TESTIMONY OF

JANLORI GOLDMAN, DIRECTOR
HEALTH PRIVACY PROJECT, GEORGETOWN UNIVERSITY
INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY

BEFORE THE
SENATE COMMITTEE ON HEALTH, EDUCATION, LABOR AND PENSIONS

ON THE

"OVERSIGHT HEARING ON MEDICAL PRIVACY"

APRIL 16, 2002

Committee Chairman Kennedy, Senator Gregg and Members of the Committee:

On behalf of the Health Privacy Project, I am very appreciative for the invitation to testify before you today at this oversight hearing on medical privacy. The Project, which is part of the Institute for Health Care Research and Policy at Georgetown University, is dedicated to broadening access to health care, and improving the quality of care by ensuring that the privacy of people's medical information is protected in the health care arena. The Health Privacy Project also coordinates the Consumer Coalition for Health Privacy, comprised of over 100 major groups representing consumers, health care providers, and labor, disability rights, and disease groups. The Coalition's Steering Committee includes AARP, American Nurses Association, Bazelon Center for Mental Health Law, National Association of People with AIDS, Genetic Alliance, National Multiple Sclerosis Society, and National Partnership for Women & Families.

The Health Privacy Project conducts research and analysis on a wide range of health privacy issues. Recent Project publications include: *Best Principles for Health Privacy* (1999), which reflects the common ground achieved by a working group of diverse health care stakeholders; *The State of Health Privacy* (1999), the only comprehensive compilation of state health privacy statutes, which we are currently in the process of updating; *Implementing the Federal Health Privacy Regulation in California* (2002); *Privacy and Confidentiality in Health Research* (2001), commissioned by the National Bioethics Advisory Commission; *Report on the Privacy Policies and Practices of Health Web Sites* (2000), which found that the privacy policies and practices of 19 out of 21 sites were inadequate and misleading; "Virtually Exposed: Privacy and E-Health" (2000), published in *Health Affairs*; and *Exposed Online: Why the New Federal Health Privacy Regulation Doesn't Offer Much Protection to Internet Users* (2001). All of our work is available to the public at our Web site, www.healthprivacy.org.

The Health Privacy Project's mission is to foster greater public trust and confidence in the health care system, thereby enabling people to more fully participate in their own care and in research without putting themselves at risk for unwanted—and unwarranted—intrusions. It is wrong to force people to choose between seeking health care and safeguarding their jobs, benefits, and reputations. People should not have to worry when taking a genetic test for breast cancer, or filling a prescription for an anti-depressant, that this most sensitive health information will be used outside the core health care setting, but they do worry and with good reason.

The new medical Privacy Rule,[1] issued by the Department of Health and Human Services (the Department) in December 2000 and in effect since April 2001, is a landmark regulation, setting in place the first comprehensive federal safeguards for people's medical records. With still a year to go before health care organizations must fully comply, the centerpieces of this new privacy law are in jeopardy. We appreciate the opportunity to share our concerns with this Committee about the Bush Administration's proposal to substantially weaken the medical Privacy Rule. We express particular concern about the Department's proposal to eliminate the patient consent requirement, and to severely weaken the limits on the marketing of people's medical records. Joining with us in opposition to these two proposed changes, are the following organizations:

- AIDS Action Council

[1] The Privacy Rule is contained in title 45 of the Code of Federal Regulations. All citations in this testimony are to the pertinent section of, or proposed amendment to, 45 C.F.R. unless otherwise noted.

- American Association for Geriatric Psychiatry
- American Counseling Association
- American Mental Health Counselors Association
- American Nurses Association
- American Psychoanalytic Association
- American Psychological Association
- Bazelon Center for Mental Health Law
- Brooklyn-wide Interagency Council of the Aging
- Consumers Union
- CWA Local 1168 Nurses United
- Electronic Privacy Information Center
- Family Violence Prevention Fund
- Genetic Alliance
- Hadassah
- National Association of People with AIDS
- National Mental Health Association
- National Organization for Rare Disorders
- NYC Chapter, National Association of Social Workers
- Title II Community AIDS Action Network
- Westchester Progressive Forum

We expect that many other organizations and individuals will voice their opposition to these proposals before the comment period closes.

