COALITION FOR PATIENT PRIVACY

October 23, 2009

Georgina Verdugo, Director
Office for Civil Rights
U. S. Department of Health and Human Services
Attention: HITECH Breach Notification
Hubert H. Humphrey Building, Room 509F
200 Independent Avenue, SW
Washington, DC 20201

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

Dear Ms. Verdugo:

The Coalition for Patient Privacy is the leading voice of consumer organizations for privacy and health IT. We are a diverse, multi-partisan group united by our efforts to prevent discrimination in employment and other key opportunities based on health information. We work to positively impact how electronic medical records are used and to ensure privacy is protected. Patients will only trust the healthcare system if privacy is assured.

We appreciate this opportunity to provide public comment on the interim final rule (IFR) establishing requirements for notification of breaches of unsecured protected health under the American Recovery and Reinvestment Act of 2009 (ARRA).[1] We look forward to working with you in your new role as Director to protect patients and consumers.

In short, we were dismayed and disappointed with the IFR, particularly with the inclusion of a "harm standard", and the exception provided for "Limited Data Sets (LDS) Lite." The broad discretion granted to industry goes far beyond Congressional intent. Moreover, from the consumer vantage point, the IFR is entirely inconsistent with the Obama Administration's public pledges to ensure transparency and accountability. There was no mention of any consideration of a harm standard in HHS previous Request for Information, thwarting any opportunity for public debate. We expect more than rhetoric; we expect consumers to be protected.

While we appreciate the desire to establish reasonable, workable regulations, patients' most sensitive information on earth, their health information, must be treated with the utmost caution and concern. When privacy is violated the patient must be informed.

[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).

The burden to the data holder to provide meaningful and timely notice cannot trump this important protection for consumers. Currently the IFR places industry priorities before patients'; the public finds this totally unacceptable.

We request the following action:
1) **Delete 45 C.F.R. 164.402(1)(i).** We strongly support the urging of the Chairmen of the House Energy & Commerce and House Ways & Means Committees to "revise or repeal the harm standard provision included" in the IFR, as requested in their October 1, 2009 letter to HHS Secretary Sebelius.[2] This exclusion weakens the breach notification requirement dramatically, granting the company that would like to avoid the cost and consequences of breach notification the power to decide if they will notify.

2) **Delete 45 C.F.R § 164.402(1)(ii)**. There remains a potential re-identification risk of limited data sets even when dates of birth and zip codes have been removed. We urge you to determine that this information should not, as a practical matter, be given safe harbor status.

3) **Delete or revise 45 C.F.R 164.402(2)(i).** If an employee of a covered entity or business associate accesses PHI unintentionally, they should NOT be allowed to use that information, even if it is allowed under the Privacy Rule.

Harm Standard

The individual harm standard is unsupported by ARRA, contradicts Congressional intent and is prone to abuse. The harm standard also reduces transparency and weakens the incentive for covered entities to encrypt information.

With respect to covered entities, the ARRA defines "breach" as the "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information."[3] In its interim final rule, HHS has interpreted "compromises" to imply a harm standard. Under HHS' interpretation, breach does not occur – and notification is not required -- unless the access, use or disclosure poses "a significant risk of financial, reputational, or other harm to individual."[4] The "significant risk of harm" determination is an internal process on the part of companies with a powerful financial and reputational bias against notification.

Further, HHS' interpretation of "breach" notably violates the ARRA's statutory language; the writing simply does not imply an individual harm standard. The statutory language refers to compromising the privacy or security of *data*, not the finances or reputation of the patient. **Congress did not intend to permit covered entities to make a value**

[2] Pg. 2. http://energycommerce.house.gov/Press_111/20091001/sebelius_letter.pdf
[3] ARRA § 13400(1)(A)
[4] IFR Pg. 20.

judgment on behalf of individual patients with regard to whether breached health information is sensitive or not. In the October 1 letter to HHS Secretary Sebelius, the Chairmen of the House Energy & Commerce and House Ways & Means Committees explicitly confirmed that the harm standard is not supported by the statutory language and contradicts Congressional intent. The letter articulated that Committee members *"specifically considered and rejected such a standard due to concerns over the breadth of discretion that would be given to breaching entities, particularly with regard to determining something as subjective as harm from the release of sensitive and personal health information."*

Additionally, the harm standard, as drafted in the IFR, undermines a second major purpose of mandatory notification: transparency. Patients should be made aware of when the institutions to which they've entrusted their data have not protected the privacy and security of that data, even when the risk of harm to the patient is not high. This educates consumers and empowers them to hold their health care providers accountable if privacy standards are too lax. As the letter from the Chairmen of the Committees to Secretary Sebelius states: *"Such transparency allows the consumer to judge the quality of a health care entity's privacy protection based on how many breaches occur, enabling them to choose entities with better privacy practices."* Instead, the harm standard keeps patients in the dark about what is happening to their data.

