PhRMA

February 17, 2011

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Office of the Secretary
Room H-113
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Preliminary FTC Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

Dear Secretary Clark:

The Pharmaceutical Research and Manufacturers of America (PhRMA) is pleased to submit these comments in response to the Federal Trade Commission's preliminary staff report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policy Makers* (Report).[1] PhRMA is a voluntary non-profit association that represents the country's leading pharmaceutical research and biotechnology companies, which are dedicated to developing medicines that allow patients to live longer, healthier, and more productive lives. In 2009, America's pharmaceutical research and biotechnology companies invested $65.3 billion in the research and development of new life-changing medicines.

PhRMA commends the Commission staff's effort to create a privacy framework that sets guidelines for the collection and use of consumer data while preserving the beneficial uses of these data. As the Report suggests, although the recent increase in consumer data collection and use has given rise to concerns among some consumers, the benefits of data collection and use are undeniable. Nowhere are these benefits more evident than in the area of health care. From enabling essential research and development of innovative, and often lifesaving, medicines to empowering consumers to make informed choices about their health care, exchange of information is essential to the continued vitality of health care in the United States. The challenge we all face is to promote the free flow of information that has been vital to the development of medical interventions while appropriately safeguarding the privacy of health care consumers.

As PhRMA and its member companies have long recognized and demonstrated, the benefits that stem from the free flow of health information do *not* have to come at the expense of consumers' privacy. Because we understand that consumers have heightened expectations of privacy when it comes to information about their health, we hold ourselves to high standards in order to protect their privacy. Accordingly, biopharmaceutical companies have

---

[1] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICY MAKERS (2010) [hereinafter STAFF REPORT].

incorporated robust privacy protections into the research, development, and marketing of our products. As PhRMA's members develop innovative products that improve patients' lives, we are constantly striving to be innovative in the protections we afford to consumer information.

As we describe in more detail below, PhRMA believes that the Report offers important concepts for a privacy framework, but we strongly believe that any framework must be sensitive to the fact that achieving the appropriate balance between protecting privacy and promoting the beneficial use of consumer data may require different measures in different industries. For example, any approach to protecting consumer privacy in the area of health care must recognize that a robust privacy framework is already in place—specifically, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the privacy and security regulations promulgated under HIPAA—and ensure that entities are not subject to redundant or conflicting obligations.

Because different industries face distinct challenges in protecting consumer privacy, PhRMA believes that any privacy framework should provide for the development of industry-specific self-regulatory codes. This is the approach recommended by the Department of Commerce in its recently released green paper on protecting online privacy.[2] As the Commerce paper suggests, an incentive for industries to develop these codes could be the provision of a safe harbor from FTC enforcement for those companies that commit and adhere to a code that meets certain requirements, such as FTC approval.[3] PhRMA believes such codes could provide much-needed concrete guidance for businesses while addressing consumer needs in a context-sensitive manner. As an example, PhRMA's *Code on Interactions with Healthcare Professionals* provides relevant, industry-specific direction to member companies for greater self-regulation.[4]

We elaborate on PhRMA's recommendations and provide additional comments on the Report below. We would be pleased to provide the Commission staff with additional information about any of these comments. In addition, PhRMA also supports the comments filed by the International Pharmaceutical Privacy Consortium (IPPC).

---

[2] *See* DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 41-51 (2010) [hereinafter GREEN PAPER].

[3] *Id.* at 43-44.

[4] : In 2008 PhRMA revised its *Code on Interactions with Healthcare Professionals* ("PhRMA Code"). This revised PhRMA Code reinforces prior industry-specific guidance, indicating that "[i]n interacting with the medical community, [industry members] are committed to following the highest ethical standards as well as all legal requirements." The PhRMA Code "is based on the principle that a healthcare professional's care of patients should be based, and should be perceived as being based, solely on each patient's medical needs and the healthcare professional's medical knowledge and experience."

