America's Health Insurance Plans

601 Pennsylvania Avenue, NW
South Building
Suite Five Hundred
Washington, DC 20004

202.778.3200
www.ahip.org

February 14, 2011

Submitted via the Internet at: https://ftcpublic.commentworks.com/ftc/consumerprivacyreport/

Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

Re: Request for Public Comments: The Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers

Dear Sir or Madam:

I am writing on behalf of America's Health Insurance Plans (AHIP) in response to the Commission's request for public comments in response to the preliminary staff report entitled, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers."[1]

AHIP is the national association representing approximately 1,300 health insurance plans that provide coverage to more than 200 million Americans. Our members offer a broad range of health insurance products in the commercial marketplace and have demonstrated a strong commitment to participation in public programs.

Our members have been at the forefront of developing business practices that ensure the privacy and confidentiality of individuals' health information in all mediums, including paper, electronic and oral formats. Health insurance plans have shown substantial leadership by devoting significant administrative and financial resources to developing and implementing private and secure business processes and systems, while also ensuring on an ongoing basis that business practices are current and keep pace with new developments and technical system solutions.

We understand and support the Commission's consumer protection role and appreciate that the agency is examining how commercial data privacy policies can better protect consumers from physical, economic, or other harm. The preliminary staff report will likely prompt more attention on privacy and security practices from those business sectors that are not currently

[1] The FTC report was made publicly available on the Internet at: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

governed by statutory or regulatory requirements. The report is also likely to continue the Congressional focus on evaluating existing laws and assessing whether changes should be implemented to keep U.S. business practices competitive with other countries.

After reviewing the report, our comments respond to the key FTC staff recommendations, which include:

- **Privacy by Design.** Companies should adopt a "privacy by design" approach by building privacy protections into their everyday business practices. This would include promoting privacy at every stage of development of products and services (e.g., data security, reasonable collection limits, sound retention policies, data accuracy, and data management procedures).
- **Simplified Choice.** Companies should provide choices to consumers about their data practices in a simpler, more streamlined way than has been used in the past. Consumer choice would not be necessary for a limited set of "commonly accepted" data practices, but for data practices that are not "commonly accepted," consumers should be able to make informed and meaningful choices.
- **Transparency.** A number of measures that companies should take to make their data practices more transparent to consumers are included in the report (e.g., clearer and shorter privacy notices, reasonable access, and affirmative consent to data uses that differ from the purposes for the data collections).
- **Education.** The paper proposes that stakeholders undertake a broad effort to educate consumers about commercial data practices and the choices available to them, particularly since increasing consumer understanding of the commercial collection and use of their information is important to facilitating competition on privacy across companies.

Privacy by Design

Issue and Recommendation 1: The current draft report would broadly apply to all commercial entities that can be reasonably linked to a specific consumer, computer, or other device (e.g., in "offline" and online situations). However, there is no substantial discussion of the business sectors that currently follow stringent federal and state privacy and security requirements (e.g., health care entities follow the Health Insurance Portability and Accountability Act [HIPAA], the Health Information Technology for Economic and Clinical Health [HITECH] Act which was included in the American Recovery and Reinvestment Act, and state privacy and security requirements), which protect consumers' data privacy and security at every stage of a company's business operations. Thus, the final FTC report should: (1) include an identification and brief discussion of existing laws and regulations that apply to certain commercial business sectors (e.g., healthcare); and (2)

focus its recommendations on commercial contexts not covered by existing privacy and security laws or regulations (i.e., exclude HIPAA covered entities and their business associates from the recommendations).

Discussion 1: The report advocates for development and adoption of a "privacy by design" approach that consists of several elements, including: a comprehensive set of Fair Information Practice Principles (FIPPs) to protect the privacy of personal information, privacy protections that are built into everyday business practices, promote transparency, consumer autonomy, and accountability; and appropriate enforcement mechanisms could be used if a violation occurs. In essence, the proposed approach would require businesses to: (1) provide notice of what information they collect from consumers and how they use it; (2) give consumers choice about how information collected from them may be used; (3) give consumers access to data collected about them; and (4) take reasonable steps to ensure the security of the information they collect from consumers.

While some business sectors may be unaccustomed to complying with privacy and security protections and processes, the health care sector is currently governed by a complex framework of statutory and legal requirements. The HIPAA framework[2] establishes the national standards for privacy and security requirements that are applicable to health care entities (referred to as HIPAA "covered entities"). The HIPAA regulations set out a number of comprehensive privacy requirements that protect information in paper, electronic, and oral forms.

The existing requirements with which HIPAA covered entities comply are very similar to the elements advanced in the report. For example, the HIPAA rules have specific provisions that require covered entities to: use and disclose only the "minimum necessary" information; provide individuals with a Notice of Privacy Practices that describes how health information may be used and disclosed; provide training to staff about privacy and security policies; allow individuals the ability to request access to, obtain a copy of their health information, and request amendments, when necessary; and have administrative, physical, and technical security features inherent in an overall security program.[3] In addition, states can build on the federal protections by enacting more stringent requirements.

