



October 23, 2009

RIN 0991-AB56
HITECH Breach Notification for
Unsecured Protected Health Information Rulemaking

Georgina Verdugo
Director
Office for Civil Rights
United States Department of Health and Human Services

Dear Ms. Verdugo:

The Consumer Partnership for e-Health (CPeH) is a coalition of consumer, patient and labor organizations working to achieve a patient-centered health care system, enabled by health information technology that facilitates shared knowledge and informed decisions. We believe that the successful adoption and use of health information technology will only occur if there is a solid foundation of privacy and security protections that help consumers trust that their personal information will not be inappropriately shared or used.

We submit the following comments in response to the interim final rule (IFR) instituting requirements for the notification of breaches of unsecured protected health information and the request for comments issued by the Department of Health and Human Services (HHS) under the HITECH provisions in the American Recovery and Reinvestment Act of 2009 (ARRA).¹

We propose the following changes to the IFR:

- Replace the "harm standard" with an acquisition-based risk assessment;
- Remove the safe harbor status of LDS Lite data and instead subject potential breaches to acquisition-based risk assessments;
- Limit notification exceptions for internal breaches.

I. The Individual Harm Standard

The HHS IFR greatly undermines the protections afforded to consumers and their protected health information in ARRA by instituting a caveat that a breach of this information *only* occurs if the access, use or disclosure poses a "significant risk of financial, reputational, or other harm to individual."² This "harm standard" weakens the original intent of ARRA, which refers to compromising the privacy or security of the *data*, and in so doing also protects the finances, reputation and other things of importance to the patient. Applying the harm standard as well as the term "significant risk," requires a much more subjective determination of whether a breach occurred. Despite the inherent bias, the HHS IFR grants the covered entity that permitted the unauthorized acquisition, access, use, or disclosure of sensitive medical data the authority to make this determination through an internal process.

¹ HHS, Breach Notification for Unsecured Protected Health Information; Interim Final Rule, Federal Register, Vol. 74, No. 163, pp. 42740 – 42770, August 24, 2009 (HHS IFR).

² IFR Pg. 20.

Congress correctly rejected a “harm standard” when drafting the breach notification provisions in ARRA, recognizing that such a standard would both undermine incentives for health care organizations to protect data and also prevent patients from being able to know what is happening to their data.³ Patient access to information about the privacy of their health information and the quality of a health care entity’s privacy protections is critical to both ensuring that consumers trust that their information is secure and not being inappropriately disclosed, and empowering them to hold their health care providers accountable when privacy standards are too lax. While ensuring that unnecessary notifications do not undermine the effectiveness of notifications about potentially harmful breaches is important, HHS should not assume that the American people will automatically feel overwhelmed by these notifications.

A better approach to ensuring that consumers are not bombarded with notifications for truly harmless breaches is the use of an acquisition-based risk assessment. In making this assessment, a covered entity should be permitted to consider only the following factors: to whom the information was impermissibly disclosed; whether the information was actually accessed or viewed; the potential ability of the recipient to identify the subjects of the data; and, in cases where the recipient is the disclosing covered entity’s business associate or is another covered entity, whether the recipient took appropriate mitigating action. It is also easier to administer and enforce than the harm standard, and would be more consistent with standards used in the FTC’s breach notification rule for PHRs.⁴

We urge you to remove the “harm standard” from the regulations and replace it with an acquisition-based risk assessment which will preserve the important incentives for data protection, transparency, and consumer education, while avoiding unnecessary notifications. Retaining the “harm standard” will severely undermine the potential to increase consumer trust provided by the ARRA breach notification provision.

II. “Limited Data Set Lite”

The Consumer Partnership for e-Health supports granting safe harbor to information that is rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology with strong encryption and destruction standards. This will provide a strong incentive for covered entities to use state-of-the-art data protections.⁵

However, we do not support the HHS IFR extension of safe harbor status to any unauthorized acquisition, access, use, or disclosure of a subset of the limited data set from which dates of birth and zip code have been removed (“LDS Lite”).⁶ This safe harbor applies regardless of the potential risk of misuse of the data. Covered entities will not have to conduct a risk analysis to evaluate the potential ability of the person or entity inappropriately receiving data to re-identify it. We strongly disagree that any inappropriate use or disclosure of LDS Lite data would pose a low level of risk solely because specific identifiers have been removed. On the contrary, given the increasing prevalence of large databases of individually identifiable information, such as

³ Energy and Commerce, and Ways and Means Leaders Urge HHS to Revisit Breach Notification Provisions, October 1, 2009. http://energycommerce.house.gov/Press_111/20091001/sebelius_letter.pdf

⁴ FTC, Health Breach Notification Final Rule, Federal Register, Vol. 74, No.163, pp. 42966.

⁵ IFR Pg. 12.

⁶ IFR Pg. 26.

those controlled by employers or health insurers, and rapidly evolving technologies, there is a growing risk that information in the LDS Lite category may be re-identified.

A limited data set is still protected health information and should be treated as such. Potential breaches of LDS Lite data should not be given safe harbor and instead should be subject to acquisition-based risk assessments, with consideration given to the likelihood the data could be re-identified.

III. Internal Breaches

The HHS IFR further undermines consumer protections by permitting workforce members of a covered entity to use with impunity any protected health information they accidentally or inadvertently access in any manner permitted under the Privacy Rule.⁷ This allows a wide variety of uses and disclosures that may not have been anticipated by the patient and of which they would have no knowledge.

We recommend that HHS remove the exception that allows uses of personal health information that are permitted under the Privacy Rule when information is accessed accidentally or inadvertently. At a minimum, HHS should limit the breach notification exception to inadvertent disclosures when steps have been taken to mitigate the improper access or receipt of information.

Consumer and patient protections must not be sacrificed for the sake of convenience to covered entities or a concern that patients will be overwhelmed by breach information. A patient-centered health care system supported by health information technology will only be realized if consumers and patients have confidence that their personal health information is being protected.

Thank you for the opportunity to comment.

Sincerely,

Members of the Consumer Partnership for eHealth

The National Partnership for Women & Families
AARP
Center for Democracy and Technology
Center for Medical Consumers
Childbirth Connection
Consumers Union
Family Violence Prevention Fund
Mental Health America
National Consumers League
National Health Law Program
SEIU

⁷ IFR Pg. 29.