Our testimony today will summarize both our concerns with and support for the Department's proposed modifications to the Privacy Rule. Our statement also includes a brief history of the Privacy Rule, and the urgent need within the public and the health care system for strong, enforceable medical privacy safeguards. In addition, we correct the misperception that the long-term cost of implementing the Privacy Rule –along with its companion HIPAA standards—will outweigh the benefits. In fact, the Office of Management and Budget (OMB) released a report last month documenting that protecting privacy, when done hand-in-hand with the related HIPAA rules, will actually result in substantial cost savings.

I. Urgent Public Need for Medical Privacy

The lack of a national health privacy law has had a negative impact on health care, both on an individual as well as a community level. One out of every six people withdraws from full participation in their own care out of fear that their medical information will be used without their knowledge or permission, as documented by a 1999 survey conducted for the California HealthCare Foundation. (Available at www.chcf.org.) These privacy-protective behaviors include patients providing inaccurate or incomplete information to doctors, doctors inaccurately coding files or leaving certain things out of a patient's record, people paying out of pocket to avoid a claim being submitted, or in the worst cases, people avoiding care altogether.

More specifically, a 1997 survey documenting people's fears about genetic discrimination showed that 63 percent of people would not take genetic tests if health insurers or employers

could obtain the results. (*Genetic Information and the Workplace,* issued on January 20, 1998 by the U.S. Departments of Labor, Health and Human Services, and Justice, and the U.S. Equal Employment Opportunity Commission). And, a recent study involving genetic counselors documents that fear of discrimination is a significant factor affecting willingness to undergo testing and to seek reimbursement from health insurers. (Hall, Mark A. and Stephen S. Rich, *Genetic Privacy Laws and Patients' Fear of Discrimination by Health Insurers: The View from Genetic Counselors*, 28 Journal of Law, Medicine & Ethics 245-57 (2000).)

An April 2001 Harris survey documents that nearly four out of ten (40%) people with multiple sclerosis said they have lied or failed to disclose their diagnosis to colleagues, co-workers, friends or even family members out of fear of job loss and stigma.

These survey figures come to life in the daily media reports of people being harmed by the use of their health information outside the core health care arena. To highlight just a few:

- Eckerd's Drug Stores in Florida is being investigated by the state Attorney General for its marketing practices. When Eckerd customers pick up their prescriptions, they sign a log indicating they do not want counseling from a pharmacist. Eckerd's has been using that signature as an authorization to use the customer's prescription drug records for mailing promotions and discounts financed by drug companies.

- Terri Seargent, a North Carolina resident, was fired from her job after being diagnosed with a genetic disorder that required expensive treatment. Three weeks before being fired, Terri was given a positive review and a raise. As such, she suspected that her employer, who is self-insured, found out about her condition, and fired her to avoid the projected expenses.

- The medical records of an Illinois woman were posted on the Internet without her knowledge or consent a few days after she was treated at St. Elizabeth's Medical Center following complications from an abortion at the Hope Clinic for Women. The woman has sued the hospital, alleging St. Elizabeth's released her medical records without her authorization to anti-abortion activists, who then posted the records online along with a photograph they had taken of her being transferred from the clinic to the hospital. The woman is also suing the anti-abortion activists for invading her privacy.

- Several thousand patient records at the University of Michigan Medical Center inadvertently lingered on public Internet sites for two months. The problem was discovered when a student searching for information about a doctor was linked to files containing private patient records with numbers, job status, treatment for medical conditions and other data.

- Joan Kelly, an employee of Motorola, was automatically enrolled in a "depression program" by her employer after her prescription drugs management company reported that she was taking anti-depressants.

- Eli Lilly and Co. inadvertently revealed 600 patient e-mail addresses when it sent a message to every individual registered to receive reminders about taking Prozac. In the past, the e-mail messages were addressed to individuals. The message announcing the end of the reminder service, however, was addressed to all of the participants.

- A few months ago, a hacker downloaded medical records, health information, and social security numbers on more than 5,000 patients at the University of Washington Medical Center. The University conceded that its privacy and security safeguards were not adequate.

In the absence of a federal health privacy law, these people suffered job loss, loss of dignity, discrimination, and stigma. Had they acted on their fears and withdrawn from full participation in their own care – as many people do to protect their privacy – they would have put themselves at risk for undiagnosed and untreated conditions. In the absence of a law, people have faced the untenable choice of shielding themselves from unwanted exposure or sharing openly with their health care providers.

