BlueCross BlueShield Association

An Association of Independent Blue Cross and Blue Shield Plans
1310 G Street, N.W.
Washington, D.C. 20005
202.626.4780
Fax 202.626.4833

June 1, 2009

Donald S. Clark
Secretary of the Commission
Office of the Secretary
Federal Trade Commission
Room H-135 (Annex M)
600 Pennsylvania Avenue, N.W.,
Washington, D.C. 20580

Attention: Health Breach Notification Rulemaking Project No. R911002

Dear Mr. Clark:

The Blue Cross Blue Shield Association ("BCBSA"), a national federation of 39 independent, community-based and locally operated Blue Cross and Blue Shield Plans ("Plans") that collectively provide healthcare coverage for more than 100 million (one in three) Americans, appreciates the opportunity to comment on the Notice of Proposed Rule Making (NPRM) regarding the "Health Breach Notification Rule" Under Section 13407 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009," published in the *Federal Register* on April 20, 2009.

BCBSA's comments focus on two areas:

1. BCBSA supports the Federal Trade Commission ("FTC") promulgating rules that require non-HIPAA covered entities (vendors of personal health records, PHR related entities, and third party service providers) to implement security safeguards, including consumer breach notification and data protection requirements. If these entities are not covered in regulations, then there is a strong probability of weakened consumer protections that will diminish consumer trust and negatively affect use of personal health records..

2. BCBSA recognizes that the FTC has incorporated the foundation of risk-based notification methodology by adding "unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, any unauthorized acquisition of such information" to HITECH's breach definition. However, the FTC should take a step further to incorporate a full risk-based methodology to determine if a breach notification is necessary.

Non-Covered Entity Breach Notification

Plans take the safeguarding of data as a very significant responsibility and support the federal government promulgating regulations that necessitate all non-HIPAA covered entities that use, access, and disclose identifiable health information ("IHI") to become compliant with privacy and security regulations. We concur with the FTC's interpretation of IHI to mean:

- Containing past, present and future health and payment information about a consumer; and

- Having an account with a vendor of personal health records or related entity, where the products or services offered by such vendor or related entity relate to particular health conditions.

If any non-covered entity stores, uses, maintains or has access to (even if only as a data repository for the consumer) IHI, then that organization should meet the definition and be responsible for meeting privacy and security requirements. This includes: 1) consumer notification if a breach occurs; and 2) implementing encryption or a similar technology that offers substantially similar safeguards.

Consumers expect their personal health information to remain private and safe. Any organization that is granted authorization by the consumer to store, access, or use his or her health information should be held accountable for keeping the data safe. We agree with the FTC's examples of entities who would qualify under the proposed rule, e.g., entities such as web-based applications that help consumers manage medications, websites that offer online personalized health checklists, companies that advertise dietary supplements online, etc.[1] These entities may not be a traditional covered entity or business associate, but are entities that should still be responsible for safeguarding certain data (e.g., encrypting or using other proven means while data are in transit or at rest) and notifying consumers if they fail to do so.

Following two years of hearings, the National Committee on Vital and Health Statistics ("NCVHS") recommended that, at a minimum, all companies that offer PHRs be treated as covered entities under HIPAA.[2]

BCBSA agrees with the NCVHS that all organizations – not just covered entities – that handle IHI should be subject to the same consumer protection rules. Otherwise, consumers could turn over their personal medical information to these entities, not understanding that they do not offer the same privacy and security protections as others. If the data are breached, and nothing has to be done about it, it could result over time in consumer distrust against the entire industry and a regression in the use of personal health records and other beneficial health information technology in this country.

Therefore, it is vital that the FTC issue a final rule that requires non-HIPAA covered entities to implement privacy and security processes for breach notification and data safeguarding. It is the most appropriate way to protect the consumer.