Since HIPAA was passed, changing business trends and new methods for storing information in electronic formats prompted the recent enactment of the HITECH Act.[4] The HITECH Act was significant because it established national standards for covered entities and their business associates to use when responding to suspected data breaches, modified a number of the existing privacy requirements (e.g., by establishing new timeframes for tracking and accounting for

[2] 42 U.S.C. §1320d, *et seq.;* 45 C.F.R. Parts 160, 162, and 164.
[3] 45 C.F.R. §§164.502(b), 164.520, 164.530(b), 164.524, 164.526, and 164.102 *et seq.*
[4] 42 U.S.C. §17921 *et seq.* *See also*, 74 Fed. Reg. 42962 (2009) and 74 Fed. Reg. 42740 (2009).

disclosures made from Electronic Health Records), and enhanced the federal and state enforcement and penalty structures. HIPAA covered entities are continuing to refine their policies and procedures based on the HITECH requirements as they are being promulgated, and in response to agency guidance and other developments. Under the HITECH Act, both the U.S. Department of Health and Human Services as well as state Attorneys General can take action if a violation of a consumer's health information privacy or security is suspected.

Simplified Choice

Issue and Recommendation 2: The report advances the need for companies to provide consumers with choice about data practices. For example, for "commonly accepted" data practices, choice would not be necessary, but should be provided for data practices that are not commonly accepted (e.g., behavioral advertising).

Since commonly accepted data practices are likely to vary by industry (e.g., real estate services as compared to retail transactions), the final report should: (1) provide more specificity regarding consistent commercial data practices; and (2) set out exemptions for certain business sectors where the report's recommendations may set up conflicts with existing legal requirements (e.g., if a federal or state law allows the collection, use, or disclosure of certain data without a consumer's consent such as disclosing data for law enforcement purposes); and (3) focus its recommendations on commercial contexts not covered by existing privacy and security laws or regulations (i.e., exclude HIPAA covered entities and their business associates from the recommendations).

Discussion 2: The issue of whether consumers should have the ability to exercise choice in how their personal data is collected, used, and disclosed is continually being evaluated by federal and state policymakers. Requiring consumers to consent to routine data collections, uses, and disclosures of data can be viewed as burdensome and unnecessary by consumers, particularly for routine and reasonably-anticipated business transactions (e.g., consumers expect that a real estate agent will collect their name and disclose their property address when listing a home for sale). However, non-routine collections, uses, and disclosures may merit further evaluation and dialog in public forums to assess how commercial entities are engaging in data practices that may pose risks to the privacy or security of data.

The practical implication of requiring consumers to consent to non-routine collections, uses, and disclosures of data raises a number of questions that have yet to be resolved by policymakers, including: how commercial data practices can vary by business sector; what existing laws or regulations allow for data collections, uses, or disclosures of certain data without a consumer's consent; and what level of "granularity" should be implemented if consumer consent would be required (e.g., whether consumers would be required to consent to a process such as disclosing

their data to facilitate an electronic purchase using a debit card at a retail store or whether consumers would be permitted to control individual data elements, such as consenting to their names and debit card numbers to be disclosed but not the items being purchased in a retail setting). These issues merit further exploration as potential unintended consequences and substantial costs and burdens on consumers and private business entities could result.

Transparency

Issue and Recommendation 3: The report advocates for companies to make their data practices more transparent to consumers. The final report should continue to recommend increased transparency of data policies and procedures to consumers.

Discussion 3: A number of measures that companies should take to make their data practices more transparent to consumers are included in the report (e.g., clearer and shorter privacy notices). However, the use of privacy policies is discussed as an incomplete way to notify consumers of privacy and security practices.

While privacy policies may be lengthy, they have been one method for commercial entities to consistently and thoroughly explain to consumers how their personal data can be collected, used, and disclosed. In addition, the requirement for business entities to have a privacy policy is often based on federal or state law or regulation. Thus, the final report should continue to recommend increased transparency of data policies and procedures to consumers and should set out more information about how federal or state requirements can affect when, how, and in what form privacy policies are issued to consumers.

Education

Issue and Recommendation 4: The report advocates that stakeholders undertake a broad effort to educate consumers about commercial data practices and choices available to them. We support such efforts, but believe public and private entities should engage in consumer education and outreach.

Discussion 4: AHIP's members fully support educational programs and outreach opportunities that provide consumers with information about how their data is collected, used, and disclosed and how business processes keep data private and secure. Public and private entities should engage in such efforts, and should collaborate when possible to provide consumers the information they need to make decisions related to their personal data.

We appreciate the opportunity to comment on the report and this important topic.

Sincerely,

Marilyn Zigmund Luke
Senior Regulatory Counsel