

VIA <https://secure.commentworks.com/healthbreachnotification>

June 1, 2009

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

Dear Commissioner Leibowitz:

Re: Health Breach Notification Rulemaking, Project No. R911002

The National Association of Chain Drug Stores (NACDS) appreciates the opportunity to provide our comments on FTC's proposed rule to implement the breach notification requirements of the American Recovery and Reinvestment Act of 2009 ("ARRA"). We hope that our perspectives are helpful to FTC as you work to finalize these rules.

413 North Lee Street  
P.O. Box 1417-D49  
Alexandria, Virginia  
22313-1480

NACDS represents traditional drug stores, supermarkets, and mass merchants with pharmacies. Its more than 170 chain member companies include regional chains with a minimum of four stores to national companies. NACDS members also include more than 1,000 suppliers of pharmacy and front-end products, and nearly 90 international members representing 29 countries. Chains operate more than 39,000 pharmacies, and employ a total of more than 2.5 million employees, including 118,000 pharmacists. They fill more than 2.5 billion prescriptions yearly, and have annual sales of over \$750 billion. For more information about NACDS, visit [www.NACDS.org](http://www.NACDS.org).

**Definition of "Breach of Security"**

FTC's proposed definition for "breach of security" under rule section 318.2(a) would create a presumption that unauthorized acquisition occurs when there is unauthorized access to unsecured PHR identifiable information, and this presumption may be rebutted with reliable evidence showing that there has not been, or could not reasonably have been any unauthorized acquisition. We appreciate FTC's recognition and establishment of a clear difference between access to information and acquisition. As FTC states in the preamble, unauthorized persons may have access to information, however the term acquisition suggests that the information is not only available to unauthorized persons, but in fact has been obtained by them. It is this recognition and distinction by FTC that causes us concern about the presumption that unauthorized acquisition has, in fact, occurred. This presumption renders FTC's distinction hollow, as the affected entities would have to undertake breach notification steps unless they can rebut the presumption that mere access is tantamount to acquisition. This is especially true for situations in which unauthorized employees may have access to certain information but do not actually acquire it because doing so would violate corporate security policies and

(703) 549-3001

Fax (703) 836-4869

[www.nacds.org](http://www.nacds.org)

procedures, and thus lead to disciplinary action or termination of employment. It may be impossible for affected entities to continuously prove that unauthorized acquisition did not occur; hence, they would be forced to overwhelm consumers with multiple breach notification requirements. We urge FTC to reverse this presumption with respect to employees of an affected entity, so long as there are security policies, procedures, and systems in place to prevent employees from acquiring unauthorized information. When a system indicates that an employee has violated policies and procedures and has acquired unauthorized information, then breach notification procedures should begin. As FTC properly recognizes in the rule's preamble "the Commission believes that the entity that experienced the breach is in the best position to determine whether unauthorized acquisition has taken place."

#### **Definition of PHR Identifiable Health Information**

We thank FTC for your recognition that "PHR identifiable health information" does not include information for which there is no reasonable basis to believe that such information can be used to identify an individual. FTC properly states that de-identified information under the HHS rules implementing HIPAA falls outside the definition of "PHR identifiable health information" and therefore is not covered by this proposed rule. Information that has been "de-identified" is, by its very nature, devoid of information that would identify an individual. It would be unwise to require notification of individuals about the breach of this type of information, as the notifying entity would, ironically, first have to seek to re-identify the information before doing so.

#### **Breach Notification Requirements**

Under rule section 318.3(b), FTC would require a third party service provider to provide notice of breach to a senior official at the PHR vendor or related entity, and to obtain acknowledgement from such official that such notice was received. FTC states that the "purpose of this requirement is to avoid the situation in which lower-level employees of two entities might have discussions about a breach that never reaches senior management. It is also designed to avoid the problem of lost emails or voicemails." We thank FTC for the wisdom of this provision, but would like to request one modification. Each entity is in the best position to understand its own business processes and reporting flows. Rather than requiring notification to a generic "senior official," we ask FTC to require a third party service provider to provide notice of breach to the PHR vendor's or related entity's designated official. This would ensure that the PHR vendor or related entity would be able to respond appropriately to such notice.

Rule section 318.3(c) provides when a breach must be treated as "discovered" for the purposes of ARRA. We applaud FTC for your recognition that certain breaches may be very difficult to detect, and that an entity with strong breach detection measures may fail to discover a breach. In such circumstances, FTC would not consider the failure to discover the breach a violation of the rule. So long as an entity has taken reasonable steps to protect information and discover breaches, they should not be considered to be in violation of the rule for breaches that reasonable measures would not prevent or detect.