I. Background: The Benefits of Health Information and FDA's Regulation of Biopharmaceutical Promotion

Biopharmaceutical manufacturers provide a significant amount of the health, medical, and pharmaceutical information available to health care professionals and patients, both through traditional means (print, broadcast, and in person) and online. In particular, biopharmaceutical companies provide information about clinical trials (including eligibility information for patients who would like to participate in clinical trials) and detailed information about which medicines are indicated for specific patients; how patients should take these medicines; what side effects patients may expect; and any warnings, precautions, and contraindications. Biopharmaceutical companies also offer detailed information about disease states and alternative treatments, including non-drug options; dietary and nutritional guidance; coupons, discount programs, and other money-saving opportunities; persistence and compliance programs; online communities and discussion forums; and other resources for patients and health care professionals alike. Given these important public health activities, it is important for biopharmaceutical companies to be able to evaluate the effectiveness of different routes of communication and to make use of appropriate methods to publicize health related information.

As people are turning to the Internet to find health information in unprecedented numbers, health care providers, researchers, government agencies, and biopharmaceutical companies are providing increasing amounts of information using online and other new media tools. According to a recent survey by the Pew Research Center, eight in ten internet users (59% of all adults) look online for health information, making it the third most popular online activity behind email and using search engines.[5] Moreover, 66% of internet users look online for information about a specific medial treatment or procedure, while 24% look for information about medicines such as drug safety.[6] Importantly, Pew also concluded that the typical search for health information online was conducted *on behalf of someone else*; thus, "the impact of their inquiries may be much broader."[7] Accordingly, one of the goals of the Department of Health and Human Services' (HHS) Healthy People 2010 initiative is to increase internet access, because "access to the Internet and subsequent technologies is likely to become essential to gain access to health information, contact health care organizations and health professionals, receive services at a distance, and participate in efforts to improve local and national health."[8]

---

[5] SUSANNAH FOX, PEW INTERNET AND AMERICAN LIFE PROJECT, HEALTH TOPICS -- 80% OF INTERNET USERS LOOK FOR HEALTH INFORMATION ONLINE 5 (Feb. 2011) *available at* http://pewinternet.org/Reports/2011/HealthTopics.aspx [hereinafter "PEW SURVEY"].

[6] *Id.* at 2.

[7] *Id.* at 8.

[8] Dep't of Health & Human Servs., Healthy People 2010 vol. 1, ch. 11, "Health Communication," *available at* http://www.healthypeople.gov/2010/Document/HTML/Volume1/11HealthCom.htm.

The Internet has also proven to be a powerful way for biopharmaceutical companies to obtain the concerns and views of health care professionals and patients that will benefit patient care and access to new medicines. Biopharmaceutical companies use information collected online to supplement market research, clinical data and other advisory opinions to monitor drug safety, refine educational materials, design or improve support programs and to develop important research programs and studies. The collection of consumer health information, both on- and off-line, is vital to research and development, tracking drug resistance patterns and disease progression, compliance with FDA information requirements, correlating patient compliance with specific outcomes, and aiding law enforcement. Important as this information is, however, PhRMA and its member companies recognize that collection of consumer information—particularly health information— may raise privacy concerns among certain consumers. For this reason, PhRMA's member companies collect and use consumer information only for limited purposes—such as those enumerated above—and take steps to protect consumer privacy by, for example, anonymizing data (where appropriate) and providing reasonable security for any data collected.

It is important to recognize that the FDA administers a strict regulatory scheme for all promotional labeling and advertising for prescription medicines by ensuring that such information provided to health care professionals and patients is scientifically accurate and not misleading.[9] Improper promotion by a drug manufacturer can cause a prescription drug to be deemed "misbranded," and if the product has been introduced into interstate commerce, such promotion could trigger enforcement action by the agency.[10] These requirements apply to diverse forms of promotion and advertising, including on websites and other online forums.

As FTC staff may be aware, in November 2009 the FDA held a two-day public meeting to discuss promotion of FDA-regulated drugs and devices online and the use of social media tools.[11] In addition, the agency is drafting guidance on promotion and safety issues involving the Internet and social media. FDA also regulates all labeling for over-the-counter (OTC) drugs, but it does not have jurisdiction over OTC drug advertising. Instead, the FTC oversees these advertisements under section 5 of the FTC Act, which declares "unfair or

---

[9] The Federal Food, Drug, and Cosmetic Act (FDCA) defines "labeling" to mean any written, printed, or graphic material upon or accompanying a drug. 21 U.S.C. § 201(m). This includes the FDA-approved prescribing information, sometimes called the "professional labeling." It also includes "promotional labeling," such as brochures, sales aids, exhibit panels, direct mail pieces, professional or patient education materials, promotional speaker slide decks, and many other materials disseminated by or on behalf of the product's manufacturer. Advertising includes both printed and broadcast advertising.

