Via Electronic Submission to https://secure.commentworks.com/ftc-healthbreachnotification/

June 1, 2009

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

Re: Federal Trade Commission 16 CFR Part 318 [RIN 3084–AB17] Health Breach Notification Rule; Health Breach Notification Rulemaking, Project No. R911002

Dear Sir or Madam:

Thank you for the opportunity to submit our comments on the above-referenced notice of proposed rulemaking. As the Federal Trade Commission (FTC) considers issues pertinent to the development of its rules requiring vendors of personal health records (PHR) and related entities to notify individuals when the security of their individually identifiable health information is breached, the National Community Pharmacists Association (NCPA) appreciates the opportunity to share our comments.

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.

In comments submitted on May 21, 2009, to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights regarding the HITECH Breach Notification guidance, NCPA asked for further clarification regarding circumstances where PHR vendors are actually business associates to covered entities and thus governed by HHS breach requirements and when these entities can use the FTC guidance. This is a very important distinction to make, as NCPA anticipates that its members will work with PHR vendors for many different patient care reasons and there are multiple ways in which PHR vendors may have a dual role as a business associate of a HIPAA-covered entity and a direct provider of a PHR to members of the public. For example, if a PHR vendor is a business associate of a community pharmacy, then presumably HHS' rule requirements would prevail. However, if a PHR vendor is a business associate of a covered entity and a breach occurs but did not contain Protected Health Information (PHI) provided by the covered entity, who is responsible for the breach notification requirements?

Once comments have been received, FTC should take an active role with HHS 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.

We ask that as the FTC works to harmonize its proposed rule with HHS' proposed rule that the following be taken into consideration:

- In regard to proposed section 318.2: Definitions, Breach of Security, FTC recognizes that when unauthorized access to unsecured PHR identifiable health information occurs, the entity that experienced the breach is in the best position to determine whether unauthorized acquisition has take place. This section creates a rebuttable presumption that allows an entity to present reliable evidence that acquisition could not have occurred or could not have reasonably occurred. NCPA believes this presumption would be difficult to rebut because the presumption suggests that access is equivalent to acquisition. As an alternative, NCPA would support a reasonableness standard allowing objective evidence to be presented that an employee or other individual actually violated existing policies and procedures and thus acquired information in an unauthorized manner. NCPA also requests that FTC work with HHS to adopt a reasonableness standard with respect to the circumstances or situations that would compromise the privacy or security of PHI in the case of HIPAA-covered entities. This will help to prevent consumers from being overwhelmed by potential breach notifications when there is no actual harm to the individual and could reduce the potential for administrative difficulties of having to rebut a presumption.

- In regard to proposed section 318.3: Breach notification requirement, FTC recognizes that certain breaches may be very difficult to detect and that even an entity with strong detection measures may fail to determine that a breach occurred. In these circumstances the failure to determine a breach would not constitute a violation of the proposed rule. NCPA asks that this reasonableness standard be applied to the breach discovery provision for HIPAA-covered entities under the HHS breach provisions as well. If a covered entity has taken reasonable steps to protect PHI they should not be in violation of the rule for breaches that reasonable measures would not prevent.

NCPA respectfully requests that you address our comments 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 16 CFR Part 318. If you have any questions, please contact me at (703) 683-8200 or john.coster@ncpanet.org.

Sincerely,

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