HHS' harm standard empowers breaching entities with precisely the subjectivity Congress intended to avoid. The IFR suggests that covered entities should consider the nature of the protected health information in making a risk assessment. One example provided was disclosure that a named patient received services at a certain hospital. In this example, the covered entity is not in a position to be able to adequately assess whether such information would harm an individual. Disclosure of such information could cause harm – loss of promotion or reputational harm, for example. However, many data holders could simply decide that these are not "significant risks of harm" unless they receive a complaint. This does not serve the patient.

Alternatively, we do find the Federal Trade Commission's (FTC) consideration of assessing whether or not any <u>data</u> (regardless of type) was acquired or accessed far more appropriate and in line with Congressional intent. If you can prove neither occurred, such as forensic evidence that a lost laptop was never opened, no notification is necessary. Congress did not intend to permit covered entities to make a value judgment on behalf of individual patients with regard to whether breached health information is sensitive or not. We also agree with the FTC's breach notification assessment that "the danger of over-notification may be overstated." The harm standard added to the IFR is overreaching and must be removed.

<u>Limited Data Sets</u>

We oppose HHS's granting safe harbor status to a subset of the limited data set (i.e., a limited data set from which dates of birth and zip code have been removed "LDS Lite") by deeming the inappropriate use or disclosure of such information is not a breach.

A limited data set is protected health information which has been partially de-identified by removing most identifiers including the name, address, social security number, and account number of an individual or the individual's relative, employer, or household member. Unlike information which has been de-identified in compliance with HIPAA, a limited data set may include dates (e.g., dates of birth, admission dates, and dates of service) as well as town or city, State, and zip code. Additionally, LDS include places of service, admission and discharge dates, all of which facilitate re-identification.

When "LDS Lite" information is inappropriately used or disclosed, covered entities are never required to notify individuals of such disclosure regardless of the recipient of the information. Neither are covered entities required to conduct a risk analysis to evaluate the recipient's potential ability to re-identify the information. HHS justified this approach based on its belief that the inappropriate use and disclosure of "LDS Lite" if subjected to a risk assessment would pose a low level of risk.

We strongly urge you to review Dr. Paul Ohm's recent publication, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, as you consider "de-identified data." Ohm explains with precision why "data can either be useful or perfectly anonymous but never both"[5]. The critical piece is whether or not "de-identified" data can be re-identified once it is combined with another dataset.

One of the few studies conducted on the HIPAA de-identification standard demonstrated that the risk of re-identification of data is significant. The study found that employers, physicians, pharmacies, employers and insurers could identify members by applying diagnosis and medication combinations to a de-identified data set with a moderately high expectation of accuracy. It is quite clear that the risk of re-identification of data in an "LDS Lite" format depends largely on the recipients of the data, their access to other information, capabilities and motivation.

Given rapidly evolving technologies and the increasing proliferation of databases, it is not appropriate to deem information not at risk solely because specific identifiers have been removed. While it may be true that removing zip codes and dates of birth may make it less likely that a limited data set will be re-identified, the level of risk of re-identification also depends on the recipient's motivation to re-identify the data. Impermissibly releasing information to recipients who have access to other mega databases of individually identifiable information and are motivated to re-identify

[5] "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" by Paul Ohm, JD, University of Colorado Law School, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

information heightens the risk that the information in the "LDS Lite" may be combined with other data and re-identified.[6] Examples of mega database holders include employers and insurers.

In sum, information in "LDS Lite" does not consistently meet the standard of being unusable, unreadable or indecipherable. It does not qualify as a "secure" technology entitled to safe harbor status under section 13402(h) of ARRA. Creating another avenue through which it is possible to grant this information safe harbor status is unwarranted and contrary to Congressional intent. We recommend that the HHS standard for de-identification should be that all data must be provably de-identified. Experts like Dr. LaTanya Sweeney have demonstrated methods to provably de-identify health data, so that data is still protected and reliable.

