May 21, 2009

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

RE: Guidance and Request for Information – HITECH Breach Notification

Dear Sir/Madam:

The American Benefits Council (the Council) appreciates the opportunity to comment on the Department of Health and Human Services' (HHS) Guidance and Request for Information ("Guidance") specifying the technologies and methodologies that render protected health information (PHI) unusable, unreadable or indecipherable to unauthorized individuals and thus "secure" PHI, not subject to the breach notification requirements imposed by the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA). 74 Fed. Reg. 19006 (April 27, 2009). The HITECH Act added new privacy and security obligations for covered entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPPA).

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 comments below specifically address the Guidance on technologies and methodologies that render PHI "secure", as well as the breach notification requirements more generally.

Methodologies to Create Secure PHI

Specific Encryption Standard Should be Example, Not Only Method to Create Secure PHI

HHS adopted a specific standard for encryption, NIST Special Publication 800-111, and stated that this would be the only permitted standard for creating secure PHI (other than complete destruction of the information). The NIST Special Publication 800-111 acknowledges, however, that there are viable alternatives to encryption. HHS should consider what other protective measures can be taken to create secure PHI, other than encryption.

The HIPAA Security Standards do not require encryption and, in fact, expressly provide that covered entities have the flexibility to determine what security standards best apply to the covered entity's particular situation. Under the HIPAA Security Standards, encryption is an "addressable" standard, which means that a covered entity must assess whether encryption is "reasonable and appropriate." 45 CFR § 164.306(d). If not, the covered entity must implement an "equivalent alternative measure." The HIPAA Security Standards set out factors the covered entity must consider when determining if encryption (and other addressable standards) are "reasonable and appropriate":

> *(b) Flexibility of approach. . . .* (2) In deciding which security measures to use, a covered entity must take into account the following factors:
>
> (i) The size, complexity, and capabilities of the covered entity.
>
> (ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
>
> (iii) The costs of security measures.
>
> (iv) The probability and criticality of potential risks to electronic protected health information.

45 CFR § 164.306(b).

In compliance with the HIPAA Security Standards, covered entities have undergone rigorous risk assessments to determine what types of security measures to implement, including whether to establish encryption procedures or "equivalent alternatives." The Guidance should recognize that HHS' own security rules allow alternatives to encryption and provide other methodologies that would be considered to create "secure" PHI.

In addition, we recommend that the Guidance recognize that there will be emerging technologies in this area that could enable covered entities an even greater ability to safeguard PHI. The ability to utilize these emerging technologies should be accounted for in future HHS Guidance. To do otherwise, could create a disincentive for covered entities to proactively assess and upgrade their security measures.

HHS Should Adopt Secure Standard for PHI in Other Forms

The HHS Guidance only addresses PHI that is encrypted or has been completely destroyed. In reality, covered entities routinely use and disclose PHI in a number of formats that could not practically meet either of these standards, but for which there are alternative protections. For example, in order to operate day-to-day, covered entities would need to transfer and review paper files, print out emails, review documents on screen, fax information, and discuss information orally with colleagues, plan participants, and health care providers. The HHS Guidance does not recognize that the routine operations of a covered entity utilize a format that could not practically satisfy the new proposed standards because the information is actually in use. In fact, ERISA's regulations require health plans to be able to use information in these formats in order to respond to questions and claims for benefits. For example, ERISA's claims procedure regulations require a health plan to respond orally to certain urgent care claims.

Covered entities currently are required by the HIPAA privacy and security regulations to have safeguards in place to protect this information. HHS should recognize that there is body of information not able to be encrypted or destroyed and provide a means of allowing this information also to be considered "secure."

HHS Should Adopt a "Harm" Threshold in Determining When a Breach Notification is Required

The HITECH Act defines "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 does not intend to require a 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. We encourage HHS to codify this standard in its Guidance – that the acquisition, access, use, or disclosure must a significant risk or harm in order to trigger the breach notification requirement. Otherwise, individuals will receive notifications for even benign "breaches" of data.

Most state breach notification laws also contain a "harm" threshold where 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. While these state laws recognize the importance of notifying individuals of a breach were 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 any 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.

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"). HHS should adopt a similar "harm" threshold in order to be consistent with state law and avoid individuals receiving notifications in circumstances that do not warrant such measures.

Information in a Limited Data Set Should be Considered Secure

HHS asked how it should treat information included in a limited data set. Information in a limited data set should be considered "secure" PHI. This information already has been stripped of most identifiers, so there is low risk of improper access. In addition, because these identifiers have been stripped, it would be virtually impossible for a covered entity to notify affected individuals by mail or email. This would mean a covered entity always would be required to give substitute notice (i.e., media notice) if there is a breach of limited data set information, when the risk is extremely low that any identifiable information actually has been compromised. As such, we recommend that the Guidance provide that limited data set information is considered "secure" PHI.

Comments Related to Breach Notification Generally

HHS Should Clarify the Notice Obligation when Breach is by Business Associate to Avoid Duplicate Notices

The HITECH Act clearly requires a covered entity to provide a security breach notification when there is a breach by the covered entity. The HITECH Act also clearly requires a business associate to notify the covered entity if there is a breach by the business associate. What is not clear is whether the business associate has an independent obligation to notify an individual of a security breach by the business associate (since the HITECH Act also provides that the business associate is directly regulated under the HIPAA security rules "in the same manner" as the covered entity). Also not clear is what the covered entity's obligation is to notify individuals when the breach is by the business associate. HHS should clarify the business associate's role when the breach is by the business associate, and specifically, clarify whether the covered entity, business associate (or both – or neither) have the legal obligation to notify an individual.

If HHS decides that both the covered entity and business associate have an obligation to notify the individual of a breach by the business associate, HHS should adopt some type of "joint notice" rule, similar to the joint notice rule already in the HIPAA privacy regulations, where only one notification would be required. *See* 45 CFR § 164.520(d).

HHS Should Allow Flexibility for Electronic Notification

The HITECH Act provides that breach notification may be provided to individuals by electronic mail "if specified as a preference by the individual." HITECH Act § 13402(e)(1)(A). The proposed FTC regulations applicable to PHR vendors state that, in order to provide electronic notification, an individual must provide "express affirmative consent." FTC Proposed Rule, 16 CFR § 318.5(a)(1).

The statute does not explain how an individual should indicate a preference for email notification and does not require affirmative consent. We encourage HHS to adopt an opt out approach for individuals to receive email notification, rather than an affirmative consent requirement. The relationship many individuals have with covered entities (particularly employer health plans and related service providers) is online, so in many cases, electronic notification is the most practical and expeditious means of communication.

In addition, the HIPAA privacy rules allow electronic delivery of the HIPAA privacy notice as long as the covered entity can "infer" agreement; affirmative consent is not required. Rather, HHS said it did not require any particular form of agreement and allows covered entities "the flexibility to provide the notice in the form that best meets their needs." See 45 CFR § 164.520(c)(3); 65 Fed. Reg. 82724 (Dec. 28, 2000). Having a different standard for this particular notification would impose a significant administrative burden and expense on covered entities, who would have to create a specific additional procedure for this single notice. We recommend that HHS allow an opt out form of electronic notice, consistent with other notice requirements applicable to covered entities.

* * *

The Council appreciates the opportunity to comment on the Guidance and Request for Information. Please do not hesitate to contact us at 202-621-1975 or kwilber@abcstaff.org with any questions or if we can be of further assistance.

Sincerely,

Kathryn Wilber
Senior Counsel, Health Policy