International Pharmaceutical
PRIVACY CONSORTIUM

1500 K Street NW • Suite 1100 • Washington DC 20005 USA
Telephone 202 230 5142 • Facsimile 202 842 8465 • Website www.pharmaprivacy.org

January 28, 2011

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230

Re: Docket No. 101214614-0614-01 - Department of Commerce Internet Policy Task Force Report on Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework

Dear Secretary Locke:

The International Pharmaceutical Privacy Consortium (IPPC) is an organization formed in 2002 and comprised of chief privacy officers and other data privacy and security professionals from a number of research-based, global pharmaceutical companies. The IPPC is committed to the promotion of sound policies for the protection of patient privacy and advancement of drug development and treatment. Information concerning IPPC membership and mission is described in Appendix A.[1]

We appreciate this opportunity to present our views on the Proposed Policy Framework for Commercial Data Privacy and Innovation ("Green Paper"). Specifically, we will address the following issues:

1) the scope of application of the Framework;
2) privacy information notices;
3) privacy impact assessments;
4) privacy codes of conduct;
5) global interoperability; and
6) a national security breach notification requirement.

We also provide in Appendix B of this submission a copy of the IPPC's 2008 document entitled "Privacy Guidelines for Marketing to U.S. Consumers." We encourage the Department's review of and feedback on these guidelines.

I. Scope of Application of the Framework

Relationship to Sectoral Privacy Laws

We agree with the Green Paper's recommendation that "a baseline commercial data privacy framework should not conflict with the strong sectoral laws and policies that already provide important protections to Americans."[2] IPPC member companies are regulated by multiple federal agencies, including the Food and Drug Administration (FDA), and our patient and consumer-directed activities often are subject to overlapping federal and state privacy and consumer protection laws. We are concerned about added complexity and the potential for inconsistent, redundant or contradictory requirements. The

[1] For further information concerning the IPPC, please visit our website at www.pharmaprivacy.org. All Appendices referenced in this comment, and additional documents adopted by the IPPC, are publicly available on this website.
[2] Green Paper Recommendation #8, at 58.

IPPC believes that in order to avoid inconsistencies, where sector-specific privacy requirements have already been enacted (e.g., HIPAA), safe harbors should be provided for organizations that are subject to those requirements. For example, where pharmaceutical companies work with HIPAA covered entities to provide resources to enroll patients in a prescription drug adherence program, fulfillment of the applicable notice, choice and access requirements under the HIPAA Privacy Rule should meet the relevant Choice and Transparency requirements of a FIPPs-based framework.

Application to Biomedical Research and Public Health Activities

In our comments to the FTC dated June 14, 2010, we urged the Department to recognize the complexity of applying a privacy framework designed principally with sales and marketing uses of information in mind to biomedical research and public health activities. The Green Paper emphasizes that it is intended to apply only in the "commercial" context. We believe that further clarity is needed regarding how the term "commercial" is being used in the Green Paper. There may be unintended consequences if biomedical research and public health activities were included within the Framework. We wish to reiterate our position that regardless of whether commercial actors are involved, the areas of biomedical research and public health should be addressed in a separate framework, such as the uniform approach to health research recommended by the Institute of Medicine in its report *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research.*[3]

II. Privacy Information Notices

There is an inevitable tension between the Department's desire for privacy information notices to be shorter and simpler with the need for such notices to be complete, accurate, and to offer the consumer sufficient detail to be able to make an informed decision. The IPPC fully agrees with the goal of making privacy notices as clear and comprehensible as possible. Indeed, certain IPPC members have been experimenting with offering layered privacy notices and other simplified and standardized means to make their notices as clear and easy to understand as possible. IPPC members also have adapted their privacy notices to alternative data collection formats, such as mobile health applications for smart phones. We encourage the Department to provide examples of privacy information notices, including language and formats that it finds meet its goals of clarity and comprehension for a variety of media. Nevertheless, because we believe that privacy information notices must necessarily be tailored to the specific data processing activities in question, we caution against any efforts to mandate prescriptive requirements or language that is not industry, field, purpose or application specific. We agree with the statement in the Green Paper that, "the range of services, business models, and organizational structures to which a FIPPs-based framework would apply counsel against attempting to develop comprehensive, prescriptive rules."[4]

III. Privacy Impact Assessments

The Green Paper encourages privacy impact assessments (PIAs) as a means to induce organizations to think through how their information systems or practices comport with FIPPs. The Paper also goes on to suggest that by making PIAs public, this would increase transparency by "provid[ing] consumers with a road map to an organization's collection and use of personal information."[5] While we concur that PIAs serve an important role in the management of privacy and data protection risks arising from an organization's collection, use and disclosure of personal information in innovative technologies or business processes, the IPPC has three concerns with the Green Paper's discussion of PIAs. First, in order to effectively serve the purpose of determining the privacy and data protection impact of a new technology or business process, PIAs must be tailored to the needs of particular industries and also

