October 23, 2009

Submitted electronically via http://www.regulations.gov

U.S. Department of Health and Human Service
Office for Civil Rights
Attention: HITECH Breach Notification
Hubert H. Humphrey Building, Room 509 F
200 Independence Avenue, S.W.
Washington, DC 20201

RE: Comments - Interim Final Rule on Breach Notification for Unsecured Protected Health Information

Dear Sir/Madam:

The American Benefits Council (the "Council") appreciates the opportunity to comment on the Department of Health and Human Services' ("HHS") Interim Final Rule on Breach Notification for Unsecured Protected Health Information ("PHI"). 74 Fed. Reg. 42740 (Aug. 24, 2009). The Interim Final Rule was issued under the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), passed as part of the American Recovery and Reinvestment Act of 2009. The HITECH Act added new privacy and security obligations for covered entities subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

The Council is a public policy organization representing principally Fortune 500 companies and other organizations that assist employers of all sizes in providing benefits to employees. Collectively, the Council's members either sponsor directly, or provide services to, retirement and health plans that cover more than 100 million Americans.

The Council requests consideration of the following comments:

Retain the "Harm Threshold" Framework Adopted in the Interim Rule

The Council strongly supports the "harm threshold" HHS adopted in its Interim Final Rule, requiring a covered entity to consider a number of factors to determine whether a

particular disclosure poses a "significant risk of financial, reputational, or other harm to the individual." 45 CFR 164.402 (definition of "breach"). If a disclosure meets the "harm threshold," the covered entity is required to provide notice to the affected individuals, the media (where applicable) and HHS.

The Harm Threshold Is Required by HITECH Act

The HITECH Act defines a "breach" as an unauthorized acquisition, access, use, or disclosure of PHI "which compromises the security or privacy of such information." HITECH Act § 13400(1) (emphasis added). The statute, as written, does not appear to require notification every time PHI is possibly mislaid or accessed. Rather, the statute only intends a notification to be sent when data actually is compromised and poses harm to the affected individual. Otherwise, individuals would receive notifications for even benign disclosures of data.

In its Interim Final Rule, HHS acknowledged this statutory requirement and adopted what it referred to as the "harm threshold." The Council strongly supports the harm threshold and believes this type of standard is not only contemplated (if not required) by the statutory language, but also offers a workable solution for covered entities to evaluate whether a disclosure should trigger a breach notification, without compromising an individual's need to understand how their information may have been disclosed in a situation where there is risk.

Harm Threshold Aligns with State Laws and Obligations of Federal Agencies

As HHS points out in the Preamble to the Interim Final Rule, a harm threshold ensures better consistency and alignment with State breach notification laws as well as existing obligations on Federal agencies. *See* 74 Fed. Reg. 42740, 42744.

These state laws provide that a notification is not required if the covered entity determines there is no significant risk that the information could be misused or could harm affected individuals.[1] While these state laws recognize the importance of notifying individuals of a breach where there is real potential for misuse or harm, they are intended to prevent multiple notices for every possible misuse of information that may not result in risk, which not only could inundate individuals with unnecessary notices but de-sensitize them to notices where there is a real threat to their information. Having a different standard between federal and state law also could cause confusion and compliance burdens for covered entities.

[1] For example, California requires a breach notification where medical information has been acquired by an unauthorized person in a manner that "compromises the security, confidentiality, or integrity of personal information." Cal. Civ. Code § 1798.82(d). *See also* Conn. Gen. Stat. § 36a-701b (breach notification not required if "not likely to result in harm to the individuals whose personal information has been acquired or accessed").

Harm Threshold Is Consistent with Federal Breach Notification Requirements

Similarly, the federal government has adopted a harm threshold for breach notifications by federal agencies. *See* Office of Management and Budget Memorandum M-07-16 (May 22, 2007) ("OMB Memorandum"). HHS cites the OMB Memorandum in the Interim Final Rule as a source of examples that covered entities may want to review for the types of factors that may need to be taken into account in determining whether an use or disclosure presents a significant harm to the individual. 74 Fed. Reg. 42740, 42744.

The OMB Memorandum requires that agencies assess the "likely risk of harm caused by the breach and then assess the levels of risk" in deciding whether a notification is required, citing a similar standard adopted under the federal Privacy Act. 5 U.S.C. § 525a(e)(10) (requiring agencies to protect against threats to security which "could result in substantial harm, embarrassment, inconvenience, or unfairness"). The OMB Memorandum states that the reason it adopted a harm threshold was that a number of experts raised concerns about unnecessary notifications and the "chilling effect" these may have on the public, "along with the costs to individuals and businesses in responding to notices where the risk of harm may be low." OMB cautioned, "Agencies should exercise care to evaluate the benefit of notifying the public of low impact incidents."

Continue to Work Within the "Harm Threshold" of the Interim Final Rule

The Council recommends that the harm threshold framework articulated in the Interim Final Regulations be retained in any final regulations. The harm threshold standard ensures that covered entities have a workable framework for compliance, while protecting individuals and their right to understand how their information may have been disclosed where there is a risk of harm. The harm threshold also ensures that the impact of notices when there <u>is</u> real risk of harm is not diminished by a flood of constant notices when there is no real threat.

The Preamble to the Interim Final Regulations provides an extensive list of the specific factors for covered entities to consider in performing risk assessments to determine if there is a significant risk of harm to an individual as a result of the use of disclosure. 74 Fed. Reg. 42740, 42744 -42745. In adopting the harm threshold, the Interim Final Rule further protects individuals by specifying that the burden is on the covered entity to demonstrate that a disclosure does not pose significant harm to trigger the breach notification. Covered entities are also required to document their risk assessments so that they can demonstrate, if necessary, that no breach notification was required following a use or disclosure of protected health information.

To the extent there are any concerns regarding the adequacy of a harm threshold standard of ensuring appropriate breach notification, we believe such concerns can be best addressed by working within this framework. This could include identification by HHS of additional factors or examples that covered entities could consider or take into account in applying the harm threshold standard.

* * *

The Council appreciates the opportunity to comment on the Interim Final Rules. Please do not hesitate to contact us at 202-621-1975 with any questions or if we can be of further assistance.

Sincerely,

Kathryn Wilber
Senior Counsel, Health Policy