II. The Genesis of the Privacy Rule

The current federal health Privacy Rule is a major victory for all health care consumers, and takes a significant step toward restoring public trust and confidence in our nation's health care system. The regulation promises to fill the most troubling gap in federal privacy law, setting in place an essential framework and baseline on which to build. Each one of us stands to benefit from the Privacy Rule in critical ways, including greater participation in the health care system, improved diagnosis and treatment, more reliable data for research and outcomes analysis, and greater uniformity and certainty for health care institutions as they develop privacy safeguards and modernize their information systems.

Most notably, the current Privacy Rule grants people the right to see and copy their own medical records; requires health care providers to obtain patient consent before using their records for treatment, payment and health care operations; imposes limits on using medical records for marketing; imposes safeguards on publicly and privately funded research use of patient data; somewhat limits law enforcement access to medical records; and allows for civil and criminal penalties to be imposed if the Rule is violated.

The Privacy Rule was issued by the Department in December 2000 in response to a mandate from Congress included in the 1996 Health Insurance Portability and Accountability Act (HIPAA), which required that if Congress did not enact a medical privacy statute by August 1999, then the Department was required to promulgate regulations. This rule has been the subject of a lengthy, thorough, and robust rule-making process – both before and since its December 2000 release in final form.

Despite intense pressure from some in the health care industry, the Bush Administration allowed this important regulation to go into effect in April 2001. The first implementation guidance issued by the Department on July 6, 2001, addresses the many misstatements and exaggerations that some in the industry have been spreading about the Privacy Rule. On its face, the guidance

was aimed at calming industry fears, and we hoped it would lead to greater acceptance of the regulation and foster compliance with the regulation. The guidance also indicated the changes the Department intended to propose to make to the regulation.

We acknowledge that the Privacy Rule—as finalized—has serious gaps and weaknesses, some of which can only be remedied by Congress, and some of which are within the Department's authority to regulate. One shortcoming is that the rule only directly regulates providers, plans and clearinghouses, and does not directly regulate employers, pharmaceutical companies, workers' compensation insurers, and many researchers. The rule also lacks a private right of action that would give people the right to sue if their privacy was violated. Under HIPAA, only Congress and the states are empowered to address these limits. However, where the Department does have the power to strengthen the Rule, it has chosen instead to dilute it.

III. Summary of the Health Privacy Project's Comments on the Department's Proposed Modifications to Consent and Marketing

A. 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 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:
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 substitutes 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.

This debate is about much more than the label on the piece of paper that a patient signs, or about whether a patient is given two pieces of paper (a notice and consent form) or just one (a notice).

There are fundamental differences between a consent process and acknowledgement of a receipt of a notice. Seeking advance permission from a patient before using or disclosing health information acknowledges first and foremost that it is the patient's decision whether to entrust others with his or her private medical information and under what circumstances. 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 refusing to provide treatment. However, it is by no means clear that providers will withhold treatment even though permitted to do so, particularly when the individual consents to some uses/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.

That the Department has chosen radical surgery – total elimination of the consent requirement – when much more targeted, privacy-protective interventions would have sufficed is especially troublesome.

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.

B. Marketing
Secs. 164.501 and 164.508(a)(3)

Proposed Modifications:
The Department proposes to reduce the Privacy Rule's privacy 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 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 has received or will receive 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 care related services or products or for products and services not related to health care.

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 a patient a letter encouraging her to switch her 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 Appendix A at 1. 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. At the opposite end of the continuum, because the covered entity is being paid to use health information to market a product or service that is totally unrelated to health, the covered entity must obtain patients' prior authorization before it can use their health information for these marketing purposes. The treatment of these two categories of health information remains relatively unchanged under the proposed modifications to the Privacy Rule. *See* Appendix A at 2.

With respect to 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, 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. In light of these conflicts, 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 communications. 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* Appendix A at 1.

Many consumers believe that the Privacy Rule's delayed opt-out approach is insufficient to protect privacy. They have urged the Department to modify the rule to require that covered entities obtain patient authorization prior to engaging in this type marketing activity (*i.e*., where the covered entity is paid to encourage the use or purchase of a health related product or service).

In response to these concerns, the Department essentially proposes to eliminate the protections (albeit inadequate) that currently exist. The Department accomplishes this by removing paid communications that encourage the use or purchase of a health related product or service entirely from the definition of "marketing." This proposed change effectively allows covered entities to make this type of paid communication without *any* prior authorization or chance to opt out. [2] *See* Appendix A at 2.

