



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](http://www.pharmaprivacy.org)

---

February 18, 2011

Mr. Donald S. Clark  
Secretary  
Federal Trade Commission  
Room H-135 (Annex P2)  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

**Re: File No. P095416 - Bureau of Consumer Protection Preliminary Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers**

Dear Mr. Clark:

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.<sup>1</sup>

We applaud the Commission's effort to address evolving privacy considerations raised by the rapid growth of innovative new technologies and business models, and we appreciate this opportunity to present our views on the Proposed Framework for Protecting Consumer Privacy. Specifically, we will address the following issues:

- 1) the scope of application of the Proposed Framework;
- 2) the scope of "sensitive" information and the means of obtaining affirmative consent;
- 3) the adequacy of privacy information notices;
- 4) what is "reasonable" access;
- 5) substantive privacy protections and the concept of "specific business purpose";
- 6) when "choice" need be provided; and
- 7) the benefits of data collection and use.

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 FTC's review of and feedback on these guidelines.

Finally, many members of the IPPC are also members of the Pharmaceutical Research and Manufacturers of America (PhRMA), and we have therefore had the opportunity to review PhRMA's comments on the Proposed Framework. We fully support PhRMA's comments.

---

<sup>1</sup> For further information concerning the IPPC, please visit our website at [www.pharmaprivacy.org](http://www.pharmaprivacy.org). All Appendices referenced in this comment, and additional documents adopted by the IPPC, are publicly available on this website.

## I. Scope of Application of the Framework

### *Application to Non-PII*

The Proposed Framework would apply to all data that can be “reasonably linked to a specific consumer, computer, or other device.” This not only is a significant expansion of the traditional distinction between personally-identifiable information (PII) and non-PII, we believe that such a scope may have the unintended consequence of applying privacy standards to data, computers and devices that have nothing to do with people. Many IPPC companies have substantial experience in implementing the requirements of comprehensive privacy and data protection laws in other countries. As a result, we recognize the distinction that must be made between computers and devices that process data that have nothing to do with people, such as data about inventories, supplies, equipment and property. Application of privacy standards designed to provide transparency to people and to protect people from privacy-related harms has no relevance to data, computers and devices that are not about people or likely to be used by or associated with people. A similar problem with the Proposed Framework relates to computers or devices that may be used by many (perhaps even hundreds or thousands) of unidentified users. In circumstances in which a specific computer or device is not associated with a specific user or discrete set of users, it is unclear what privacy risks warrant the application of protections to data that can be linked to such computer or device. For example, it is unclear why privacy protections should be applied to data associated with a specific hospital medical device in the absence of other publicly available data linking such device to specific patients.

The report states that the proposed scope “encompasses a more modern approach that is reflected in recent Commission initiatives” and then cites the FTC’s Health Breach Notification Rule and the Staff Report on Self-Regulatory Principles for Online Behavioral Advertising (“OBA Report”) as examples of such initiatives.<sup>2</sup> In fact, however, the proposed scope of application would represent a significant expansion beyond both the Health Breach Notification Rule and the OBA Report. First, the Health Breach Notification Rule applies to breaches of unsecured health information “that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.”<sup>3</sup> We are unable to see how the Breach Notification Rule serves as precedent for the expansion of privacy protections to data that can be linked to a specific computer or device but not an individual consumer. While the OBA Report is more on point, its context relates to the privacy risks associated with the collection of data on the user(s) of a computer or device in order to deliver personalized content back to that computer or device.

Accordingly, the IPPC urges the Commission to narrow the scope to data that reasonably can be used to identify an individual consumer. Where data can be identified principally only through access to a confidential key or some other reference dataset whose disclosure is limited by law or contract, the risk of re-identification is low. We believe the risk of data re-identification must be weighed against the beneficial uses of that data. Thus, for example, we believe that the public interest in advances in medical science warrants permitting pseudonymized (or partially de-identified) data to be used for biomedical research even though there may be some small risk that the data could be re-identified by a researcher.

