America's Health
Insurance Plans

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

202.778.3200
www.ahip.org

January 28, 2011

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Room 4725
Washington, D.C. 20230

Re: Request for Comments on the Green Paper Addressing Commercial Data Privacy and the Internet

Dear Sir or Madam:

I am writing on behalf of America's Health Insurance Plans (AHIP) in response to the Department's request for public comments on the report, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework."[1] A Notice announcing the availability of the report and requesting public comments was published in the *Federal Register* on December 21, 2010.

We applaud the Commerce Department for leveraging the expertise of the National Telecommunications and Information Administration, the Patent and Trademark Office, the National Institute of Standards and Technology (NIST), and the International Trade Administration to create an Internet Policy Task Force. As part of its work, we understand that the Task Force is conducting a comprehensive review of the nexus between privacy policies and copyright requirements, the global flow of information, cyber-security, and innovation in the Internet economy. These are important and timely issues that will continue to have major implications for U.S. businesses and the consumers they serve.

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

[1] The report is available on the Internet at: http://www.ntia.doc.gov/internetpolicytaskforce/.

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 appreciate that the Internet Policy Task Force is examining how commercial data privacy policies can advance the goals of protecting consumer trust in the Internet economy while also promoting innovation. We support these goals and offer our recommendations for ways that the Task Force can build on the five specific Policy Options outlined in the report:

1) Adoption of a comprehensive set of Fair Information Practice Principles (FIPPs) to protect the privacy of personal information in commercial contexts not covered by an existing "sectoral" law.
2) Use of comprehensive FIPPs as the basis for recognizing expanding interoperability between U.S. and international commercial data privacy frameworks.
3) Adherence to voluntary industry codes of conduct.
4) Creation of a new Privacy Policy Office within the Department of Commerce to help provide the Administration with greater expertise and a renewed focus on commercial data privacy.
5) Setting a national standard for notifications following security breaches involving personal information in the commercial context.

We recognize that the Task Force issued the paper to promote public dialog about these issues and does not intend the paper to be a commitment to the specific policy proposals. Rather, the report explains that the key recommendations are intended to "play a key role in policy discussions within the Obama Administration."[2]

Our comments below are organized to correspond with each of the five principles and are intended to inform the Task Force's knowledge base by: (1) explaining how existing privacy and security requirements protect consumer data within the health care sector effectively; (2) advocating for increased federal coordination to ensure that all affected agencies (e.g., the U.S. Department of Health and Human Services [HHS], the Federal Trade Commission [FTC]) coordinate efforts to eliminate any differences in interpreting federal legal requirements or applicable policies; and (3) informing the Task Force's work in development of future white papers.

FIPPs

Policy Option 1a: The report advocates for adoption of a comprehensive set of Fair Information Practice Principles (FIPPs) to protect the privacy of personal information in commercial contexts

[2] Report page iv.

not covered by an existing law. The FIPPs would increase transparency, encourage purpose specifications and use limitations, and foster verifiable evaluation and accountability programs.

Discussion 1a: The health care sector is governed by a complex framework of statutory and legal requirements. The Health Insurance Portability and Accountability Act (HIPAA) and corresponding regulations[3] set 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, which are very similar to the elements that would be contained in FIPPs. 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.[4] 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 Health Information for Economic and Clinical Health (HITECH) Act, as included in the American Recovery and Reinvestment Act.[5] 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 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 as the HITECH requirements are being promulgated, and in response to agency guidance and other developments. Under the HITECH Act, both HHS as well as state Attorneys General can take action if a violation of a consumer's health information privacy or security is suspected.

Recommendation and Conclusion 1a: The health care sector currently follows stringent federal and state privacy and security requirements (e.g., HIPAA, HITECH Act, state privacy and security requirements). The Task Force should continue to focus its work and recommendations on commercial contexts not covered by existing laws or regulations.

---

[3] 42 U.S.C. §1320d, *et seq.;* 45 C.F.R. Parts 160, 162, and 164.
[4] 45 C.F.R. §§164.502(b), 164.520, 164.530(b), 164.524, 164.526, and 164.102 *et seq.*
[5] 42 U.S.C. §17921 *et seq.* *See also,* 74 Fed. Reg. 42962 (2009) and 74 Fed. Reg. 42740 (2009).

Policy Option 1b: The report advances the need for consumers to provide informed consent for how their information is collected, used, and disclosed. Specifically, the report solicits public comments related to whether: (1) non-governmental entities should be granted authority to enforce privacy and security requirements, in addition to federal regulatory enforcement; (2) the FTC should be granted an expansion of its statutory authority over commercial entities; and (3) commercial data privacy legislation should include a private right of action.