[2] The Department's explanation that it is proposing to "explicitly require covered entities to first obtain the individual's specific authorization before sending them any marketing materials" "based on consumer concerns that

We oppose this change 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 to be "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 and select patients based on their health information 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.[3]

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.[4]

Third, the proposed modification eliminates any control that an individual may have over the use of his protected health information for receiving 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 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

---

the marketing provisions in the current rule does not protect individuals' privacy" is disingenuous at best, given that they accomplish this by removing an entire category of communications from the definition of "marketing." *See* Department's Press Release, March 21, 2002.

[3] *See e.g.*, Robert O'Harrow, Jr., *Prescription Fear, Privacy Sales* The Washington Post, February 15, 1998 at A1; Henry l. Davis, "More Eckerd Questions," *St. Petersburg Times*, March 5, 2002 at 1E.

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

remuneration for making the communication. We would apply this standard to both health related and non-health related communications. Using this definition presents a rather 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. Health care consumers should have control over whether their health information is used for profit-making purposes that are only tangentially related to their health.

Appointment reminders and prescription refill notices

A number of concerns have been raised about communications, such as appointment reminders and prescription refill notices, that 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, if a covered entity is receiving payment from a third party for making the communication, it is pursuing activity that is at least partially 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.

IV. Summary of Health Privacy Project Comments on Other Proposed Modifications

1. Hybrid Entities
Sec. 164.504

Proposed Modification:

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. Permit (as conditioned below) covered entities whose primary functions are health care to be hybrid entities.
- 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.

2. Disclosures of Protected Health Information Related to FDA-regulated Products or Activities
Sec. 164.512(b)

Proposed Modifications: The Department proposes to create an extremely broad exception to the general requirement to obtain authorization prior to the disclosure of protected health information. The proposed modification would allow 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." Under this proposed modification, disclosures would no longer be required by, or at the direction of, the FDA.

HPP Recommendations: The Health Privacy Project strongly opposes the Department's proposal and urges the Department to retain the current provisions of the Privacy Rule. The Privacy Rule provides a specific series of public health related exceptions to the authorization requirement. The proposed modifications, however, would create a vague and general standard, under the rubric of "public health," that would open the door to the release of protected health information to pharmaceutical companies and arguably to tobacco companies as well. We do not see a genuine public health need that justifies such a significant expansion in the Privacy Rule.

3. 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.

4. 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 to the provisions on reviews preparatory to research so that researchers could remove protected health information from a covered entity's premises for recruitment purposes.
(3) commends the Department for retaining an individual's right to revoke a research authorization, but 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.

5. Individual Authorization
Sec. 164.508

Proposed Modifications:
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 under the Privacy Rule; (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 an individual knows how his or her information will and will not be used or disclosed so that s/he 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.

6. 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.

7. 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 Recommendations*:* 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.

8. 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.

9. 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." 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).

10. 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 supports 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.

11. Minimum Necessary and Oral Communications
Sec. 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; and
- 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.

12. 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.

V. Cost: OMB Reports Privacy Regulation will Save Money

According to a March 2002 report just issued by OMB's Office of Information and Regulatory Affairs (OIRA), the Department estimates that the cost associated with implementing the Privacy Rule (approximately $17 billion over ten years) will be greatly offset by the cost savings associated with implementing HIPAA's transactions standards (approximately $29 billion **saved** over ten years). *See* Appendix B for excerpt of report. The cost of implementing the Privacy Rule must not be viewed in isolation. The Privacy Rule is an integral – and necessary – part of a package of Administrative Simplification rules. The goal of standardizing electronic health care transactions is to create efficiencies and save money. When the Privacy Rule is implemented together with the transactions standards and other Administrative Simplification rules, as contemplated by Congress, a net savings will be achieved. Finally, we must also acknowledge the benefits reaped by increased patient participation in health care and research, as well as the qualitative benefits that are achieved by furthering this important societal value.