### *Relationship to Sectoral and Other Specialized Privacy Laws*

The application of the Proposed Framework to data collection and use in areas already covered by sector-specific privacy laws is unclear. 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

---

<sup>2</sup> Proposed Framework at 43.

<sup>3</sup> See definitions of “breach of security” and “PHR identifiable health information” at 16 CFR § 318.2(a) and (e).

requirements. The IPPC believes that in order to avoid inconsistencies, where sector-specific privacy requirements have already been enacted (e.g., HIPAA), the Framework should provide safe harbors for organizations that are subject to those requirements and, further, should recognize how fulfillment of those requirements satisfies the requirements of the Proposed Framework. 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 the Proposed Framework. We also support tailored alternatives that provide incentives for accountable industry self-regulation such as the industry-specific, voluntary, enforceable, FTC-approved codes of conduct proposed by the Department of Commerce.<sup>4</sup>

Similarly, the IPPC is uncertain as to how the Proposed Framework would apply to other areas that are already covered by specialized privacy laws. For example, the Children's Online Privacy Protection Act (COPPA) already applies to information on children under age 13, and both Congress and the FTC have separately considered the merits of extending COPPA protections to teenagers.<sup>5</sup> The IPPC believes that the Framework should provide Safe Harbors for organizations that are in compliance with such specialized privacy laws.

#### *Application to Biomedical Research and Public Health Activities*

In our comments to the FTC dated April 14, 2010, we urged the Commission 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. However, the Proposed Framework is silent on the issue of whether it would apply to biomedical research and public health activities. There may be unintended consequences of including biomedical research and public health activities within the scope of the Framework. For example, the re-use of personal information by health care providers, organizations and researchers can be important to improving health care quality, reducing costs, and developing new treatments and other forms of health innovation, but the Framework's emphasis on purpose limitation<sup>6</sup> could hinder these important secondary uses. We therefore wish to reiterate our position that these areas 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*.<sup>7</sup>

## **II. Scope of "Sensitive Information" and Means of Obtaining Affirmative Consent**

The report states that certain types of sensitive information warrant special protection, such as information about children, financial and medical information, and precise geolocation data. The FTC requests comment on the scope of "sensitive information" and the most effective means of obtaining affirmative consent to the collection and use of sensitive information. The IPPC believes that health information combined with demographic information alone, such as gender and age, should not be considered sensitive information unless it is linked to a specific identifiable individual. While it is true that demographic information and certain health conditions may be statistically correlated (e.g., breast cancer is more common in women than men), the privacy risks associated with the use and disclosure of such information are generally minimal and certainly do not rise to the level of risks associated with a diagnosed medical condition.

---

<sup>4</sup> See The Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (2010) at 41-51.

<sup>5</sup> See, e.g., Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 75 Fed. Reg. 17,089.

<sup>6</sup> See Proposed Framework at 76-77 [is this the right reference or should we reference pages 45-46?].

<sup>7</sup> Please see our comments of April 14, 2010, for further discussion.

The IPPC also requests clarification of how the principles are intended to apply in the context of requests for information about medical conditions and treatments. Pharmaceutical companies frequently receive such requests not only from patients, but also from physicians and other caregivers, as well as concerned family and friends. Are all such inquiries to be treated as relating to sensitive information? If a company does not know the type of individual making the inquiry, presumably the principles related to sensitive information would be inapplicable because a medical privacy interest would not be triggered?

It is important that the Framework remain flexible with respect to permissible means of obtaining affirmative consent to the collection and use of sensitive information. For example, requests for health and treatment information may be made via postal mail, through the internet, or by phone call, so both written and verbal consent must be valid. Moreover, pharmaceutical companies should be permitted to respond to requests made by caregivers, family or friends for information to be sent to a patient without first having to confirm that the patient in fact consents to being sent such information.

