

**VIA Electronic Submission to <http://www.regulations.gov>**

May 21, 2009

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

*Re: Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information [45 CFR Parts 160 and 164]*

Dear Sir or Madam:

Thank you for the opportunity to submit our comments on the above-referenced guidance. As the Department of Health and Human Services (HHS) considers issues pertinent to the development of its interim final regulations for breach notification, the National Community Pharmacists Association (NCPA) appreciates the opportunity to share our recommendations.

NCPA represents America's community pharmacists, including the owners of more than 23,000 independent community pharmacies, pharmacy franchises, and chains. Together they employ over 300,000 full-time employees, and dispense nearly half of the nation's retail prescription medicines.

**NCPA's comments focus on the following areas:**

- Maintaining an exemption from breach notification requirements for information contained in limited data sets;
- Concerns regarding federal and state conflicts for notification and general breach laws and the administrative and compliance challenges presented;
- The need for clarification to the definition of breach under *American Reinvestment and Recovery Act (ARRA)* and to provide more specific examples of circumstances raised by the statutory definition;
- The need for further clarification regarding HHS's regulatory enforcement of breaches and examples of circumstances that would result in violations defined by ARRA that could result in monetary penalties;
- Challenges faced by community pharmacies in issuing notice, particularly in circumstances where a business does not have an internet home page or those pharmacies in rural areas that do not have ready access to national media; and,

- The need to specify circumstances where personal health record (PHR) vendors are actually business associates to covered entities and thus governed by HHS breach requirements and when these entities can use the Federal Trade Commission (FTC) guidance.

### **Technologies and methodologies that render Protected Health Information (PHI) unusable, unreadable, or indecipherable**

As technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals will undoubtedly change over time, we support the annual update of guidance specifying such technologies and methodologies. We also support the recognition of differing states of data, such as “data in motion,” and the differences in security methods for such data states. Regarding PHI in a limited data set, this should be treated as unusable, unreadable or indecipherable for purposes of breach notification, and information contained in limited data sets should maintain an exemption from breach notification requirements. The risk to re-identification is minimal and PHI in a limited data set can be utilized for meaningful purposes in the healthcare field, including vital research regarding the use of prescription medications for purposes of adherence and improved health outcomes.

### **Areas of conflict with state breach notification laws**

Most independent community pharmacies regularly work with patients and physicians on an interstate basis. Currently, varying state standards allowed by the HIPAA Privacy Rule serve as a serious impediment to sharing information in a truly interoperable national health information network. A patchwork of state breach notification laws cause concern for our members who may have to determine which law applies if a breach occurs related to both PHI, to which provisions in the HITECH Act applies, and non-PHI but still personal and private information, to which the state law would apply. There may be a significant conflict between federal and state law regarding notification. HHS should be mindful of trends in state regulatory enforcement in this area. While federal and state regulations are important in this area, without some level of consistency, administrative efficiencies intended by the use of electronic systems could be reduced because health care entities must invest time and resources into complying with a multitude of regulations.

### **Definition of “breach” and need for a reasonableness standard**

Regarding the Act’s definition of “breach”, NCPA appreciates the exclusion of unintentional disclosures in the definition of breach. However, we seek clarification regarding which unauthorized activities would compromise the privacy or security of PHI. NCPA suggests that in the final breach guidance and forthcoming regulations, HHS more plainly define circumstances that illustrate the definition of breach. For example, if a prescription is initially handed to the wrong patient and that patient notices the error and the pharmacy then provides the proper prescription, this could be an example of an unauthorized person who would not reasonably be able to retain disclosed PHI and therefore would be seemingly exempt from the breach notification requirement. However, proving the employee’s intent could be a subjective analysis because it could be unclear whether the employee intentionally handed the wrong prescription to the patient or whether it was an error. In most similar circumstances, the breach would be unintentional; however, the interpretation would be left solely to

the parties involved: the employee and the patient who may have differing views. Should the pharmacy report the breach to be cautious because intent of the employee is subject to interpretation? Furthermore, could this brief encounter with another patient's information rise to the level of having the ability to retain PHI? This is one example of many circumstances not clarified in current guidance or in law. Health care providers and consumers would benefit from further clarification of these provisions.