[10] 21 U.S.C. §§ 352(a), (f), (n).

[11] See transcript and presentations at http://www.fda.gov/aboutfda/centersoffices/cder/ucm184250.htm.

deceptive practices to be unlawful" and section 12 of the FTC Act, which prohibits the dissemination of false and misleading drug advertisements.[12]

Both FDA and the FTC have acknowledged the importance of the flow of information between biopharmaceutical manufacturers and patients and health care professionals.[13] In requesting comments on First Amendment issues related to claims made in drug labeling and advertising, FDA in 2002 explained that "[r]ecent years have witnessed increased attention by consumers to their own medical care. The public's interest in, and access to, useful and truthful information about medical products have skyrocketed."[14] FDA characterized this development as "generally positive" but noted that it "presents unique challenges to the FDA, which regulates a wide range of both products and words."[15] In responsive comments, the FTC explained that a

> flexible approach to commercial speech—one that encourages the dissemination of accurate speech and tailors restrictions to prevent speech that is false or misleading—will result in greater dissemination of valuable information with benefits for both consumers and competition. In contrast, the evidence indicates that broad restrictions on the dissemination of truthful commercial speech, while effectively stopping false or misleading information, can deprive consumers of useful information as well.[16]

The FTC also described how FDA's current approach to direct-to-consumer (DTC) advertising of prescription drugs[17] has led to an increase in the flow of useful information

---

[12] 15 U.S.C. §§ 45, 52. Historically, FDA had jurisdiction over the labeling of all drugs, and the FTC had jurisdiction over the advertising of all drugs, but in 1962 Congress transferred regulatory authority for prescription drug advertising from the FTC to FDA by enacting section 502 of the FDCA, which states that "no advertisement of a prescription drug [shall] be subject to the provisions of section 12 through 17 of the [FTC] Act." 21 U.S.C. § 352(n). Regulatory authority for OTC drug advertising remained with the FTC.

[13] In fact, the FTC Act expressly recognizes that communications concerning drugs made "only to members of the medical profession," and meeting other requirements, are not actionable as "false advertisements" under the Act. *See* 15 U.S.C. § 55(a)(1).

[14] 67 Fed. Reg. 34942, 34943 (May 16, 2002).

[15] *Id.*

[16] Fed. Trade Comm'n, Comments of the Staff of the Bureau of Economics, the Bureau of Consumer Protection, and the Office of Policy Planning of the Federal Trade Commission, FDA Docket No. 02N-0209, at 22 (Sept. 13, 2002).

[17] The FDCA requires that prescription drug advertising contain a true statement of "information in brief summary relating to the side effects, contraindications, and effectiveness" of the drug (the "brief summary requirement"). 21 U.S.C. § 352(n). Drug manufacturers usually meet the brief summary requirement for DTC print advertisements by including in the advertisement the entire section of the FDA-approved product labeling that discusses side effects and contraindications of the drug. For broadcast DTC advertisements, however, FDA allows companies to include a "major statement" of risks and to make "adequate provision" for consumers to obtain the FDA-approved labeling for (continued...)

from drug manufacturers to consumers. According to the FTC, empirical evidence suggests that this information flow may improve consumer welfare by prompting consumers to seek out information about medications and medical conditions, some of which may not have been diagnosed previously, and by enhancing conversations between patients and their health care providers about treatment options, allowing patients to make better-informed health care decisions for themselves.[18]

Given the value of health care information that can be provided by biopharmaceutical manufacturers and the increased reliance on the Internet by both health care professionals and patients, the rapidly expanding array of online tools can be used to educate health care professionals and consumers about the appropriate use of medicines and other medical products. At the same time, PhRMA supports effective privacy policies and practices, because they are essential to protect individuals who make use of resources provided by drug manufacturers and other entities. These measures must be structured in a way that protects and enhances the flow of information from manufacturers to patients and their caregivers. Moreover, any privacy framework must respect the jurisdictional authorities of both FDA and the FTC and must complement the existing regulatory schemes of both agencies.

PhRMA offers more detailed comments on the Report below.

