach taken is not targeted and would not limit disclosures to these specific situations. At the very least, covered entities should be required to obtain assurances from non-covered providers, prior to disclosure of protected health information, that the recipient will not use protected health information for any other purpose or disclose it to others.

Item 4: One covered entity may disclose protected health information to another covered entity for specified health care operations activities of the recipient, if both entities have a relationship with the individual who is the subject of the protected health information.

According to the preamble, this proposed change to the Privacy Rule responds to concerns from health plans about their ability to obtain information needed for quality assessment activities, including accreditation and performance measures such as HEDIS (the Health Plan Employer Data and Information Set). *See* 67 Fed. Reg. 14782. Yet the health care operations activities for which disclosures would be permitted go well beyond quality assessment activities. Indeed, by referencing two components of the existing definition of "health care operations" (indicated under (1) and (2) below) and adding health care fraud and abuse detection or compliance (from another section of the existing definition of health care operations), one covered entity could disclose protected health information for the following health care operations activities of another covered entity:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of

generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment.

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

(3) Health care fraud and abuse detection or compliance.

There are two major problems with this approach. First, and most important, the Department has not even attempted to articulate the need to permit disclosures from one covered entity to another covered entity for such a broad range of purposes. As noted above, the preamble refers to disclosures by providers to health plans for quality assessment activities, including accreditation and performance measures. While such limited disclosures may justify a modification or clarification of the Privacy Rule, the Department proposes going way beyond fixing the stated concern. Again, the above list is far broader than the needs outlined in the preamble. It is far from clear why one covered entity should be permitted to share protected health information with another covered entity to perform all of these functions. For example, why should one covered entity be permitted to disclose protected health information to another covered entity for training programs? Again, instead of attempting to solve one problem with a targeted solution, the Department proposes to substantially relax the privacy protections in the Privacy Rule without even articulating why, let alone providing adequate justification.

Second, the Department has not explained why the concept of the organized health care arrangement, which is already in the Privacy Rule, does not already address concerns about health plans obtaining needed information from participating health care professionals about patients enrolled in the health plan. The definition of organized health care arrangement seems ideally suited to a health plan and its participating providers. *See* § 164.501. It specifically refers to joint activities such as quality assessment and improvement activities. Under an organized health care arrangement, providers participating in a plan's network could share protected health information about plan members necessary to carry out their joint activities.

If the Department ultimately decides to alter the Privacy Rule to permit disclosures between covered entities for certain – we urge, more limited – health care operations purposes, there are three safeguards in the proposal that are essential to retain.

- The requirement that both entities have a relationship with the individual who is the subject of the protected health information. As noted in the preamble, without this limitation, a health plan could seek to obtain protected health information about an individual who is not enrolled in the health plan, contrary to reasonable expectations. *See* 67 Fed. Reg. 14783.

- The requirement that these disclosures be among covered entities only, not among one covered entity and a non-covered entity. As noted in the preamble, this ensures that the information, once disclosed, will continue to be subject to the Privacy Rule. *See* 67 Fed. Reg. 14782.
- The continued application of the minimum necessary standard to these requests and disclosures. *See* 67 Fed. Reg. 14783.

11. DEFINITION OF PROTECTED HEALTH INFORMATION AND PROPOSED EXCLUSION OF "EMPLOYMENT RECORDS" Sec. 164.501

Proposed Modification:
The Department proposes to amend the definition of "protected health information" in section 164.501 to explicitly exclude "employment records," referred to in the preamble as "individually identifiable health information . . . held by a covered entity in its role as employer." *See* 67 Fed. Reg. 14804.

Health Privacy Project Recommendation:
The Health Privacy Project opposes this proposal because it threatens to undermine important safeguards in the Privacy Rule. The plain language of the proposed text appears to move outside of the Privacy Rule *any* use or disclosure of employees' health plan records, as well as information shared with an employer's on-site clinic where that clinic is a covered provider under the current Privacy Rule. Thus, through a sweeping "technical correction" in the applicable definition, this proposal takes health information that *is* protected by the Privacy Rule and renders it unprotected. This is especially dangerous because of the legitimate concern people have that employers will use protected health information, including genetic information, inappropriately to make employment-related decisions (such as deciding which employees to promote or fire).

Rationale:
Towards the end of the preamble's discussion of hybrid entities (discussed elsewhere in these comments), the Department proposes to amend the definition of "protected health information" in order "to avoid needless application of the hybrid entity provisions to a covered entity's activities as an employer." *See* 67 Fed. Reg. 14804. Specifically, the Department proposes to amend the definition of "protected health information" in section 164.501 to explicitly exclude "employment records." The Department states in the preamble that this exclusion refers to "individually identifiable health information . . . held by a covered entity in its role as employer," a characterization that itself renders protected health information unprotected. But the language of the proposed regulatory change appears to sweep even broader to encompass certain health information of employees whether their employer is a covered entity or not.