Discussion 1b: Given the recent changes in the HIPAA and HITECH Act enforcement structures and processes, we do not believe that further legislative actions are necessary at this time to change existing privacy and security requirements, the enforcement processes applicable to the health care sector (i.e., HIPAA covered entities and their business associates), or private rights of action. As discussed above, existing federal regulatory efforts are currently focused on developing and issuing regulations to conform to the HITECH Act, and these requirements need time to be promulgated by federal agencies and implemented by affected entities to allow the benefits of the law and regulations to be fully realized. New legislative changes at this time could cause significant duplication in regulations and guidance, conflicts in interpretations and agencies' jurisdictions, and increased costs for affected business entities, without substantial, corresponding benefits to consumers.

Recommendation and Conclusion 1b: The Task Force should focus its legislative recommendations on commercial entities that are not covered by existing privacy or security laws or regulations.

International Issues

Policy Option 2: The report discusses the use of comprehensive FIPPs as the basis for recognizing expanding interoperability between U.S. and international commercial data privacy frameworks.

Discussion 2: The report explains that differing legal frameworks and new technologies present international privacy challenges and can complicate commercial data flows across national borders. As a result, the Task Force recommends that the commercial data privacy framework be updated using FIPPs in order to protect the Internet's important role in our economy and society. While this is a laudable goal, the report is currently unclear as to how the use of FIPPs will improve individuals' privacy and security protections from a practical standpoint, particularly since the report recognizes that a key vulnerability of FIPPs is that their use can lead to "a waste of resources" or that they "might not be sufficiently protective."[6]

[6] Report page 41.

One of the key ways in which a breach of the privacy or security of information via the Internet will directly affect individuals is through criminal activity associated with identity theft. Several years ago, a President's Identity Theft Task Force evaluated the international issues that create an environment for identity theft to occur and for criminals to thwart prosecution. Two key themes emerged: (1) a lack of consistent laws and procedures across international borders; and (2) a lack of international investigation and prosecution of cybercrimes. Given the current focus on data privacy and security related to the Internet, the Internet Policy Task Force should consider the prior recommendations of the Identity Theft Task Force for addressing unique international variables that promote the use of the Internet as a criminal tool and create substantial risks to cyber and national security.

Recommendation and Conclusion 2: The Internet Policy Task Force, in conjunction with the U.S. Departments of Justice and State, should seek ways to mobilize international enforcement opportunities in prosecuting cyber crimes and criminal actions resulting from privacy and security breaches via the Internet. For example, U.S. officials could work with other countries to assist, train, and collaborate with international allies in appropriate enforcement activities.[7]

Voluntary Industry Codes of Conduct

Policy Option 3: The report advocates for adherence to voluntary industry codes of conduct.

Discussion 3: We support the use of voluntary industry codes of conduct as a way to improve consistency in privacy and security protections to protect consumers. The report suggests a process by which the FTC could approve such codes of conduct, providing a "safe-harbor" from enforcement actions if the entities comply with the approved, voluntary standards.

Using this model, we raise two issues that merit further evaluation and discussion: (1) whether federal agencies other than the FTC (e.g., HHS, the U.S. Department of Labor, the U.S. Department of the Treasury) have available resources and could provide appropriate oversight for codes of conduct developed by various sectors or entities over which the federal agencies have jurisdiction; and (2) the manner by which the FTC and the U.S. Department of Justice would address potential antitrust concerns related to such voluntary codes of conduct.

We also suggest that if voluntary codes of conduct are developed, federal agencies reviewing the codes should develop certain objective criteria to ensure benefits to consumers. For example, such criteria should emphasize that the codes are: tailored to specific entities, business products,

[7] Key recommendations from the September 2008 President's Identity Theft Task Force should also be evaluated as appropriate for this project and future work related to the Internet Policy Task Force.

and factual situations; not designed to provide a single, universal approach for all commercial entities (i.e., do not set forth a one-size-fits-all approach); and intended to allow for innovation and flexibility in business models and designs.

Recommendation and Conclusion 3: We believe that voluntary industry codes of conduct may be useful in establishing consistent privacy and security frameworks by business sectors. Before adopting such a recommendation, we encourage the Internet Policy Task Force to consult with federal regulatory agencies and specifically the FTC and the U.S. Department of Justice to identify jurisdictional issues, available agency resources, and potential legal considerations (e.g., antitrust).

Department of Commerce Privacy Policy Office

Policy Option 4: The report recommends that a new Privacy Policy Office be established within the U.S. Department of Commerce to help provide the Administration with greater expertise and a renewed focus on commercial data privacy.

Discussion 4: We encourage all federal agencies to establish a Privacy Officer to ensure that public data privacy and security practices are consistent with consumers and private entities' requirements and expectations for protecting personally identifiable information. We are concerned, however, that the current proposal would create a Commerce Department Privacy Policy Office to serve as a center of commercial data privacy policy expertise, which could duplicate the functions of existing federal agencies.