Conclusion

When President Bush allowed the Privacy Rule to go into effect last April, he issued a strong statement about the need to protect patient privacy and foster confidence that people's "personal medical records will remain private." The President also pledged during his campaign to support a law requiring that a "company cannot use my information without my permission to do so," and expressed support for strong laws protecting medical and genetic privacy. In fact, William Safire dubbed him the "privacy President" in a New York Times column shortly after the Privacy Rule went into effect. But, if the Department's proposed changes become final, the Privacy Rule will legalize many of the practices that caused public outcry for a law. We urge the Bush Administration not to roll back the important gains our country has made in protecting the privacy of people's medical records. We urge policymakers to look at the substantial progress being made by doctors, hospitals, and health plans in complying with the Rule. And finally, we urge that glitches in the regulation be addressed through narrowly tailored fixes that preserve the integrity of the final Rule.

ADDENDUM TO
HEALTH PRIVACY PROJECT TESTIMONY

Organizations Supporting Health Privacy Project's Recommendation on Consent
*National Multiple Sclerosis Society

Organizations Supporting Health Privacy Project's Recommendations on Consent and Marketing
AIDS Action Council
American Association for Geriatric Psychiatry
American Counseling Association
American Mental Health Counselors Association
American Nurses Association
American Psychoanalytic Association
American Psychological Association
Bazelon Center for Mental Health Law
Brooklyn-wide Interagency Council of the Aging
*Center for Medical Consumers
Consumers Union
CWA Local 1168 Nurses United
Electronic Privacy Information Center
*Epilepsy Foundation
Family Violence Prevention Fund
Genetic Alliance
Hadassah
*Legal Action Center
National Association of People with AIDS
*National Association of Social Workers
National Mental Health Association
National Organization for Rare Disorders
NYC Chapter, National Association of Social Workers
Title II Community AIDS Action Network
Westchester Progressive Forum

* Organizations that endorsed Health Privacy Project recommendation(s) after submission of written testimony

HEALTH PRIVACY PROJECT
INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY
GEORGETOWN UNIVERSITY

MARKETING
CURRENT PRIVACY RULE

TEST: DOES COVERED ENTITY RECEIVE REMUNERATION FOR COMMUNICATION* RECOMMENDING PRODUCT OR SERVICE?

NOT MARKETING

NOT PAID FOR RECOMMENDING PRODUCT OR SERVICE

Requirements
No authorization required

Example
Pharmacy on its own initiative recommends different medicine to avoid adverse drug reaction.

MARKETING

PAID FOR RECOMMENDING HEALTH RELATED PRODUCT OR SERVICE

Requirements
No prior authorization required if material:

- Gives patient chance to **opt out** of receiving further communications;
- **Notifies** patient that covered entity is being paid; and
- **Identifies** covered entity as source of communication.

Example
Drug company pays pharmacy to identify and send patients taking drug co.'s brand of medicine prescription refill reminders.

Example
Drug company pays pharmacy to identify patients taking certain medicines and to send them letters recommending they switch to drug company's brand.

PAID FOR RECOMMENDING PRODUCT OR SERVICE _NOT_ RELATED TO HEALTH

Requirements
Prior authorization required

Example
Pharmacy is paid by third party to identify patients taking depression medicine and to send them advertisements for vacation destinations.

* All communications are made by a covered entity and encourage a patient to purchase or use a product or service.

HEALTH PRIVACY PROJECT

INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY
GEORGETOWN UNIVERSITY

MARKETING

PROPOSED MODIFICATIONS TO PRIVACY RULE

TEST: DOES COMMUNICATION* RECOMMEND A PRODUCT OR SERVICE RELATED TO HEALTH?

NOT MARKETING

NOT PAID FOR RECOMMENDING PRODUCT OR SERVICE

Requirements

No authorization required

Example

Pharmacy on its own initiative recommends different medicine to avoid adverse drug reaction.

PAID FOR RECOMMENDING HEALTH RELATED PRODUCT OR SERVICE

Requirements

- **No authorization**
- **No opt out**
- **No notification** that covered entity is paid to encourage purchase or use product or service
- **No identification** of source of material

Example

Drug company pays pharmacy to identify and send to patients taking drug co.'s brand of medicine prescription refill reminders

Example

Drug company pays pharmacy to identify patients taking certain drugs and to send letters encouraging them to switch to drug company's brand.

MARKETING

PAID FOR RECOMMENDING PRODUCT OR SERVICE *NOT* RELATED TO HEALTH.

Requirements

Prior authorization required

Example

Pharmacy is paid by third party to identify patients taking depression medication and to send them advertisements for vacation destinations.

* All communications are made by a covered entity and encourage a patient to purchase or use a product or service.