---

[1] Deloitte's *Washington Bulletin* (May 4, 2009) "FTC Proposes Health Breach Notification Rule"
[2] National Committee on Vital Health Statistics. (Dec. 21, 2007) *"Enhanced Protections for Uses of Health Data: A Stewardship Framework for 'Secondary Uses' of Electronically Collected and Transmitted Health Data."*

Risk-Based Notification

In contrast with the HITECH definition of breach for covered entities – "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information" – for non-covered entities the term breach simply means "*acquisition* [emphasis added] of unsecured IHI on an individual in a PHR without the authorization of the individual." Thus, the FTC points out, that there may be unauthorized access as well, but further investigation is necessary to determine whether the data also has been acquired. Unauthorized persons may have access to protected information if it is available to them. The term acquisition, however, suggests that the information is not only available to unauthorized persons, but has actually been obtained by them.

The FTC examples equate "obtain" with some degree of harm. For instance, unauthorized acquisition occurs when an employee views records to find information about a particular public figure and sells that information to a gossip magazine. In this scenario, unauthorized acquisition *and harm* occurred. However, unauthorized acquisition has not occurred when an employee inadvertently accesses the database, realizes that it was not the intended data, and logs off *without reading, using, or disclosing anything* [emphasis added]. In other words, the employee did nothing with the data to cause any degree of harm.

The FTC further implicitly introduces the idea of harm by noting that since the definition of IHI relates to "the health or condition" of the individual, it would include the fact of having an account with a vendor of PHRs or a related entity, where the products or services offered by such vendor or related entity relate to particular health conditions (e.g., mental illness or AIDS). But what if there was unauthorized acquisition of the names of people who used a PHR (and simply their names) where that product does not relate to any particular health condition: e.g., John Doe uses HealthVault. Would the PHR vendor have to notify all of its customers/users that an unauthorized person acquired the information, even if health data were not involved in the acquisition? In this type of case, we do not think notification should be required as any notification such as this would be inconsistent with the logic implied by the FTC.

BCBSA believes the FTC's recognized difference between acquisition and access should lead the agency more explicitly to give PHR vendors the flexibility to determine when a notice is necessary, as is the case under California law, while also providing a fairly objective standard against which compliance can be measured. Under guidance issued by the California Office of Privacy Protection, a variety of factors should be considered in determining whether information has been acquired, such as indications that (1) an unauthorized person is in the physical possession and control of protected data (such as from a lost or stolen computer or other device); (2) protected data has been downloaded or copied; and (3) an unauthorized person has used protected data to open new accounts. These factors are discussed in the California Office of Privacy Protection's publication, "Recommended Practices on Notification of Security Breach Involving Personal Information"[3] and should be considered when the FTC finalizes its rule.

[3] Roberson, C. (2008). *Identity theft investigations.* New York: Kaplan Publishing.

Allowing PHR vendors to assess risk is important because, as the FTC has previously testified, requiring a notice when a security breach poses little or no risk of harm might create unnecessary consumer concern and confusion. "If notices are required in cases where there is no significant risk to consumers, notices may be more common than would be useful. As a result, consumers may become numb to them and fail to spot or act on those risks that truly are significant. In addition, notices can impose costs on consumers and on businesses, including businesses that were not responsible for the breach. For example, in response to a notice that the security of his or her information has been breached, a consumer may cancel credit cards, contact credit bureaus to place fraud alerts on his or her credit files, or obtain a new driver's license number. Each of these actions may be time-consuming for the consumer, and costly for the companies involved and ultimately for consumers generally."[4]

Therefore, BCBSA recommends that no notification be required if there is not a significant risk of identity theft or other similar harm. If no significant risk is proven during the 60 day window, then no notice must be issued to the consumer or reported to the FTC. BCBSA is committed to protecting all of its members from identity theft, but countless unnecessary notifications could desensitize them to the notifications – putting them at greater risk if a real threat were to occur.

Thank you for the opportunity to comment on the proposed rule. If you have any questions, please contact Joel Slackman on my staff at 202.626.8614 or Joel.Slackman@bcbsa.com.

Sincerely,

Justine Handelman
Executive Directory, Legislative and Regulatory Policy

[4] Prepared statement of the Federal Trade Commission before the Committee on Commerce, Science, And Transportation, U.S. Senate on Data Breaches and Identify Theft (June 16, 2005).