II. Comments on the Proposed Framework

A. Scope

The framework set out in the Report would apply to all commercial entities that collect or use information that can be "reasonably linked to a specific consumer, computer, or other device," regardless of whether that information is "personally identifiable information" (PII).[19] PhRMA has three comments about the scope of the proposed framework.[20]

---

the product. *See* FDA, *Guidance for Industry: Consumer-Directed Broadcast Advertisements* (Aug. 9, 1999), *available at* http://www.fda.gov/RegulatoryInformation/Guidances/ucm125039.htm.

[18] FTC Comments, at 31.

[19] *Id.* at 43.

[20] In addition to the following comments on the scope of the proposed framework, PhRMA also supports the International Pharmaceutical Privacy Consortium's (IPPC) recommendation that the scope be narrowed to include only data that can be reasonably linked to an individual consumer. PhRMA agrees with the IPPC that, as currently defined, the proposed framework could be understood to impose privacy requirements on data, computers and devices that have no connection to individual consumers, such as data that companies collect about inventories, supplies, equipment and property.

Harmonization of Privacy Requirements. The proposed framework appears potentially to cover entities whose data practices are currently regulated by the privacy rule promulgated under HIPAA (the "HIPAA Privacy Rule"), which is administered by HHS.[21] Although the data practices of PhRMA's member companies are not governed directly by the HIPAA Privacy Rule (because our members are generally not "covered entities" under the Rule[22]), its requirements nonetheless affect our members' practices, because biopharmaceutical companies often work with covered entities to conduct both research and commercial activities. For example, most clinical research sponsored by biopharmaceutical companies is conducted by physicians at academic medical centers, which are HIPAA-covered entities. The collection of data from research subjects must therefore comply with the HIPAA Privacy Rule, as well as FDA regulations regarding protection of data during applicable clinical trials.[23] Similarly, biopharmaceutical companies often engage pharmacies to send refill reminders to patients whose prescriptions are about to lapse; because pharmacies are covered entities, these communications which benefit healthcare treatment must comply with HIPAA.[24]

Clearly, any FTC privacy framework must be harmonized with the HIPAA Privacy Rule, applicable FDA requirements, and the various state laws governing health privacy so that companies do not face redundant or conflicting federal or state obligations. The FTC should also be cognizant of the many international privacy regulations to which PhRMA's member companies are subject and, to the extent possible, should seek to harmonize any framework with those regulations. Moreover, PhRMA believes that Commission staff should be cognizant of the potential for consumer confusion stemming from additional regulation of privacy in the health care industry. For example, much of the health information collected by HIPAA-covered entities for research purposes is collected pursuant to a HIPAA authorization that is completed by the person providing the information. If the Commission were to require different or additional authorization for the use of that person's information, the process could become unduly complicated, diminishing the likelihood of informed choice.

Given the important public health issues at stake regarding communication of health-related information, the existence of related laws and guidances, and resource constraints,

---

[21] Entities covered by these federal regulations often must also comply with various state laws regulating health privacy. *See, e.g.*, Cal. Civ. Code §§ 56–56.37 (governing the use and disclosure of medical information by providers of health care, among other entities); Tex. Health & Safety Code Ann. §§ 181.001–181.205 (imposing restrictions on the use and disclosure of protected health information by health care providers, among other entities).

[22] Under HIPAA, covered entities are health care providers that conduct electronic transactions for which a standard has been adopted under HIPAA, health care clearinghouses, and health plans. 45 C.F.R. § 160.102.

[23] *See, e.g.*, 21 C.F.R. § 56.111(a)(7) (specifying that institutional review boards (IRBs) must ensure adequate protection of patient health care information in clinical trials).

[24] Biopharmaceutical companies that offer refill reminder programs do *not* typically receive access to identifying information about patients who participate in the programs unless a patient explicitly allows such access via an opt-in consent mechanism.

we strongly urge FTC staff to leverage the expertise of other agencies, such as HHS and FDA, in creating a framework that recognizes the distinct challenges to protecting health information privacy[25].