### **III. Privacy Information Notices**

There is an inevitable tension between the Commission'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. As a hortatory exercise, 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 Commission 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 mandating overly detailed language that is not industry, field, purpose or application specific. For this reason, we have significant concerns regarding the feasibility of standardizing privacy notice language across industries.

### **IV. Providing Reasonable Access**

The Proposed Framework states that "if implemented properly, taking into account the costs and benefits of access in different situations, access could significantly increase the transparency of companies' data practices without undue burden."<sup>8</sup> The Framework then goes on to suggest that where a company maintains data to be used for authentication or decision-making purposes, it may be appropriate to provide access to the actual data; however, where companies maintain data solely for marketing purposes, they may choose to disclose only the categories of consumer data they possess and to provide a suppression right that allows consumers to be removed from marketing lists. The IPPC agrees that the degree of consumer access (i.e., access to actual data versus access to the categories of data maintained) should depend upon the purposes for which the data are maintained.

Unless a company already possesses sufficient data in order to be able to authenticate the identity of a consumer requesting access, providing an access right to actual data would create a significant privacy risk. The IPPC therefore agrees that it is safer for such companies to only disclose the categories of information they maintain in response to access requests rather than disclosing actual data. Otherwise, companies would be forced to gather and maintain additional information on consumers so as to be able to authenticate requestors' identities. Further, it must also be noted that the administrative burdens and associated costs to companies of responding to access requests can be significant. This is

---

<sup>8</sup> Proposed Framework at 73-74.

particularly true in the case of decentralized systems and databases. We believe these costs also support a "sliding scale" of consumer access rights.

## **V. Substantive Privacy Protections and Specific Business Purpose**

The IPPC supports a "Privacy by Design" approach to ensuring that privacy protections are systematically embedded into organizational business practices. We concur that data security, data integrity, and data quality are important substantive privacy protections. Consistent with the concerns we raised in Part I of our comments, we believe that limiting collection of personal information to a specific business purpose may impede important uses of personal information for public health and health care innovation purposes. Organizations should be able to collect information for more than a single business purpose. Important biomedical and health innovations may be developed from scientific hypotheses and strategies that are formed only after further analyses of data following other biomedical research discoveries or health outcomes findings. We believe these are legitimate business needs for which data should be retained. We encourage the Commission to consider the principle of privacy accountability as a comprehensive programmatic mechanism for organizations to protect personal information. This may provide accountable organizations greater flexibility in retaining and using data for secondary purposes that provide important biomedical, health and other advances for society.<sup>9</sup>

## **VI. Choice**

The IPPC supports the Commission's efforts to simplify consumer choice. We agree that consumer choice need not be provided before collecting and using consumer data for certain commonly accepted practices, including fraud prevention and legal compliance. For example, pharmaceutical companies are required to report to the FDA adverse events associated with their products of which they become aware and for which there is (i) an identifiable patient; (ii) an identifiable reporter; (iii) a specific drug or biologic involved in the event; and (iv) an adverse event or fatal outcome. Requiring pharmaceutical companies to obtain consumer consent before collecting and reporting such adverse event information would present a conflict of laws and could have serious public health consequences. However, the IPPC also believes this example illustrates the importance of considering commonly accepted practices that may be industry-specific in addition to certain uses that may be commonly accepted across industries.

In the context of first-party marketing, the IPPC believes that the consumer's affirmative choice can be presumed. For example, when a consumer visits a pharmaceutical web site seeking information on a product or condition, it can be presumed that the consumer consents to the collection of that information which is necessary to deliver the information or respond to the request. Imposing an additional requirement for express consent – just because information deemed "sensitive information" may be involved" – would hinder the ability of consumers and pharmaceutical companies to interact and communicate, and would thus present an untenable restriction of First Amendment rights.

