Filed electronically at: secure.commentworks.com/ftc-healthbreachnotification

June 1, 2009

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex M)
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: Health Breach Notification Rulemaking, Project No. R911002

Dear Sir/Madam:

The American Benefits Council (the Council) appreciates the opportunity to comment on the Federal Trade Commission's (FTC's) Notice of Proposed Rulemaking and Request for Public Comment (Proposed Rules), which provide rules for personal health record (PHR) related entities with respect to the security breach notification requirements under the Health Information Technology for Economic and Clinical Health (HITECH) Act. 74 Fed. Reg. 17914 (Apr. 20, 2009).

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 HITECH Act was passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA) and added new privacy and security obligations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Act requires the FTC to issue interim final rules applicable to PHR related entities and the Department of Health and Human Services (HHS) to issue interim final rules applicable to HIPAA covered entities (i.e., health plans and health care providers implementing HITECH's security breach notification requirements.

The Council previously submitted comments on the Department of Health and Human Services' (HHS) Guidance and Request for Information 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 comments below specifically address the FTC's proposed rules for health breach notification.

1. Harmonization of FTC & HHS Rules Governing Security Breach Notification

The preamble to the proposed rules states that the FTC is consulting with HHS to "harmonize" its proposed rule with HHS' proposed rule. 74 Fed. Reg. 17915. Most of the Council's members are either covered entities or business associates under the HIPAA privacy and security rules. Many have relationships with PHR related entities as well. As such, the Council has a strong interest in the FTC's proposed rules given the FTC's intent to harmonize its rules with HHS and because of our members' relationships with PHR related entities.

The Council supports the harmonization of HHS and FTC rules as it would provide HIPAA covered entities and PHR related entities with a consistent set of rules within which to work. To this end, we encourage both agencies to consider the existing framework that applies to covered entities, such as state laws and the HIPAA privacy and security rules themselves, so that the security breach notification rules are not inconsistent with rules that currently apply to these entities.

The FTC specifically asked about the dual role of PHR related entities and whether these entities also may be covered entities or business associates. The FTC proposed regulations expressly carve out from the definition of "PHR related entity" an entity that is a HIPAA covered entity or to the extent it is acting as a business associate. FTC Proposed Rules, 16 CFR § 318.2(f). The Council recommends that the FTC and HHS adopt clear carve out rules, similar to this definition, clarifying which rule applies to, and which agency has enforcement authority over, an entity that may have a dual role.

2. The Council Supports the "Harm" Threshold in Determining When a Breach Notification is Required

The FTC proposed rules define "breach of security" as acquisition of unsecured PHR identifiable health information without the authorization of the individual. FTC Proposed Rules, 16 CFR § 318.2(a). The definition states that unauthorized acquisition will be presumed to include unauthorized access unless the PHR related entity has reliable evidence showing that there has not been, or could not have reasonably been, any unauthorized acquisition of such information.

The Preamble to the rules further notes that, while there may be unauthorized access, data may not have actually been acquired, "The term acquisition, however, suggests that the information is not only available to unauthorized persons, but in fact has been obtained by them." The Preamble states that the entity that experienced the breach is in the "best position" to determine whether unauthorized acquisition has taken place. 74 Fed. Reg. 17915.

The Council strongly supports this distinction between access and actual unauthorized acquisition of data, often referred to as a "harm" threshold. The HITECH Act defines "breach" under the rules for HIPAA covered entities and PHR related entities slightly differently, but both definitions contemplate there being some type of harm. The definition of "breach" applicable to PHR related entities requires "unauthorized acquisition" of data, and the definition of "breach" applicable to HIPAA covered entities requires a "compromise" of data.[1] We recommend that both the HHS and FTC rules adopt a "harm" threshold rule as a basis for the notification standard to create consistency in how the two agencies define and interpret when a "breach" has occurred that triggers notification.

In addition, most state breach notification laws 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 for federal and state law is likely to cause confusion and increase administrative burden and cost for covered entities. [2]

3. The FTC 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 FTC proposed rules state that, in order to

---

[1] As applicable to HIPAA covered entities, 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).

[2] 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").

provide electronic notification, an individual must provide "express affirmative consent." FTC Proposed Rules, 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 the FTC 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 and PHR related entities 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 does 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 increase administrative costs for covered entities and PHR related entities, who would have to create a specific additional procedure for this single notice. We recommend that the FTC and HHS allow an opt out form of electronic notice, consistent with other notice requirements applicable to covered entities and PHR related entities.

4. Covered Entities and PHR Related Entities Should Have Flexibility to Determine Manner and Sufficiency of Media Notice Based on Circumstances of Breach

The HITECH Act provides that if a breach involves more than 500 individuals, the covered entity or PHR related entity must provide notice to "prominent media outlets." HITECH Act § 13402(e)(2). The proposed FTC rules restate this rule, but add that the notice must include the same content requirements as the notice to individuals. FTC Proposed Rule 16 CFR § 318.5(b). In the Preamble to the proposed rules, the FTC provides an example where a press release should be sent to a "number of state or local print publications, network, and cable new shows, and radio stations." 74 Fed. Reg. 17919. The FTC specifically requested comment on the standards and criteria that should apply in determining the adequacy of such media notice.

The Council recommends that covered entities and PHR related entities be permitted flexibility to determine the information that should be provided and to which media outlets. Each breach situation, geographical region, and workforce and customer base involved will be different. As the FTC notes in the preamble to the regulations, the entity that experienced the breach is in the "best position" to determine whether there has been unauthorized access. Similarly, that entity

would be in the best position to determine which, and how many, media outlets should be informed and what information should be provided.

If entities are required to provide lengthy notices to multiple media outlets, it could result in a costly and cumbersome process which could, which would not only delay notice being sent, but also interfere with timely broadcast by the media. We recognize requirements for media notice are intended to quickly disseminate information about a possible breach, alerting individuals who may need to contact the breaching entity. We believe this purpose can be best accomplished if the covered entity is able to quickly gather the information necessary for the media notice and target the particular media that is appropriate in a given situation.

* * *

The Council appreciates the opportunity to comment on the Notice of Proposed Rulemaking and Request for Public Comment. 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