Industry-specific Factors and Consumer Expectations. A single framework covering all entities engaged in the collection or use of consumer data may not be the most effective way to ensure consumer privacy while promoting the beneficial use of information. The Report states that such broad coverage is necessary because consumers are "generally unaware of the number of online and offline entities that collect their data, the breadth of the data collected, and the extent to which data is shared with third parties[.]"[26] PhRMA agrees that all entities that collect, use, or maintain consumer information share responsibility for the appropriate protection of that information. But given the diversity of those entities—and the different expectations of privacy consumers bring to their relationships with them—a single framework risks being too broad to provide meaningful guidance to a diverse range of businesses and meaningful protections to consumers. For example, the Report's suggestion that consumers be given the opportunity to exercise choice regarding data collection and use that is not "commonly accepted"[27] means very little in an era in which consumers' expectations of privacy are constantly evolving and vary widely according to the context in which their data are being collected or used. A broad requirement such as the one proposed could create uncertainty among businesses, stifling the innovative use of data for beneficial purposes.

A single framework may also be insufficiently sensitive to the needs of consumers. For example, the proposed framework contains a requirement that privacy notices become more standardized so that consumers may compare the privacy practices of different

---

[25] HHS and the FTC recently engaged in this type of interagency cooperation in promulgating breach notification rules for electronic health information pursuant to the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"). *See* Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (Aug. 24, 2009) (codified at 45 C.F.R. pts. 160 & 164); Health Breach Notification Rule, 74 Fed. Reg. 42,962 (Aug. 25, 2009) (codified at 16 C.F.R. pt. 318). Although each agency issued its own rule, and the two rules generally covered different kinds of entities, the agencies recognized that there could be situations where one entity could be subject to both rules. The agencies therefore worked together to harmonize the rules in order to minimize the burden on entities finding themselves in such situations. *See* 74 Fed. Reg. 42,964. As the Commission explained in the statement of basis and purpose for its rule, harmonization was also necessary for both agencies' rules to adequately protect consumers in the event of a data breach. The Commission described a possible scenario in which a "business associate" of a HIPAA-covered entity would have been required to notify its customers directly of a data breach while also notifying HIPAA-covered entities to which it provided services so that those entities could in turn notify individuals affected by the breach. *Id.* This situation might have led to consumers receiving multiple notices for the same breach. Not only would this have been a waste of resources; it also could have led to considerable consumer confusion.

[26] STAFF REPORT at 42.

[27] *Id.* at 57.

entities quickly and easily.[28] While businesses might improve the ways in which they communicate their data practices to consumers, a single standardization requirement may be inadequate to account for the different kinds of information that consumers will find important depending on the entity with which they engage. A consumer may want to know different information about the data practices of, for example, an online advertising network than about the data practices of a neighborhood grocery store (or a large chain that tracks purchases in return for discounts). In the biopharmaceutical context, companies may be required by the FDA to collect individually identifiable information to help assure drug safety; such a collection – especially if required by the government – may not easily fit into a single framework primarily designed for other purposes.

Industry-specific Codes. As an alternative to the broad single framework proposed by the Report, PhRMA proposes that staff follow the Department of Commerce's suggestion in its recent green paper on privacy and support the development of industry-specific self-regulatory codes.[29] As the Commerce paper suggests, an incentive for industries to develop these codes could be the provision of a safe harbor from FTC enforcement for those companies that commit and adhere to a code that meets certain requirements, such as FTC approval. PhRMA supports this approach. Industry-specific codes could provide much-needed concrete guidance for businesses while addressing consumer needs in a context-sensitive manner. The specificity of the codes would empower consumers through relevant and timely information, by encouraging greater and more consistent transparency among companies within specific industries regarding their data collection and management practices. At the same time, clear rules about the collection and use of consumer data would provide businesses confidence as they find innovative ways to employ consumer information responsibly. Rather than leaving it to businesses to interpret the vague terms of a one-size-fits-all framework, industry-specific codes would address the particular business practices within an industry that implicate privacy concerns.

For example, the use of anonymized, or pseudonymized (key-coded), health information is vital to our members' research and development of innovative medical treatments, but the Report's proposed framework is unclear about what protection, if any, should be given to this information. Uncertainty about the protections that apply to such data in the clinical research context could have a chilling effect on innovative research and development. An industry-specific code could set forth specific requirements around the collection, maintenance, and use of such data (*e.g.*, a requirement that those data be subject to reasonable and appropriate security requirements) that would protect consumers' privacy while allowing innovators to use consumers' data in ways that can benefit the public health. As an example, biopharmaceutical company sponsors of clinical studies should make clinical investigators aware of their responsibility to maintain key codes for anonymized clinical research data in a secure location that can be accessed only by approved and authorized personnel under appropriate safeguards.

