UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

February 17, 2000

U.S. Department of Health and Human Services
Assistant Secretary for Planning and Evaluation
Attention: Privacy-P, Room G-322A
Hubert Humphrey Building
200 Independence Avenue SW
Washington, D.C. 21201

Dear Sir or Madam:

The Federal Trade Commission (the Commission or FTC) is pleased to offer comments on the proposed privacy standards pursuant to Section 262 of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").(1) HHS has proposed a Rule (2) to protect the privacy of individually identifiable "health information"(3) maintained or transmitted electronically. It proposes standards for: the privacy rights of individuals who are the subject of this information; procedures for the exercise of those rights; the authorized uses of this information; and required disclosures concerning such use. The Rule applies to health plans, health care clearinghouses, and certain health care providers.

The Commission strongly supports the Rule's proposed "individual authorization," or "opt-in," approach to the ancillary use of individually identifiable health information for purposes other than those for which the information was collected. Our comments also suggest that HHS may wish to consider suggestions to improve the disclosure requirements in two proposed forms -- the General Notice and the Model Authorization forms.

A. Interest and Expertise of the Federal Trade Commission

The FTC is a law enforcement agency whose mission is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and to increase consumer choice by promoting vigorous competition. The Commission's primary legislative mandate is to enforce the Federal Trade Commission Act ("FTCA"), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.(4) With the exception of certain industries, the FTCA provides the Commission with broad law enforcement authority over entities engaged in or whose business affects commerce(5) and with the authority to gather information about such entities.(6) Pursuant to these responsibilities, the Commission has acquired considerable experience in addressing deceptive health care practices,(7) and has long had particular interest in, and gained extensive experience dealing with, privacy and consumer protection issues.(8)

Beginning in April 1995, the Commission held a series of public workshops on online privacy. It also has examined: Web site practices in the collection, use, and transfer of consumers' personal information; self-regulatory efforts and technological developments to enhance consumer privacy; consumer and business education efforts; the role of government in protecting online information privacy; and special issues raised by the online collection and use of information from and about children. The Commission issued three reports to Congress based on its initiatives in the privacy area: *Self-Regulation and Privacy Online: A Report to Congress* (July 1999); *Privacy Online: A Report to Congress* (June 1998) ("1998 Report"); and *Individual Reference Services: A Report to Congress* (December 1997). These efforts have provided a forum for dialogue among members of the information industry and online business community, government representatives, privacy and consumer advocates, and experts in interactive technology.

Further, the Commission has brought enforcement actions under Section 5 of the Federal Trade Commission Act to address deceptive online information practices.(9)

The Commission in its 1998 Report documented the widespread collection on the Internet of personal information from young children, and recommended that Congress adopt legislation setting forth standards for the online collection of personal information from children. Just four months after the 1998 Report was issued, Congress enacted the Children's Online Privacy Protection Act of 1998 ("COPPA").(10) As required by the Act, on October 20, 1999, the Commission issued a final *Children's Online Privacy Protection Rule*, which implements the Act's fair information practice standards for commercial Web sites directed to children under 13 and Web sites that knowingly collect personal information from children under 13.(11)

B. Individual Authorization: The Proposed "Opt-in" Approach Protects Consumer Privacy

Section 164.508(a)(2) of the proposed HHS Rule requires that covered entities first obtain written "individual authorization" before they use or disclose individuals' protected health information for any purpose other than health care treatment, payment, or health care operations. Thus, individual authorization is required before the protected information can be used for marketing of health items or services or sale of the information to third parties.(12) We believe that this "opt-in," or "express consent," requirement is the most appropriate approach for the use of sensitive medical information for purposes other than those for which it was collected.(13)

In enacting COPPA, Congress similarly required an "opt-in" approach with respect to most information obtained online from and about children. COPPA requires operators of websites directed to children and operators who knowingly collect personal information from children to, among other things, obtain prior verifiable parental consent for the collection, use, and/or disclosure of personal information from children.(14)

Like personally identifiable information about children, personal medical information is among the most sensitive types of information collected from individuals. Consistent, national survey results demonstrate that, of all the types of individual information collected, consumers are most troubled by the prospect of unauthorized disclosure of medical information.(15) Over three-quarters of the public believes that it has lost control over how companies apply and circulate personal information,(16) and those who know the most about the application of medical information -- physicians, and heads of medical societies, health insurers, and hospitals -- also belong to the group that is most concerned about threats to personal privacy.(17) In addition, seventy-five percent of consumers seeking health information on the Internet are "concerned" or "very concerned" about the health sites they visit sharing their personal health information with a third party, without their permission.(18) This concern is accompanied by strong consumer support for protections for medical information.(19)

