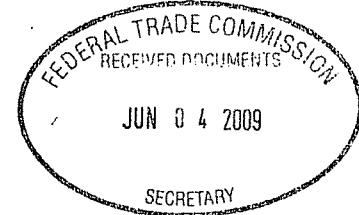


1500 K Street NW • Suite 1100 • Washington DC 20005 USA
Telephone 202 230 5142 • Facsimile 202 842 8465 • Website www.pharmacprivacy.org

June 2, 2009

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex M)
600 Pennsylvania Avenue, NW
Washington, DC 20580



Re: Health Breach Notification Rulemaking, Project No. R911002¹

Dear Mr. Clark:

The International Pharmaceutical Privacy Consortium (IPPC) is an organization formed in 2002 and comprised of chief privacy officers and other data privacy and security professionals from 15 research-based, global pharmaceutical companies. The IPPC is committed to the promotion of sound policies for the protection of patient privacy and advancement of drug development and treatment.² The purpose of these comments is primarily to request further clarification of certain terms used in the Proposed Rule.

I. Definition of "PHR identifiable health information"

Section 318.2(e) of the Proposed Rule defines "PHR identifiable health information" as "individually identifiable health information, as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and with respect to an individual, information (1) that is provided by or on behalf of the individual; and (2) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." The Proposed Rule states that this definition is "substantively identical" to section 13407(f)(2) of the American Recovery and Reinvestment Act of 2009.³ In fact, however, paragraph (e), as proposed, omits the word "includes," as used in the following quotation from the Act: "individually identifiable health information, as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and includes, with respect to an individual, information . . ." The use of the word "includes" is important because it clarifies that the second part of the sentence relates back to "individually identifiable health information" and should not be read as a separate, independent item. Indeed, were the second half of the sentence to be read as an independent item, there would be no connection between the information that is described in that part of the sentence (i.e., information that is provided by or on behalf of the individual and which can be used to identify the individual) and the *health* of the individual.

Section 318.2(e) also references the definition of "individually identifiable health information" under the Social Security Act (as amended by HIPAA), but it does not recite that definition. Section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)) defines "individually identifiable health information" as information that "(1) is created or received by a health care provider, health plan, employer, or health

¹ 74 Fed. Reg. 17,914 (April 20, 2009).

² For further information concerning the IPPC, please see our website at www.pharmacprivacy.org.

³ Id. at 17,916.

Mr. Donald S. Clark, Secretary
Federal Trade Commission
June 2 2009
Page 2

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." It would facilitate understanding of the meaning of "PHR identifiable health information" if the definition of "individually identifiable health information" were included either in paragraph (e) or in a new paragraph. The inclusion of this definition clarifies, for example, that PHR identifiable health information is a subset of information received by a health care provider, health plan, employer, or health care clearinghouse.

II. Definition of "Personal Health Record"

The Proposed Rule defines a "personal health record" as an "electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." It would be helpful for the FTC to provide examples of what types of electronic records of health-related information do and do not constitute PHRs, particularly in light of the fact that the Act defines PHR identifiable health information as a subset of information received by a health care provider, health plan, employer, or health care clearinghouse. For example, please confirm that PHRs do not include web sites that merely allow individuals to enter contact information to receive information on diseases or products, to sign up for certain health tracker tools or other disease-related support programs, or to receive discounts on health care products if such information is not received by a health care provider, health plan, health care clearinghouse, or the individual's employer (as such term is defined at 26 U.S.C. § 3401(d)). Moreover, it would be helpful to receive confirmation that that the phrase "managed, shared, and controlled" is to be read as three necessary criteria to trigger the PHR definition and not as three independent and individually sufficient triggers.

III. Definition of "Breach of Security"

The Proposed Rule, like the Act itself, defines a "breach of security" as the acquisition of unsecured PHR identifiable health information of an individual in a personal health record without the authorization of the individual. It would be helpful if the FTC would clarify that a breach of security would not include uses and disclosures of health information similar to those for which an authorization or opportunity to agree or object would not be required, and which are allowable, under the HIPAA Privacy Rule at 45 C.F.R. § 164.512. For example, disclosure of PHR identifiable health information without the individual's authorization for purposes of judicial and administrative proceedings or public health activities should not constitute a "breach."⁴

We thank you for your consideration of our comments. Please do not hesitate to contact us with any questions.

Sincerely,

2

Peter Blenkinsop
Secretariat and Legal Counsel

⁴ cf. 45 C.F.R. § 164.512(b) and (e).