---

[28] *Id.* at 70-72.

[29] *See* GREEN PAPER at 41-51 (2010).

PhRMA and its members have extensive experience with industry codes. PhRMA's principles and guidelines concerning interactions with health care professionals, clinical trials, and direct-to-consumer advertising provide guidance for biopharmaceutical companies engaged in those activities. Our efforts in this area have been recognized by the HHS Office of the Inspector General (OIG), which has cited PhRMA's *Code on Interactions with Healthcare Professionals* as "a good starting point" for compliance with the anti-kickback laws.[30] Section 12 of the PhRMA Code encourages the appropriate uses of non-patient-identified prescriber data and states:

> Companies that choose to use non-patient identified prescriber data to facilitate communications with healthcare professionals should use this data responsibly. For example, companies should (a) respect the confidential nature of prescriber data; (b) develop policies regarding the use of the data; (c) educate employees and agents about those policies; (d) maintain an internal contact person to handle inquiries regarding the use of the data; and (e) identify appropriate disciplinary actions for misuse of this data. In addition, companies should respect and abide by the wishes of any healthcare professional who asks that his or her prescriber data not be made available to company sales representatives. Companies may demonstrate this respect by following the rules of voluntary programs that facilitate prescribers' ability to make this choice.

Many PhRMA member companies have also endorsed the International Pharmaceutical Privacy Consortium's *Privacy Guidelines for Marketing to U.S. Consumers*, which set forth best practices for the collection and use of consumer data for marketing purposes.[31]

The Use of Anonymized Data. The proposed framework's application to all data that can be "reasonably linked to a specific consumer, computer, or other device" may prevent the beneficial collection and use of data in which there is lowered expectation of privacy. The Report bases its recommendation on the observation that "the traditional distinction between PII and non-PII continues to lose significance due to changes in technology and the ability to re-identify consumers from supposedly anonymous data."[32] PhRMA recognizes that any privacy framework must account for the fact that advances in technology and the widespread availability of public information have, in some instances, made it possible to "re-identify" anonymized data. The Report's suggestion that this phenomenon be addressed by treating virtually all

---

[30] 67 Fed. Reg. 62057, 62063 (Oct. 3, 2002).

[31] *See* Letter from Int'l Pharm. Privacy Consortium to Donald S. Clark, Secretary, Fed. Trade Comm'n, App'x C., Apr. 14, 2010 (Privacy Roundtable Comments), *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00124.pdf.

[32] STAFF REPORT at 43.

consumer data equally is, however, unnecessary and could be damaging to many beneficial uses of anonymized consumer data. The use of anonymized and key-coded data is critically important to the biopharmaceutical industry for both the double-blind clinical trials used to study new medicines, as well as post-marketing surveillance required by FDA. Also, our members use anonymized data to track drug resistance patterns and disease progression, to correlate patient compliance with treatment with health outcomes, and to aid law enforcement. Thus, anonymized aggregated health data can serve as a valuable source of information for studying the incidence and spread of disease and analyzing and comparing the cost-effectiveness of different medical therapies.

The scope of the Report's proposed framework is potentially so broad as to require consent for every conceivable collection or use of consumer data, regardless of whether those data have been anonymized. Moreover, because (after it has been re-identified) such information might be considered "sensitive," the Report may be construed to require opt-in consent for the use of virtually all consumer health information. Such a requirement would introduce an unnecessary impediment to the exchange of information that is vital to research and development of medical interventions. A better approach—one that would preserve innovators' ability to make use of anonymized data while ensuring consumers' privacy—would focus on providing appropriate protections for anonymized data by, for example, requiring that all such data be subject to security requirements.