When a covered entity (whether a health plan, health provider, or clearinghouse) is functioning as a covered entity, the protected health information it creates or receives concerns its customers, members, patients, or clients. On the other hand, when a covered entity is functioning as an employer, the health information it creates or receives concerns its own employees (and their dependents). Thus, from the Department's explanation in the preamble, this proposed modification affects the extent to which the Privacy Rule protects information that a covered entity creates or receives about its own employees (and their dependents). While much of that health information clearly is not protected or impacted by the Privacy Rule (*e.g.*, information about an employee's fitness for duty provided by a non-covered entity), some of that medical information will be protected. For example, the Privacy Rule protects health information when it is created or received by a covered entity that is either a component of the covered entity (a covered provider such as on-site clinic) or a separate covered entity (an employer-sponsored

group health plan). These are separate covered entities under the Privacy Rule, but they still reflect the covered entity functioning as an employer with respect to its employees. Thus, even if the exclusion tracked the preamble ("individually identifiable health information . . . held by a covered entity in its role as employer"), it sweeps too broadly and turns protected health information into unprotected health information.

But the proposed regulatory language goes even further. It refers to "employment records," which could be interpreted to include certain health information of employees whether their employer is a covered entity or not. Most employers are not themselves covered entities because they are not engaged in health-related functions. But the health plan they offer to their employees (and their dependents) is a covered entity. (The Privacy Rule refers to these as "group health plans" and defines them as a subset of the term "health plan." *See* § 160.103.) The exclusion for "employment records" could be interpreted to apply to the health information created or received through employer-sponsored group health plans, thus moving the health plan claims of every working American (and their dependents) outside the scope of the Privacy Rule.

Similarly, an employer's on-site clinic might be a covered provider under the Privacy Rule if the clinic engages in the requisite standard electronic transactions. The exclusion for "employment records" could also be interpreted to apply to the health information created or received in such clinics, again with the effect of moving protected health information outside the scope of the Privacy Rule.

It is essential that any exclusion from the definition of protected health information be as narrowly crafted as possible. This is especially true when it comes to health information compiled by employers because of the legitimate concern people have that employers will use protected health information, including genetic information, inappropriately to make employment-related decisions (such as deciding which employees to promote or fire). The Privacy Rule contains important provisions to protect against inappropriate disclosures *to* employers and inappropriate uses of protected health information *by* employers. Most notable are the provisions governing employer-sponsored health plans. The Privacy Rule includes elaborate provisions governing the flow of protected health information from these group health plans to the employers that sponsor them, including the erection of firewalls and concrete assurances that the employer will not use protected health information for employment purposes. *See* § 164.504(f). These provisions apply whether the employer happens to be a covered entity (like a hospital) or a non-covered entity (like a car manufacturer). The proposed modification is especially dangerous because it threatens to unravel these protections.

The preamble attempts to limit the effect of the proposed exclusion by stating that it "does not apply to individually identifiable health information held by a covered entity when carrying out its health plan or health care provider functions." *See* 67 Fed. Reg. 14804. It is not clear what this limitation means. It is not clear if it refers to a covered entity carrying out its health plan or health care provider functions *with respect to its customers, members, patients, or clients*, or if it refers to a covered entity carrying out such functions *with respect to its employees*. In either case, the proposed exclusion language ("employment records") does not reflect any such limitation and, instead, lends itself to a relatively expansive reading. Nor does the preamble

reference to "individually identifiable health information . . . held by a covered entity in its role as employer" adequately capture such a limitation.

The proposed term "employment records" is not only dangerously broad, but it is confusing given the backdrop of federal employment laws. The Americans with Disabilities Act (as well as other federal laws) requires that medical information obtained by an employer be collected on separate forms and kept in confidential medical files, separate from personnel or other employment-related records. These laws distinguish between medical information and other types of employment records compiled by employers. Thus, it is especially confusing for the Department to propose the use of the term "employment records" as a way of referring to certain medical records compiled by employers.

12. DISCLOSURE OF ENROLLMENT AND DISENROLLMENT INFORMATION TO SPONSORS OF GROUP HEALTH PLANS
Proposed Sec. 164.504(f)(1)(iii)

Proposed Modification:
The Department proposes to permit group health plans (as well as HMOs and issuers) to disclose to the sponsor of the group health plan (usually an employer) information on whether an individual is participating in the group health plan (or is enrolled in, or has disenrolled from, the HMO or issuer).

Health Privacy Project Recommendation:
The Health Privacy Project does not oppose this proposed modification because it is limited to information about whether the individual is participating in or enrolled in the plan and does not permit the disclosure of any other protected health information.