[3] Please see our comments of June 14, 2010, for further discussion.
[4] Green Paper at 32.
[5] Green Paper at 36.

compatible with particular companies' organizational structures. Such customization does not lend itself well to publication of PIA results in a manner that is consistent, simple or meaningful to consumers. Indeed, well drafted privacy information notices provide better transparency to consumers than publication of PIAs. Second, publication of PIAs raises a separate challenge of protecting proprietary and confidential strategic and other corporate information. Third, there are costs associated with conducting such assessments which should not be overlooked in determining the contexts in which the risks associated with a technology or information practice necessitate or justify a PIA versus those that do not. A fuller discussion of such costs and the need in this context to balance costs and benefits is warranted. For these reasons, we do not believe that the publication of PIAs should be mandated.

IV. Privacy Codes of Conduct

The IPPC supports the Department's efforts to encourage accountable industry self-regulation through industry-specific, voluntary, enforceable codes of conduct.[6] The IPPC agrees that the development of industry-specific codes of conduct can provide a means to address the data privacy issues and challenges that are specific to an industry in a way that a broadly applicable FIPPs framework simply cannot. We support the creation of further incentives to develop such codes, such as the suggested safe harbor for companies that commit and adhere to an appropriate voluntary code of conduct. We also encourage the Department to convene industry, government and other stakeholders in discussions about privacy standards and codes for industries, like the pharmaceutical industry, which are subject to multiple federal and state privacy laws and regulations, including, but not limited to those related to commercial data privacy.

V. Global Interoperability

Many IPPC member companies have substantial operations in foreign jurisdictions with comprehensive privacy and data protection laws that impose administrative obstacles to the movement of personal information even where organizations maintain accountability for that data as it crosses country borders. We support increased cooperation by the U.S government with data protection regulators in other countries to further accountability-based global movement of personal information and to facilitate global trade. We encourage multifaceted approaches that address the unique needs of industries subject to multiple overlapping, and often conflicting, laws and regulations in multiple domestic and foreign jurisdictions.

VI. National Security Breach Notification Requirement

The IPPC agrees with commenters who have argued in favor of a national security breach notification requirement that preempts state laws.[7] As noted by such commenters, monitoring the ever-shifting 'patchwork' of breach notification laws creates a significant compliance burden. Moreover, the differences in state laws mean that businesses must either treat consumers differently based on where they reside – which may lead to confusion among consumers – or businesses must attempt to comply nationally with the most stringent state standard. This latter option can lead to over-notification, i.e., notification in circumstances that the majority of states do not even consider a "breach," resulting in consumers receiving notification in circumstances in which there is little or no risk of harm. Thus, allowing state legislatures to experiment in this area leads to impacts that are felt by consumers in other states. The IPPC therefore supports the Green Paper's recommendation that "consideration should be given to a comprehensive commercial data security breach framework for electronic records that includes notification provisions,"[8] provided such a framework would harmonize requirements across all 50 states.

[6] Green Paper at 41-51.
[7] Green Paper at 57.
[8] Green Paper recommendation #7 at 57.

A breach notification requirement should be triggered only where there is a significant risk of harm resulting from the breach.

We thank you for your consideration of our comments and would welcome the opportunity to discuss these issues with you. Please do not hesitate to contact us with any questions.

Sincerely,

Peter Blenkinsop
Secretariat and Legal Counsel

APPENDIX A: INTERNATIONAL PHARMACEUTICAL PRIVACY CONSORTIUM

MEMBERS

The IPPC is an association of companies that face worldwide responsibility for the protection of personal health information and other types of personal data. Members of the IPPC include:

- Abbott Laboratories
- AstraZeneca
- Baxter International
- Bristol-Myers Squibb
- Elan Pharmaceuticals, Inc.
- Eli Lilly and Company
- GlaxoSmithKline
- Merck & Co., Inc.
- Novartis
- Pfizer Inc.
- Genentech (Roche)
- Sanofi-aventis
- Takeda Pharmaceuticals

MISSION

The IPPC was formed in 2002 to promote responsible privacy and data protection practices by the research-based, global pharmaceutical industry. Maintaining data confidentiality and subject privacy are essential to clinical research, pharmacovigilance, and other activities of the pharmaceutical industry. The IPPC seeks to increase awareness of privacy and data protection issues and to engage government in a dialogue about the need for data to support cutting edge biomedical research and other public health activities. The IPPC pursues opportunities to collaborate with government and other stakeholders to develop data protection practices that enhance data subject privacy.