Under rule section 318.4(a), breach notifications would have to be made without “unreasonable delay.” We agree with this reasonableness standard; however, we ask FTC to consider that when an employee alerts management about a potential breach, an investigation must be conducted to determine if a breach has, in fact, occurred. This necessary step should be included in the determination of whether any delay is reasonable.

The substitute notice requirement under section 318.5(a)(4)(i) would require posting on the home page of the Web site for a period to of six months. We respectfully request FTC to reconsider this unnecessarily lengthy posting time period. Leaving information on a Web site for an unnecessarily long period of time would lead to confusion for consumers, as they may see information about the same incident and wonder if the posting refers to the same or a newer incident. We believe that an appropriate period of time would be 60 days, the same amount of time by which a patient must be notified about a breach.

The alternative form of substitute notice under section 318.5(a)(4)(ii) would be media notice “in major print or broadcast media, including major media in geographic areas where individuals affected by the breach likely reside.” The FTC’s proposed rule is substantively identical to the statutory language in ARRA, but would add “which shall be reasonably calculated to reach individuals affected by the breach.” We agree with FTC’s assessment that because the notice is intended to serve as a substitute to particular individuals, it should be reasonably calculated to reach those individuals. We commend FTC for this proposal.

Section 318.5(c) would require notification to FTC within five business days if the breach was with respect to 500 or more individuals. As mentioned above, when an employee alerts management about a potential beach, an investigation has to be conducted to determine if a breach occurred and the number of people potentially affected. We believe in many cases that five business days would not allow enough time to conduct a proper investigation, especially for large corporations. In addition, law enforcement may request that the entity not disclose information about the investigation to anyone. Most investigations will, in fact, require many weeks to complete. We believe a more reasonable time frame would be 60 days, the same as the time limit for notifying individuals.

#### **Potential Conflict with State Laws**

We request clarification from FTC with regard to the interaction of FTC’s breach notification requirements with state laws. States laws may have different or conflicting breach notification requirements. For example, Massachusetts law specifically prohibits the notification from including the nature of the breach and the number of residents

affected.<sup>1</sup> It seems that it may be impossible to comply with both FTC's proposed rules and Massachusetts law.

Considering the reasoning behind the Massachusetts law, we question the wisdom of FTC's breach notification requirement to the media. In such instances, it may cause more harm than good to alert potential opportunists to the fact that certain consumers' sensitive information has been breached and may be available for misuse.

### **Reasonableness Standard**

We recommend that FTC adopt a reasonableness standard with respect to the circumstances or situations that would compromise the privacy or security of PHR identifiable information, as many states have already adopted for sensitive consumer information. Our research has found that 19 states<sup>2</sup> have adopted such a standard. Generally, these states require the consumer be notified unless misuse of the information is not reasonably possible. For example, if an employee accidentally took information home one night and returned it the next day, there would be no risk of harm. It would not make much sense to require a breach notification in this instance. Such reasonableness standard prevents consumers from being overwhelmed by breach notifications where there would be no risk of harm to the individual.

If the purpose of the breach notification is to empower consumers to protect themselves, only those breaches that merit action by the consumer should be subject to notification. Otherwise, consumers will waste time and resources seeking to remediate harmless breaches.

### **Entities with Dual Status**

As FTC alludes in the rule preamble, there are entities for which it may not be clear whether they should be regulated by FTC, HHS, or both under the provisions of ARRA. This confusion will extend to HIPAA covered entities as they will need to know how to interact with these potentially indeterminate entities. We urge FTC to work with HHS to develop clear guidelines so that all stakeholders may have a clear understanding of which rules apply to which entities. Moreover, we urge FTC to work with HHS to harmonize these proposed rules as much as possible.

---


<sup>1</sup> M.G.L.A. 93H § 3

<sup>2</sup> Those 19 states are the following: AZ, AR, CO, DE, FL, ID, KS, LA, ME, MI, MO, NJ, NC, OH, PA, RI, VT, WA and WY.

**Conclusion**

Thank you, again, for the opportunity to comment on FTC's proposed rules to implement the breach notification requirements of ARRA. Please feel free to contact me at [knicholson@nacds.org](mailto:knicholson@nacds.org) or 703-837-4183, if we can provide further assistance.

Sincerely,

  
Kevin N. Nicholson, R.Ph., J.D.  
Vice President  
Government Affairs and Pharmacy Advisor