B. Privacy By Design

The Report calls on businesses to incorporate substantive privacy and security protections into their everyday practices and at all stages of the development of their products and services. PhRMA agrees that a "privacy by design" principle is important to any privacy framework. Our industry's approach to protecting consumer privacy exemplifies the Report's suggestion that "privacy . . . be a basic consideration—similar to keeping track of costs and revenues, or strategic planning."[33] For example, PhRMA's *Principles on Conduct of Clinical Trials and Communication of Clinical Trial Results*, which were revised in 2009, reflect our members' commitment to protecting the privacy rights of research participants and ensuring the provision of adequate informed consent.[34] Similarly, PhRMA's *Code on Interactions with*

---

[33] *Id.* at i.

[34] PHRMA, PRINCIPLES ON CONDUCT OF CLINICAL TRIALS AND COMMUNICATION OF CLINICAL TRIAL RESULTS (2009), *available at* http://www.phrma.org/files/attachments/042009_Clinical%20Trial%20Principles_FINAL.pdf. As FDA has stated, the agency's regulations "require[] that potential participants be given appropriate information about the study to enable them to decide whether to enroll in the clinical trial. This process is known as 'informed consent,' and it must be in writing. The informed consent process provides an opportunity for the researcher and patient to exchange information and ask questions. Patients invited to enter a trial are not obligated to join, but can consent to participate if they find the potential risks and benefits acceptable. A consent form must be signed by the participant prior to enrollment and before any study procedures can be performed. Participants also have the right to leave a study at any time. At the same time, people need to know that circumstances may arise under which their (continued...)

Healthcare Professionals provides that companies that use non-patient identified prescriber data should take specific steps to ensure that these data are used responsibly, including:

- respecting the confidential nature of prescriber data,
- developing policies regarding the use of the data,
- educating employees and agents about those policies,
- maintaining an internal contact person to handle inquiries regarding the use of the data, and
- identifying appropriate disciplinary actions for misuse of these data.[35]

Biopharmaceutical companies also recognize that the privacy protections they build into their design processes must be sufficiently flexible to accommodate consumers' rapidly evolving expectations of privacy as well as their continued demands for innovative products. PhRMA believes that any framework requiring privacy by design must acknowledge the need for flexibility and be adaptable to evolving privacy norms. For this reason, time-bound restrictions, such as the Report's suggestion that companies collect only "information necessary to fulfill a specific, legitimate business need" and that companies retain consumer information "for only as long as they have [such a] need," are not advisable.[36] Collection and retention requirements based on "legitimate business need" assume that a business's "needs" for consumer information are static. The concept thus fails to account for the fact that, as the Commerce green paper recognizes, "creative re-use of existing information" has led to important innovations in ways that are consistent with consumer expectations of privacy.[37] The Commerce paper rightly suggests that such innovations should not come at the expense of consumer privacy. But rather than imposing impediments such as the "legitimate business need" requirement, that report suggests that a more flexible approach, which weighs the harms of such reuse against its benefits and calibrates requirements accordingly, may be appropriate. PhRMA strongly supports this option, which would permit the innovative reuse of consumer information in a way that is consistent with health care consumers' expectations of privacy.[38] In addition, consistent with our

---

participation may be terminated by the researcher, without their consent." FDA, "FDA 101: Clinical Trials and Institutional Review Boards," *available at* http://www.fda.gov/ForConsumers/ConsumerUpdates/ucm134723.htm.

[35] PHRMA, CODE ON INTERACTIONS WITH HEALTHCARE PROFESSIONALS, *available at* http://www.phrma.org/files/attachments/PhRMA%20Marketing%20Code%202008.pdf

[36] STAFF REPORT at 45-47.

[37] *See* GREEN PAPER at 38.

[38] HHS is currently considering a more flexible approach to the future research use and disclosure of information protected by the HIPAA Privacy Rule. *See* Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40,868, 40,893-94 (July 14, 2010). Under the HIPAA Privacy Rule, an individual's authorization for the use or disclosure of such (continued...)

call for flexibility, FTC must take into account the various record retention requirements imposed on biopharmaceutical companies by the FDA and other regulators as well as the challenges faced by companies managing legacy systems after mergers and acquisitions.

C. Choice

The Report next recommends a more "simplified approach to offering and communicating privacy choices" to consumers. The approach would emphasize the importance of providing choice "at a time and in a context in which the consumer is making a decision about his or her data."[39] At the same time, the proposed approach would represent a "streamlin[ing]" of the notice and choice process by carving out a set of "commonly accepted [data] practices" (*e.g.*, product fulfillment and first-party marketing) for which choice would not be necessary.[40] PhRMA supports the effort to identify those data practices that are so "obvious from the context of the transaction" that consent may be inferred.[41] It is important, however, that the criteria used to identify such practices accommodate consumer expectations of privacy by recognizing that the same practice may be "obvious" in one context but not another. For this reason, we believe that the concept of "commonly accepted practices" is of limited utility unless it is tailored to specific industries.