The IPPC additionally supports an interpretation of "first-party" which provides companies with flexibility in determining how to structure their business operations. A group of commonly affiliated companies ought to be permitted to share personal information for first-party purposes, including sharing information among affiliates globally, if they have held themselves out to the consumer as a single entity through common branding or other techniques. How a company holds itself out to consumers plays a more important role in the creation of consumer expectations than a corporation's formal legal structure. Of course, the scope of any opt-out options provided to the consumer ought to mirror any express or presumed consent (in addition to possibly providing more granular options) so that a consumer can just as easily opt-out of a use of information as opt-in.

---

<sup>9</sup> See Bruening, P. Accountability: Part Of The International Public Dialogue About Privacy Governance. *World Data Protection Report* 10/10 (2010).

Another situation in which uses and disclosures of personal information should be permitted as a "commonly accepted practice" relates to mergers and acquisitions. When a consumer registers to receive information about a product or service, the consumer expects to continue to receive such information regardless of whether the product or service is provided by Company A or successor Company B. The FTC should add to its list of "commonly accepted practices" disclosures of personal information to successors-in-interest of a product or service (through merger or acquisition) and subsequent uses and disclosures of personal information by such successors-in-interest, to the extent these uses and disclosures would have been permitted by the prior entity and the successor entity is in a related market. This is consistent with the FTC settlement agreement reached in the Toysmart bankruptcy case, which prohibited Toysmart from selling its customer list as a stand-alone asset but permitted the disclosure of the list to a buyer in a related market as a package along with the web site to which the customer list related.<sup>10</sup>

The IPPC agrees with the Commission's opinion that online contextual advertising should also fall with the "commonly accepted practices" category.<sup>11</sup> As stated in the Proposed Framework, such advertising is transparent to consumers and presents minimal privacy intrusion as compared to other forms of online advertising. For example, consumers understand and expect that if they enter a search query for a disease or condition, treatment options for such disease or condition may be presented on the page showing search results.<sup>12</sup>

The IPPC supports the Commission's aims to improve consumer choice in connection with online behavioral advertising; however, we urge the Commission to further these aims through flexible means that encourage widespread adoption of self-regulatory standards that can readily adapt to innovative changes in technology and business models. We believe more time is needed to evaluate the adoption and effectiveness of industry self-regulation (such as the Self-Regulatory Program for Online Behavioral Advertising developed by the Direct Marketing Association and other industry associations) prior to further consideration of a universal "Do Not Track" mechanism. Moreover, further examination of how Do Not Track technologies can be implemented while still enabling consumers to make granular choices is necessary before mandating such a mechanism.

## **VII. Benefits of Data Collection and Use**

The Proposed Framework provides only a cursory overview of the benefits of data collection and use. In comparison to the extensive discussion of privacy risks throughout the paper, the reader is left with the impression that the risks are great while benefits few. A more balanced discussion is needed. In the pharmaceutical context, data collection and use are essential to provide consumers and caregivers seeking information on medical diseases, conditions and treatments with the information they seek. This may occur, for example, in online interactions, over the phone, or at health fairs and clinics. As the report is focused almost entirely on the online space, we will do so here as well.

A 2009 survey by the Pew Research Center found that 61% of American adults (83% of Internet users) look for health information online.<sup>13</sup> 42% of all adults say that they or someone they know has been helped by following medical advice or health information found on the internet.<sup>14</sup> Nevertheless, the internet supplements but does not replace the advice of health professionals. 86% of Americans still ask

---

<sup>10</sup> See <http://www.ftc.gov/opa/2000/07/toysmart2.shtm>.

<sup>11</sup> Proposed Framework at fn. 55.

<sup>12</sup> We recognize that such advertising may in some circumstances raise other, non-privacy issues, such as the appropriate presentation of fair balance of benefit and risk information, and we look forward to the Food and Drug Administration's guidance on internet and social media promotion, expected to be published in the first quarter of 2011.

<sup>13</sup> Susannah Fox & Sydney Jones, Pew Internet and American Life Project, *The Social Life of Health Information --Americans' Pursuit of Health Takes Place Within a Widening Network of Both Online and Offline Sources* 4 (June 2009).