On January 18, 2011, the President issued Executive Order (EO) 13563 which called for a 21st century regulatory structure under which federal agencies must weigh and balance costs and benefits when adopting regulations and do so in a transparent environment, with input from experts, businesses, and ordinary citizens. In addition, the EO requires agencies to avoid excessive, inconsistent, and redundant regulations.

In the area of health information privacy, multiple agencies are currently evaluating privacy and security privacy policies for their own operations, as well as for the entities over which the agencies have jurisdiction. As discussed above, the HHS Office for Civil Rights is the primary agency with authority for promulgating health information privacy and security regulations. However, multiple federal agencies have begun to examine health privacy policies and issue regulations, reports, or other guidance documents based on their jurisdictional authority or interest in emerging issues.[8] The U.S. Department of Commerce's efforts would further expand

[8] For example, the HHS Office for Civil Rights, acting under the HITECH Act, recently set requirements for HIPAA "covered entities" and business associates to respond to suspected data breach situations. In a similar effort, the

and appear to duplicate these efforts.

Recommendation and Conclusion 4: All federal agencies should appoint a Privacy Officer to ensure that public data privacy and security policies and procedures adequately protect consumers' information. Federal agencies should coordinate efforts related to privacy and security requirement to avoid duplication of efforts and ensure consistency with the regulatory requirements applicable to various entities and business types.

National Data Breach Requirements

Policy Option 5a: The report advocates establishing a national standard for notifications following commercial security breaches involving personal information.

Discussion 5a: AHIP's members fully support the establishment of national standards for notifying consumers if their information is involved in a data breach situation. Future legislative and regulatory efforts should focus primarily on those business sectors and entities that do not currently comply with federal data breach notification requirements. In addition, federal efforts should evaluate whether state laws should be preempted to enable a consistent, federal data breach framework.

Recommendation and Conclusion 5a: The HITECH Act establishes consistent requirements for HIPAA covered entities and their business associates to follow in the event a breach of the privacy or security of data was detected. Future legislative and regulatory efforts should: (1) look to the HITECH requirements as a model that could be applied to business sectors or entities that currently do not conform to federal data breach requirements; and (2) evaluate how a national standard can be developed to avoid duplication of efforts and ensure consistency in requirements applicable to commercial entities.

Policy Option 5b: The report recommends that the Administration review the Electronic Communications Privacy Act, with a view to addressing privacy protections in cloud computing

---

FTC set regulatory requirements for personal health record vendors and similar entities. The HHS Office of the National Coordinator for Health Information Technology also has active advisory bodies evaluating privacy and security requirements in various electronic mediums and settings. The HHS Centers for Medicare & Medicaid Services develops privacy and security parameters for federal health benefits programs. There is also activity occurring at the Department of Homeland Security, the National Institute of Standards and Technology, the Office of Personnel Management, and within the States to develop various privacy and security requirements and projects. A President's Council of Advisors on Science and Technology also issued a report that made recommendations on how to protect the privacy and security of data in electronic environments.

and location-based services to ensure that, as technology and market conditions change, the Act will continue to protect individuals' expectations of privacy and effectively punish unlawful access to and disclosure of consumer data.

Discussion 5b: The National Institute of Standards and Technology (NIST) recently hosted a public workshop to explore the emerging uses of cloud computing technologies.[9] In addition, the White House Office of Management and Budget (OMB) continues to promote the use of cloud computing by federal agencies.[10] While some public or private entities may have experience using cloud computing, some may not have the technical background to understand how cloud computing can promote or make vulnerable the privacy and security of information contained in the "cloud."

Recommendation and Conclusion 5b: We support the recommendation for the Administration to evaluate the Electronic Communications Privacy Act in consideration of cloud computing and location-based services. We encourage the Task Force and the Administration to expand the scope of its work to also evaluate other privacy and security laws (e.g., the Privacy Act of 1974[11], the Electronic Signatures in Global and National Commerce Act[12]). In addition, the Task Force, in collaboration with NIST and other appropriate federal agencies, should issue guidance: (1) describing cloud computing and location-based services and how these technologies may improve or make vulnerable commercial privacy and security practices currently in use; and (2) providing recommendations or information for public and private entities about how to address and mitigate privacy and security risks (i.e., how agencies and entities may use cloud computing and location-based services to consistently ensure privacy and security protections).

---

[9] Information related to the NIST workshop is available on the Internet at: http://www.nist.gov/itl/cloud/cloudworkshopii.cfm.

[10] *See*, OMB Memorandum dated September 14, 2010 detailing "The Accountable Government Initiative: An Update on Our Performance Management Agenda," as available on the Internet at: http://www.whitehouse.gov/sites/default/files/omb/memoranda/2010/AccountableGovernmentInitiative_09142010.pdf.

[11] 5 U.S.C. §552a.

[12] 15 U.S.C. §7001 *et seq.*

We appreciate the opportunity to comment on the report and stand ready to provide information as future projects and policies develop on this important topic.

Sincerely,

Marilyn Zigmund Luke
Senior Regulatory Counsel