Rationale:
The Privacy Rule permits group health plans to disclose "summary health information" (which may be protected health information) to sponsors of group health plans for two limited purposes: (1) allowing the sponsor to obtain bids for providing insurance coverage under the group health plan; or (2) modifying, amending, or terminating the group health plan. *See* § 164.504(f)(1)(ii). To constitute "summary health information," the information must be stripped of all identifiers except for zip codes. *See* § 164.504(a). Before disclosing any other type of protected health information to the plan sponsor, the group health plan must ensure that the plan documents include privacy-related assurances, including the erection of firewalls and assurances that the plan sponsor will not use protected health information for employment-related actions or decisions. *See* § 164.504(f)(2).

The text of the Privacy Rule does not explicitly refer to disclosures to plan sponsors about whether an individual is participating in the group health plan (or enrolled in the HMO or issuer). However, the preamble to the final Privacy Rule states: "We note that a plan sponsor may perform enrollment functions on behalf of its employees without meeting the conditions above [relating to summary information and plan document requirements]." *See* 65 Fed. Reg. 82509.

The Department proposes to add to the text of the Privacy Rule the following (proposed § 164.504(f)(1)(iii)):

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

This proposed modification is acceptable because it is limited to very specific information (whether the individual is participating or not) and does not permit the disclosure of any other health information.

13. MINIMUM NECESSARY AND ORAL COMMUNICATIONS
Secs. 164.502(a) and 164.530(c)

Proposed Modification:
The Department proposes to:

- Modify the Privacy Rule to add a new provision which would explicitly permit certain "incidental" uses and disclosures that occur as a result of an otherwise permitted use or disclosure under the Privacy Rule.
- Modify the administrative requirements to expressly require covered entities to reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Health Privacy Project Recommendation:
The Health Privacy Project does not believe a modification expressly permitting incidental uses is necessary, but understands that the Department wishes to calm the fears of some of those in the health care industry. We commend the Department for including a related modification that expressly requires covered entities to reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Rationale*:*
The Privacy Rule imposes a requirement that covered entities "reasonably safeguard" protected health information from any intentional or unintentional use or disclosure that is in violation of the rule. Some in the health care industry chose to read this "reasonable" standard as an absolute strict prohibition against incidental or unintentional disclosures that could occur as a by-product of common and essential health care communications and practices. In response to these concerns, the Department issued guidance in July 2001 clarifying that the standard was not absolute but reasonable. We believe the text of the Privacy Rule and the guidance sufficiently clarify this issue. However, we recognize that the Department wishes to assure these concerned covered entities that the standard is one that requires reasonable, not absolute, protections.

We strongly support the Department's expressly conditioning permitted incidental uses and disclosures on the covered entity's compliance with the applicable requirements of the minimum necessary standards and the standards that require safeguards. *See* § 164.502(a)(1)(iii).

We also believe that the proposed express requirement that covered entities reasonably safeguard protected health information to limit incidental uses or disclosures is essential to ensuring that the incidental use provisions are not abused. *See* § 164.530(c).

14. BUSINESS ASSOCIATE TRANSITION PROVISIONS
Sec. 164.532 (d) & (e)

***Proposed Modification*:**
The Department proposes new transition provisions to allow most covered entities to continue to operate under certain existing business contracts with business associates for up to one year beyond the current compliance date for the Privacy Rule.

***Health Privacy Project Recommendation*:**
The Health Privacy Project recommends that the Department retain the existing compliance date for all aspects of the Privacy Rule**.** The Department has provided covered entities with a model business associate contract, which should ease compliance efforts.

Rationale:
Under the proposed modification, if prior to the ***effective date*** of the modified provision, a covered entity enters into and is operating under a written contract with a business associate, the covered entity essentially receives up to a one-year delay in having to enter into a contract that meets the requirement of the Privacy Rule with the business associate. We believe this approach will encourage covered entities to enter into stopgap contracts instead of encouraging them to formally execute business associate contracts.

The Department has provided a model business associate contract, which should ease the burden in complying with the business associate by the original compliance date. Moreover, executing stopgap contracts merely adds to the cost of implementing the Privacy Rule.

We believe the original compliance date should be maintained.

The Health Privacy Project's comments are endorsed by:

Alliance for Fairness in Reforms to Medicaid
American Association of People with Disabilities
American Counseling Association
American Nurses Association
American Public Health Association
ARPKD/CHF Alliance
Bazelon Center for Mental Health Law
Center for Democracy and Technology
Center for Medical Consumers
Center for Reproductive Law & Policy
Citizen Action of New York
Electronic Privacy Information Center
Epilepsy Foundation
Families USA
Family Violence Prevention Fund
Florida AIDS Action
Hadassah, the Women's Zionist Organization of America
National Alliance for the Mentally Ill
National Association of People with AIDS
National Association of Social Workers
National Health Law Program, Inc.
National Mental Health Association
National Multiple Sclerosis Society (only on consent for treatment, payment, and health care operations)
National Organization for Rare Disorders
New York Legal Assistance Group
The Arc of the United States
Title II Community AIDS National Network