Congress also recognized this special sensitivity of health care information when it adopted an "opt-in" regime to safeguard the medical data of patients who undergo treatment for alcohol or drug abuse in programs receiving federal funds or subject to federal regulation.(20) Congress took similar action in requiring an "opt-in" approach for the furnishing of personal medical information by credit bureaus for employment purposes or in connection with credit or insurance transactions.(21)

The use or disclosure of individual health care information for purposes ancillary to the purposes for which it was collected should be entitled to similar "opt-in" protection. HHS recognizes the potential for ancillary uses, including, among others, targeted marketing of new products. HHS further acknowledges that once a patient's health information is disclosed outside of the treatment and payment arena, it can be very difficult for the individual to determine what additional entities have seen, used and further disclosed the information.(22) It is likely that many consumers would choose not to share their personal medical information for such ancillary uses, particularly in these circumstances. Requiring authorization from the patient in this instance is appropriate.(23)

C. Section 164.508(d)(ii): Requests for Authorizations Should Be Specific

Section 164.508(d)(ii) of the proposed Rule requires only that a covered entity's request for individual authorization to permit ancillary uses of health information contain "[a] description of the purpose(s) of the requested use or disclosure."(24) This limited disclosure may not adequately inform consumers of the actual, intended use of the information. By contrast, Section 164.512(d) requires that the General Notice of information practices must describe the intended uses and disclosures "in sufficient detail to put the individual on notice of the uses and disclosures expected to be made of his or her protected health information."(25) This latter standard helps ensure that individuals understand what uses and disclosures will be made of their sensitive health information. Such understanding is crucial to ensure that individuals make informed choices about how their health information is used.

In its current formulation, Section 164.508(d)(ii) might encourage or permit covered entities to use broad or vague language to describe the purpose of a requested use or disclosure. For example, an intended marketing use of individual health information might be described with the phrase "to provide you with information about your health care," which tells the patient little about the actual intended use of the information. HHS may wish to consider applying to authorizations required by the proposed Rule the "in sufficient detail" standard now applied to the required General Notice disclosure.

D. Notice of Information Practices Should be Clear and Conspicuous

Sections 164(a)-(d) require that covered health plans and health care providers give consumers adequate notice, by means of a "General Notice of Information Practices," of their policies and procedures with respect to health information. The Notice must include an explanation of all of the patients' rights granted by the Rule, including rights to grant and revoke authorizations for ancillary uses and to request restricted use.(26) Section 164.512(e) of the proposed Rule requires covered entities to "provide" the Notice to consumers at the time that service is first delivered, make copies available for consumers to take, and post it in their offices. Where face-to-face contact is unlikely, providers could provide the Notice by mail, e-mail, or by linking it to their website.(27)

The Notice document is the only general disclosure and explanation of patients' rights required by the proposed Rule, and the information it contains is important to consumers' understanding of their rights under the Rule. For this reason, it is important that this notice not be buried in fine print, placed in inconspicuous locations, or otherwise hidden. To this end, we suggest that Section 614.512(e) state that covered entities "must make the notice required by this section available, in a clear and conspicuous manner. . . ." In this context, the principle of "clear and conspicuous" requires that the Notice should be noticeable and understandable so that it gives consumers meaningful and effective notice of their rights under the Rule. To make it more likely that the Notice satisfies the clear and conspicuous standard, HHS may wish to consider requiring that the Notice be provided to the consumer under separate cover.

E. Model Provider Notice and Authorization Forms

The proposed Rule includes a sample "Provider Notice of Information Practices" form(28) and a model "Authorization For Release of Information" form(29) that may be used in providing the Rule's required General Notice and in obtaining individual authorization for ancillary uses of protected health information. HHS may wish to consider language and format changes to help ensure that the form effectively communicates to patients important information about their authorization rights.

For example, the General Notice is currently titled "Provider Notice of Information Practices." We would suggest that the title more directly tell consumers that the document concerns their privacy rights. A title such as "Important Information - Your Privacy Rights" may accomplish that objective.

Similarly, in certain instances additional information may improve the Authorization form. For example, the notice provided in Section C. 2. of the form concerning patients' right to revoke any authorization given would, in our view, be made more effective by adding the names of the providing organization and contact person that patients need to notify to effectuate any such revocation.

Conclusion

We are pleased to submit these comments. Please contact Matthew Daynard, at (202) 326-3291, if there are questions about our comments or additional assistance that we may provide in your efforts in this important matter.

By direction of the Commission.

Endnotes:

1. Public Law 104-191 (August 21, 1996).

2. 64 FR 59918 (Nov 3, 1999).

3. "Health information" is defined in HIPAA as "any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual." Section 160.103.

4. 15 U.S.C. § 45(a).

5. The Commission does not have criminal law enforcement authority. Further, certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance, are wholly or partially exempt from Commission jurisdiction. See Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2), and the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

6. 15 U.S.C. § 46(a). The Commission's authority to conduct studies and prepare reports relating to the business of insurance is limited, however.