The Report also seeks comment on its recommendation that a universal opt-out, or "do not track," mechanism be developed in the context of online behavioral advertising. PhRMA would support an effort to enable consumers to exercise more control over the collection and use of their data by parties with whom they do not have a direct relationship (*e.g.*, online advertising networks, advertising exchanges, and data aggregators). But PhRMA encourages the FTC to take a thoughtful approach to the development of any "do not track" mechanism. The Commission should adopt a policy that weighs the significant benefits that have come with the rise of online behavioral advertising—for example, a more relevant web browsing experience and the continued availability of free web content—against the harms, which are generally remote and intangible. For this reason, PhRMA believes that any "do not track" mechanism should not treat a consumer's decision regarding online behavioral advertising as "all or nothing." Rather, the mechanism should incorporate granular controls that allow users to receive targeted advertisements from certain entities while opting out of tracking and targeting

---

information for research is "research-study specific." *See id.* (citing 67 Fed. Reg. 53,182, 53,226). HHS is considering whether to amend the rule in a way that would increase the availability of this information for future research while still protecting individual privacy. *See id.* The agency has requested comments on three options for amending the Rule. Under one of these options, it would be permissible to disclose or use protected health information for future research purposes "to the extent such purposes are adequately described in the authorization such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for such future research." *Id.*

[39] *Id.* at 57.

[40] *Id.* at 53.

[41] *See id.* at 54.

by others. Consistent with our comments on privacy by design, above, PhRMA believes that industry-specific controls might be more appropriate for different types of information collected for different purposes.

D. Transparency

The Report also seeks comment on its proposed transparency principle, which would require companies to create more standardized privacy notices, provide consumers reasonable access to the data that companies maintain about them, and provide robust notice and obtain affirmative consent for material, retroactive changes to data policies.[42] PhRMA supports the effort to make companies' data practices more transparent to consumers. PhRMA has three comments on the transparency principle.

First, PhRMA supports the staff's recommendation that privacy notices become more standardized, but we suggest that standard notices be industry-specific so that they may be tailored to the specific kinds of information collected and information that a consumer will find important based on the company with which he or she engages. A good approach might be for stakeholders in a particular industry to develop a model privacy notice for that industry. The notice could be developed though the same process used to develop that industry's self-regulatory code and could reflect the principles embodied in that code.

Second, PhRMA believes that requiring a company to obtain opt-in consent for changes to its data policies would create similar problems to the requirement that a company retain data for only as long as it has a "legitimate business need." As noted above, a policy that restricts creative and beneficial reuse of data could stifle innovation that benefits patients. PhRMA recommends instead that a company be required to provide robust notice of any change on its website or other means if practicable, as well as an opportunity for consumers to opt out. This approach would preserve companies' ability to innovate through repurposing consumer data while also protecting consumers' ability to control how their data are used.

Third, PhRMA supports providing consumers access to data that a company maintains about them. Specifically, PhRMA supports reasonable consumer access to one's personal information that has not been anonymized. Requiring companies to provide access to all anonymized information would impose an unreasonable burden on businesses and may actually increase privacy risks (because the data may have to be re-associated with the consumer who seeks access to it or it may expose one's personal data to someone else inadvertently). Furthermore, consumer access should be subject to reasonable search expense and time limits. A requirement that companies provide access to information that may have been collected many years ago may prove unworkable in many cases, and, in any event, would constitute a severe information technology burden on companies. Similarly, because retrieving information about a consumer may require a great deal of time and resources, companies should be given a

---

[42] *Id.* at 70-77.

reasonable amount of time to respond to requests for access. Companies should also be required to request sufficient evidence of one's identity prior to granting access to any personal data.

* * *

Thank you for the opportunity to comment on the FTC's preliminary staff report. Please do not hesitate to contact me if you have any questions.

Respectfully submitted,

Jeffrey K. Francer
Assistant General Counsel