Internal Breaches

ARRA excludes from the definition of breach certain cases of unintentional internal acquisition of protected health information, provided such information is not "further acquired, accessed, used, or disclosed without authorization."[7] Unfortunately, the HHS IFR contradicts this statutory framing by allowing the person or entity that inadvertently or accidentally receives the information to further use it in any way permitted under the Privacy Rule.[8] In other words, if the individual in good faith accidentally accesses data they were not authorized to access, it is not a breach if they subsequently use that data in a manner that is permitted by the Privacy Rule.

If an employee of a covered entity or business associate accesses PHI unintentionally, they should NOT be allowed to use that information, even if the use or disclosure is allowed under the Privacy Rule. The Privacy Rule is far too broad, allowing use and disclosure of PHI without consent for "treatment, payment and healthcare operations." Such discretion is out of step with patients' expectations about how their information can be used. It is a wholly insufficient safeguard against inappropriate use and should not be an exception to breach notification.

Timing of Notice to Secretary

The IFR's 60-day deadline for reporting breaches to the Secretary is contrary to the "immediate" notice required by the ARRA. Section 13402(d) of the ARRA requires a covered entity to furnish required breach notification to affected individuals without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered. In contrast, Section 13402(e)(3) of the ARRA requires covered entities to notify the Secretary "immediately" of breaches of unsecured protected health

---

[6] See Steven Clause, et al. "Conforming to HIPAA Regulations and Compilation of Research Data," 61 *American Journal of Health System Pharmacy* 1025-1031 (2004).

[7] ARRA, § 13400(1)(B).

[8] HHS IFR Pg. 29.

information involving 500 or more individuals. Even though this latter provision clearly establishes a different deadline for notifying the Secretary vis a vis notifying an affected individual, HHS has interpreted it as having the same meaning -- that covered entities are required to provide notice to the Secretary concurrent with providing notice to the individual. This interpretation is contrary to generally accepted rules of statutory construction that the use of different phrases in a statute have different meanings. Providing notice to the Secretary in advance would enable HHS to provide technical assistance in crafting and furnishing breach notification.

Additional Transparency Enhancements

We repeat our initial recommendations for improved transparency submitted in May, 2009 in response to the Request for Information. It is very troubling that HHS appears to be so highly influenced by industry, especially when it fails to invite public comment on significant new additions and changes not present in the statue such as a harm standard.

- We request that HHS release the log of meetings, attendees at each meeting, and names of the external experts in health informatics and security that it consulted with to develop this guidance and publish all materials and documents provided by these consultants.
- All experts consulted should be required to disclose all conflicts of interest in writing.
- Cite resources and recommendations within regulations, a practice the FTC implements.

Conclusion

Ensuring ironclad protections against theft and misuses of PHI must be the price of doing business in health care. If an entity cannot or will not protect our most sensitive data, they should not be in the health care business. We currently have higher standards and expectations for our financial data than we do for our health data. With a breach of financial records, a consumer faces a significant headache, but ultimately can have their credit and funds restored; this is not the case with health records. A stigmatizing diagnosis, condition or prescription in the wrong hands can cause irreversible damage and discrimination. There is no perfect delete or recover button for restoring the privacy of health information that has been used or disclosed via a breach.

The burden to the data holder to report breaches cannot trump this important protection for consumers. The Coalition urges HHS to revise the current IFR now so that it is aligned with the intent of our elected officials and the paramount principles of transparency and accountability. Do not wait until April 2010. Thank you for this opportunity to provide feedback. We look forward to working with you.

Sincerely,

The Coalition for Patient Privacy

AIDS Action
American Association of People with Disabilities
American Civil Liberties Union
American Council of the Blind
Clinical Social Work Association
Consumer Action
JustHealth
The Multiracial Activist
The National Coalition of Mental Health Professionals and Consumers
Patient Privacy Rights
Private Citizen, Inc.
Telecommunications for the Deaf & Hard of Hearing, Inc.
U.S. Bill of Rights Foundation

cc. Secretary Kathleen Sebelius

Senator Olympia Snowe

Representatives:
Henry A. Waxman
Charles B. Rangel
John D. Dingell
Frank Pallone, Jr.
Pete Fortney Stark
Joe Barton