May 29, 2009

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

Re: Health Breach Notification Rulemaking, Project No. R911002

Dear FTC Commissioner:

On behalf of the Institute for Health Freedom (a Washington, DC-based non-profit educational organization founded in 1996 to educate the public about health-freedom issues: www.ForHealthFreedom.org), I am submitting the following comments in response to the Federal Trade Commission's request for public comments on the rule to require vendors of electronic personal health records (PHRs) to notify the FTC and affected individuals if **unsecured** health data are breached.

Data breaches are a significant problem in this country. Since January 2005, the U.S. has experienced more than 261 million data breaches, according to Privacy Rights Clearinghouse. Moreover, it is estimated that 12 percent of data breaches occurred with medical organizations, according to Open Security Foundation and DataLossDB.org.

To that end, it is important for Americans, policymakers, vendors, and the FTC to consider: Why are consumers only receiving breach notifications of **unsecured** health data in PHRs? What about breaches of **secured** health data in PHRs; will citizens get notifications of those breaches?

Also, the FTC should consider that email may not be an effective enough means for notification, and that a combined approach of both a telephone call and letter is the most effective method, according to a 2005 survey titled "National Survey on Data Security Breach Notification." The consumer survey found that "The most effective communication method appears to be a combined approach of telephone and letter."

As noted above, data breaches are a serious problem in the United States. According to Privacy Rights Clearinghouse, since January 2005, the U.S. has experienced 261,441,493 breaches (as of May 4, 2009): www.privacyrights.org/ar/ChronDataBreaches.htm#CP

Moreover, a 2005 national survey on data security breach notification found that: More than 1 out of 10 adult Americans (11.6 percent) reported receiving notification of a security breach during a one-year period; about 86 percent of breaches were related to the loss or theft of customer/consumer information; and about 14 percent of breaches

involved employee, student, medical, and taxpayer data. See the "National Survey on Data Security Breach Notification": www.whitecase.com/news/detail.aspx?news=670

Open Security Foundation and DataLossDB.org reports that 12 percent of data breaches involved medical organizations: http://datalossdb.org/statistics

Additionally, 44 states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information, according to the National Conference of State Legislatures: www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

To that end, it is important for the FTC to address: How will the federal breach-notification rule affect consumers' rights under existing state laws?

All told, it is important for the FTC to stress in its consumer protection role that health data are personal, and **individuals should be informed about breaches**, in the most effective way, **regardless of whether the data was secured or unsecured**.

Thank you kindly for considering these important issues.

Sincerely,

Sue A. Blevins, President
Institute for Health Freedom
Washington, DC
www.ForHealthFreedom.org