<sup>14</sup> *Id.* at 7.

a health professional when they need health information.<sup>15</sup> For prescription drugs, information found online serves to encourage open patient-physician communications, but it is the healthcare provider who ultimately determines what to prescribe based on his or her professional judgment.

Healthcare outcomes are improved when patients are engaged in their treatment program. Informed consumers are more likely to recognize disease symptoms and to seek appropriate care. In turn, informed patients are more likely to adhere to physician-prescribed treatment regimens. Appropriate, proactive, and consistent use of prescription medications helps individuals to lead healthier lives and can prevent or delay the need for more costly medical services and procedures. Pharmaceutical companies play an important role in the healthcare system not only by manufacturing prescription drugs and devices but also by serving as an informational resource for interested patients and physicians. Online media serve these goals in the following ways:

- **Empower Patients with Information.** Consumers who recognize disease symptoms and understand treatment options can more effectively seek appropriate care and make better-informed health decisions in consultation with their health care providers. Heightened awareness of available therapies and their benefits, risks and side effects of these therapies, empowers patients to work with their physicians to make important decisions about their healthcare.
- **Encourage Patients to Communicate with Physicians.** Pharmaceutical company communications about prescription drugs encourage patients to consult with their physicians about health conditions to determine what treatment options are available.
- **Decrease Patient Inhibitions in Addressing Sensitive Conditions.** Consumer-directed information about available prescription therapies encourages patients to speak with health care providers about their medical symptoms and treatment options. Patients who suffer from medical problems that may carry a social stigma or historically have been viewed as too personal to discuss with a physician are now, as a result of greater information, education, and understanding, more likely to discuss with their physicians their symptoms and possible treatments.
- **Promote Improved Medication Compliance.** Medication non-compliance is a significant public health concern – it has a negative impact on patients' health and significantly raises healthcare costs. Direct-to-consumer prescription drug advertisements prompt patients to take their medicine regularly and refill prescriptions as necessary.

Pharmaceutical manufacturers communicate this information both directly through manufacturer-controlled web-based media and indirectly through advertising on independent or manufacturer-supported web-based media. Data collection and use are necessary to communicate effectively with consumers and caregivers who go online seeking information. Simply put, the internet is not a static medium. Instead, it allows for an interactive experience between the user and site operator, and among many users of the same site. This may occur, for example, through online tools that enable users to enter symptoms and in turn receive information on possible causes. Or it may occur through online and mobile tools that enable users to keep track of their symptoms and other health markers on a daily basis. Or it may occur via a user's registration to receive further information about a product or condition, or to sign up to receive a periodic newsletter. Along the same lines, social media have allowed for the creation of support groups and patient communities so that those suffering from or caring for someone with an illness can obtain information, advice and encouragement.

---

<sup>15</sup> Id. at 15.

Mr. Donald S. Clark, Secretary  
Federal Trade Commission  
February 18, 2011  
Page 8

We recognize that there are some who idly dismiss such activities as commercially-motivated enterprises. Nevertheless, we reject the notion that a pharmaceutical company's efforts to increase patient and caregiver awareness of products and services are incompatible with patient and caregiver efforts to obtain accurate, balanced and truthful information about health conditions and treatment options. Pharmaceutical manufacturer support of and advertising on third-party web sites help to sustain the economic viability, and thus availability, of those sites. Pharmaceutical advertisements are regulated by the Food and Drug Administration to ensure that the content is truthful, scientifically accurate, and contains an appropriate balance between benefits and risks. Indeed, information provided by pharmaceutical companies in the form of labeling and advertising is the only FDA-regulated promotional information about prescription medicines online. We do not see any privacy harms associated with third party health web sites using information about the profiles of their users to select the advertisements and promotional content that is most suited to their needs and interests, provided such uses are clearly disclosed to users at the point of data collection.

---

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,

A rectangular box with a thin red border, used to redact the signature of Peter Blenkinsop. The box is empty, with only a small black speck visible near the top center.

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.