GOALS

The IPPC goals are to:

- Engage government and stakeholders in the biomedical research and healthcare communities in a constructive dialogue on significant issues of privacy and data protection.
- Serve as a resource for sound analyses of privacy and data protection requirements and compliance tools tailored to the pharmaceutical industry.
- Serve as a forum for industry dialogue and promote responsible privacy and data protection practices.
- Promote consistent privacy and data protection standards that can be achieved on a worldwide basis.
- Remain on the leading edge of privacy and data protection.

SCOPE OF ACTIVITIES

The IPPC advances understanding of existing and emerging data protection and security rules in Europe, the US, and other key countries. The Consortium engages regulators and policymakers in the following areas:

- Biomedical research
- Pharmacovigilance
- Sales and marketing
- Market research
- Human resources programs
- Other corporate programs

APPENDIX B: PRIVACY GUIDELINES FOR MARKETING TO U.S. CONSUMERS

This document sets forth voluntary privacy guidelines for marketing by pharmaceutical companies to U.S. consumers. These guidelines are aspirational in nature. Companies endorsing this document aim to follow these guidelines in their day-to-day business operations in connection with the collection, use, disclosure, and maintenance of written and electronic personal information that identifies an individual consumer and is retained by a company for marketing purposes. These companies also take steps to ensure that vendors who may communicate with consumers on their behalf comply with these guidelines or applicable privacy and data protection laws.

I. NOTICE

1. When personal information is collected directly from consumers, inform those consumers about:

   (a) the identity of the entity collecting the information;

   (b) the purposes for which the information is being collected;

   (c) the types of third parties to whom the information may be disclosed; and

   (d) where provided, the means by which consumers can access and amend personal information about themselves.

2. Where the means by which personal information is being collected is not obvious (e.g., passive or automatic collection of information through website tracking), include a notice of this fact in a privacy statement.

3. When personal information about a consumer that will be used to market to that consumer is received from a third party, obtain assurances from that third party that notice was provided to the consumer and that appropriate permissions were obtained to share the personal information with the pharmaceutical company.

II. PERMITTED USES AND DISCLOSURES

1. Limit uses of personal information collected or received to:

   (a) those that are compatible with the purposes indicated in the notice given. Maintain processes to enable consumers to withdraw permission (opt-out) at any time and process such requests within a reasonable timeframe;

   (b) those that have been subsequently authorized by the consumer;

   (c) those that are necessary to comply with a legal or ethical obligation;

   (d) those that are necessary to ensure compliance with applicable laws and to detect and prevent inappropriate acts or practices, or to investigate, make or defend a legal claim; and

   (e) those that have been requested by governmental authorities.

2. Limit disclosures of personal information collected or received to:

(a) others working for or on behalf of the company;

(b) others with whom the company jointly markets products or services;

(c) those that are compatible with the notice given at the time the information was collected;

(d) those that are incidental to permissible uses of the information;

(e) third parties to whom the consumer has authorized disclosure;

(f) in the event of a sale or transfer of the business, successors and assignees;

(g) those that are necessary to investigate, make or defend a legal claim; and

(h) those that have been requested by governmental authorities or compelled by legal process.

III. ACCESS AND AMENDMENT

When contacted by a consumer who has provided appropriate verification of his or her identity with a specific request related to personal information, work reasonably with that individual to address his or her specific concern.

Circumstances that may prevent a company from fully complying with an individual's request include those that would:

- affect the company's ability to comply with a legal or ethical obligation;
- affect the company's ability to detect and prevent inappropriate acts or practices, or to investigate, make or defend a legal claim;
- result in the disclosure of proprietary information; or
- result in the disclosure of personal information of other individuals.

IV. SECURITY

1. Take reasonable precautions to protect personal information from loss and misuse, as well as unauthorized access, disclosure, alteration and destruction, commensurate with the sensitivity of the information processed.

2. Obtain assurances from vendors that they will protect personal information from loss and misuse, as well as unauthorized access, disclosure, alteration and destruction, commensurate with the sensitivity of the information processed, and that they will promptly notify the company of security incidents involving personal information.

3. Promptly investigate security incidents involving personal information and provide appropriate notice in accordance with applicable law.

V. ENFORCEMENT

1. Employ appropriate measures to receive and, as appropriate, respond to privacy complaints and requests.

2. Adopt appropriate measures and take corrective actions against employees who are found to have violated company privacy policies. Take appropriate corrective actions against agents who have violated privacy policies or law.