With respect to the circumstances or situations that would compromise the privacy or security of PHI, we strongly recommend that HHS apply a reasonableness standard in the determination of the levying of fines on entities involved in breaches. NCPA is concerned that community pharmacies would receive a disproportionate share of fines. In many cases, larger, corporate pharmacies would be more affected by the public reporting requirements because of the large number of patients these corporations serve. In contrast, NCPA members, as small business owners, would more likely be affected by monetary penalties. While NCPA members seek to ensure the highest level of security for all patient records, absolute security of health records is nearly impossible to achieve even for the most technologically advanced systems and companies. NCPA is particularly concerned about external entities that would gain unauthorized access to electronic records. For example, if an outside entity hacks into the computer records of a community pharmacy, the breach provisions would apply and individuals have the right to be notified. However, NCPA remains concerned that despite language in the ARRA to protect individuals and entities in certain circumstances, more regulatory guidance is necessary to protect entities that act in good faith and to define the new levels of penalties, particularly willful neglect, that will trigger monetary penalties. While NCPA appreciates that not all situations will be covered, more guidance will be helpful to providers in avoiding unnecessary penalties.

### **Need for alternative methods of notice when a breach occurs**

In the case where there is insufficient or out-of-date patient contact information that precludes direct written breach notification to the individual, a substitute form of notice is allowed. NCPA recommends that such notice be allowed to include a posting or written handout in the pharmacy. If there is insufficient contact information for more than 10 affected individuals that precludes written notice, a conspicuous posting on the pharmacy's web site, or notice in major print or broadcast media that includes a toll-free number, is required. Based on an internal analysis of NCPA member business practices, we estimate that only 51% of independent community pharmacies actually have a website. In addition, 52% of independents are located in areas with a population of less than 20,000 people, where major print or broadcast media access may be limited.<sup>1</sup> For these reasons, we recommend that in the case of insufficient contact information for more than 10 affected individuals, pharmacies be allowed to include a posting or written handout in the pharmacy in lieu of posting on a website or in major print or broadcast media. Finally, the vast majority of independent community pharmacy owners do not have a toll-free number that their patients can use to access the pharmacy. Therefore, we ask, in instances where a toll-free number doesn't exist, that this requirement be waived.

---

<sup>1</sup> 2008 NCPA Digest, sponsored by Cardinal Health

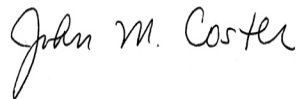
**Circumstances that constitute business associate relationships with covered entities**

NCPA anticipates that its members will work with vendors of personal health records (PHR) for many different patient care reasons and that these partnerships will assist community pharmacies provide better care and outcomes, particularly through medication therapy management programs. However, it is for this reason that NCPA would like to see further clarification in the HHS guidance regarding circumstances that constitute business associate relationships with covered entities. NCPA understands that FTC seeks comment in this area because of its primary authority over breaches by PHR vendors delegated under ARRA. Once comments have been received, HHS, as the agency with experience in privacy and security enforcement, should take an active role with FTC in developing specific guidance and regulations in this area. These clarifications will provide assurances to NCPA members and other health care entities that PHR vendors must maintain a greater level of accountability for maintaining PHI and thus provide more incentive to enter into agreements knowing that both parties must maintain information at the highest level to prevent unauthorized uses and disclosures.

NCPA respectfully requests that you address our concerns regarding the breach notification requirements. NCPA supports the use of health information technology (HIT) to improve quality of care, better coordinate care, and reduce costs. We also recognize the need for patients to be confident that providers are protecting their health information and only using it for legitimate purposes relating to treatment, payment and health care operations.

NCPA appreciates the opportunity to comment on 45 CFR Parts 160 and 164. If you have any questions, please contact me at (703) 683-8200 or [john.coster@ncpanet.org](mailto:john.coster@ncpanet.org).

Sincerely,



John M. Coster, Ph.D., R.Ph.  
Senior Vice President, Government Affairs  
National Community Pharmacists Association