7. *See, e.g.*, Schering-Plough Healthcare Products, Inc., Docket No. C-3741 (May 16, 1997) (consent) (sun protection products); Olsen Laboratories, Inc., 119 F.T.C. 161 (1995) (consent) (arthritis treatment products); Synchronal Corp., 116 F.T.C. 989 (1993) (consent) (baldness cure and cellulite treatment); and Nutri/System, Inc. 116 F.T.C. 1408 (1993) (consent) (diet clinic services).

8. The Commission also has law enforcement responsibilities under the Fair Credit Reporting Act, which, among other things, provides certain privacy protection for consumers by limiting consumer reporting agencies' disclosure of information in their consumer reports to entities for statutorily prescribed "permissible uses." 15 U.S.C. §§ 1681 et seq.

9. In the Commission's first Internet privacy case, GeoCities, operator of one of the most popular sites on the World Wide Web, agreed to settle Commission charges that it had misrepresented the purposes for which it was collecting personal identifying information from children and adults through its online membership application form and registration forms for children's activities. *GeoCities*, Docket No. C-3849 (Feb. 12, 1999) (consent order).

In its second Internet privacy case, the Commission alleged, among other things, that Liberty Financial Companies, Inc., operator of the Young Investor Web site, falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously. As alleged, this information was maintained in identifiable form. *Liberty Financial Cos., Inc.*, Docket No. C-3891 (Aug. 12, 1999) (consent order).

In its most recent Internet privacy case, Online auction house ReverseAuction.com, Inc. agreed to settle Commission charges that it violated consumers' privacy by harvesting consumers' personal information from a competitor's site, eBay, and then sending deceptive spam to those consumers soliciting their business. *FTC v. ReverseAuction.com*, Inc., Civil Action No. 000032 (D.C.D.C., Jan 6, 2000) (stipulated consent order).

10. 15 U.S.C. §§ 6501 et seq.

11. 64 FR 59888 (Nov. 3, 1999).

12. 64 FR at 60055.

13. There is important precedent for this approach. In 1977, the federal Privacy Protection Study Commission recommended that, with enumerated exceptions, "no medical care provider should disclose, or be required to disclose, in individually identifiable form, any information about any such individual without the individual's explicit authorization." *Personal Privacy in an Information Society*, The Report of The Privacy Protection Study Commission, July 1977 at 306.

An instructive discussion of the "opt-in" versus "opt-out" choice to privacy protection is provided by the National Telecommunications and Information Administration ("NTIA") in its report on privacy issues. U.S. Dept. of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995). NTIA concluded that, on balance, the determining factor in the choice between the two approaches to gaining consumer consent for use of personal information should be the nature of that information, and that ancillary use of "sensitive" information should require express prior consent ("opt-in"), while non-sensitive information could be used if the affected consumer fails, after notice, to take some affirmative action to restrict that use ("opt-out"). *Id.* at 25. In making the distinction between "sensitive" and "non-sensitive" information, the NTIA further concluded that information relating to health care (*e.g.*, medical diagnoses and treatments) should be considered "sensitive." *Id.*

14. 15 U.S.C. 6502(b)(1). The requirements provide certain limited exceptions to this general rule for the collection of "online contact information," such as an e-mail address. Id.

15. Testimony of Alan F. Westin, Editor & Publisher, *Privacy & American Business*, on "Sensitive Data: Medical and Financial Information Online," *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, Federal Trade Commission, June 4, 1996 at 143.

16. HARRIS-EQUIFAX, HEALTH INFORMATION PRIVACY STUDY 2, 33 (1993).

17. Alan F. Westin, *Interpretive Essay*, in HEALTH INFORMATION PRIVACY STUDY, *supra* note 17, at 22.

18. *Ethics Survey of Consumer Attitudes About Health Web Sites*, California Health Care Foundation, at 3 (Jan. 2000).

19. HEALTH INFORMATION PRIVACY STUDY, *supra* note 17, at 97-103.

20. Disclosure of health information for these patients can take place only under certain specified conditions, one of which is the prior written consent of the patient; the other three are: (1) to medical personnel to the extent necessary to meet a medical emergency; (2) to qualified personnel to conduct scientific research, audits, or program evaluations; and (3) if authorized by court order. Public Health Service Act, 42 U.S.C. § 290dd-2.

21. Fair Credit Reporting Act § 604(g), 15 U.S.C. § 1681(b).

22. 64 FR at 59952.

23. HHS may wish to remain flexible regarding the requirement that individual authorization be "written." New technology options, such as using digital signatures to verify identity, may become widely available in the near future that would be less costly to implement.

24. *Id.* at 60056.

25. *Id.* at 60059.

26. *Id.*

27. *Id.*

28. *Id.* at 60049.

29. *Id.* at 60065.