UnitedHealth Group
9900 Bren Road East, MN008-T700
Minnetonka, MN 55343

February 18, 2011

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

RE: FTC Staff Preliminary Report on Protecting Consumer Privacy - File No. P095416

Dear Commissioners and Staff,

UnitedHealth Group is pleased to provide the Federal Trade Commission our comments on the Preliminary FTC Staff Report entitled "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (the "Report"). We support the efforts of the Commission to propose a comprehensive national framework for the commercial use of consumer data.

UnitedHealth Group is dedicated to making our nation's health care system work better. Recognized as America's most innovative health care company by *Fortune* magazine, our highly-diversified and comprehensive array of health and well-being products and services empowers individuals, expands consumer choice, and strengthens patient-provider relationships. Our 80,000 employees serve the health care needs of more than 75 million individuals, develop and advance new health technologies and enhance financial and operational connectivity across the health care system. Our role as a national leader in both private and public health benefits programs and services enables us to continuously foster innovative health solutions aimed at creating a modern health care system that is more accessible, affordable and personalized for all Americans. We offer these comments based on our experience in developing and delivering innovative solutions through our electronic health record (EHR) and health information exchange technologies, as well as our health plan offerings in the commercial, Medicare, and Medicaid markets across the country.

UnitedHealth Group supports the Commission's efforts in conducting public roundtable discussions and drafting its proposed framework with a goal of improving consumer choice and privacy. We believe that a strong privacy framework is important for protecting consumer trust as well as for promoting innovation. We have described our specific recommendations and concerns related to the Commission's proposed framework below.

A. Scope of the Proposed Framework

With respect to the Commission's proposal that the framework apply "to all commercial entities that collect consumer data that can be reasonably linked to a specific consumer, computer, or other device,"[1] we urge the Commission to avoid applying its framework over existing industry-specific frameworks. Where existing laws provide for a robust privacy and security framework, we believe it is important that the Commission not seek authority to impose additional requirements. We note the Department of Commerce's decision in its "Green Paper" not to make recommendations with respect to data privacy laws and policies that cover specific industry sectors, such as health care. We urge the Commission to consider a similar approach. It will be critical for commercial entities already subject to robust privacy and security requirements that any new framework not impose overlapping compliance obligations. Specifically, we request that the Commission offer a safe harbor to companies that function as a covered entity or business associate under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HIPAA contains detailed requirements for protecting the privacy and security of patient information, including rules for notifying patients in the event of a breach of protected health information. Congress recently strengthened HIPAA through the HITECH Act, which created a federal data breach notification law for HIPAA covered entities and also strengthened HIPAA's existing privacy and security requirements. The HITECH Act provides for stronger enforcement of HIPAA, including enforcement by State attorneys general as well as higher penalties for noncompliance. UnitedHealth Group is deeply committed to protecting the privacy of its members in accordance with the HIPAA requirements. We are concerned that efforts to create a national privacy framework may result in two sets of requirements for HIPAA covered entities. We urge the Commission to avoid imposing an additional framework on the information already protected by HIPAA. Overlapping sets of requirements will have the effect of increasing compliance costs – and thus health care costs – without providing consumers with greater protection.

B. Privacy by Design

UnitedHealth Group supports the concept that companies should promote consumer privacy throughout their organizations. This includes incorporating substantive privacy protections, such as security and data retention practices, and maintaining comprehensive data management procedures. Indeed, in our capacity as a HIPAA covered entity, this approach acts as a guiding principle. The HIPAA framework requires robust privacy policies that govern practices throughout an entity's activities as well as workforce training on these policies. HIPAA covered entities already take the steps described by the Commission as Privacy by Design. Indeed, some of the language recommending proposed standards is drawn directly from HIPAA, and the Commission acknowledges that the HIPAA Security Rule requires the same protections that the Commission recommends. For example, as part of Privacy by Design, the Commission states that companies should employ reasonable safeguards, including physical, technical and administrative safeguards, to protect information. In addition, the Commission notes that the level of security required should depend on the sensitivity of the data, the size and nature of the company's business operations, and the types of risks the company faces. These and other Privacy by Design principles reflect the existing HIPAA framework.

C. Simplifying Consumer Choice

UnitedHealth Group appreciates the Commission's recommendations that consumer choice be simplified. As part of this proposal, the Commission suggests that companies offer consumers a choice at a time and in the context in which a consumer is making decisions about data. We are concerned about this approach in the context of the health care system. Offering consumer choice at the time and

[1] Report at 41.

in the context in which the consumer is making decisions about data may not work in the provision of and payment for medical care. Rather, in the health care context, patients typically make choices about the health care they receive, and payment for that health care, at the beginning of a relationship with a health care provider. The HIPAA framework requires a notice of privacy practices be provided at that initial contact and periodically thereafter. Patients have certain rights with respect to their information at all times, and uses and disclosures of information not expressly permitted under HIPAA would require patient authorization. We urge the Commission to consider this and other circumstances in which consumer decisions at the time and in the context in which the consumer is making decisions about the data may not always be appropriate. For example, it may not be appropriate for a patient in an emergency situation to be required to make decisions regarding how or with whom their data is shared. Again, we believe that any such principles should exempt information covered by HIPAA.

1. Situations in which consumer choice is not required:

UnitedHealth Group appreciates the Commission's suggestion that companies do not necessarily need to provide consumer choice before using consumer data for certain "commonly accepted practices"[2]. We agree that providing choice for such practices would be unnecessary, because the data use is obvious or necessary for public policy purposes. We support the list of commonly accepted practices proposed in the Report and urge the Commission to continue to provide guidance to companies on what the agency would consider commonly accepted uses.

i. *First Party Marketing:* We support the recommendation to exclude first party marketing from the proposal to require consumer choice. We believe that this exception should extend to commonly branded affiliates. Where the business relationship between the affiliates is clear to consumers based on common branding or similar means, the companies' practices should be considered first party marketing. This is consistent with a reasonable consumer expectation that commonly branded or similarly connected companies may engage in targeted first party marketing.

We also ask the Commission to make clear that this exception would apply where a vendor is acting on behalf of the first-party marketer. The Commission states that the first party marketing exception would apply "where companies share consumer information with service providers acting at their direction for the [exceptions to consumer choice], provided there is no further use of the data."[3] We support the recognition that first party marketers may continue to use vendors to carry out communications, and we urge the Commission to make clear in any final report that such activities are permitted.

With respect to first party marketing, we also believe that the exception should include circumstances in which the information is sensitive data. The consumer likely has provided such data to the company, and it would seem reasonable to assume that the consumer would have the same type of expectations for "sensitive" data as for other data provided to the company. We also believe that first party marketers should be able to communicate with a consumer in other contexts, such as a website retailer sending offers via postal mail. Consistent with current commercial practice, we expect that individuals would have the ability to opt-out of future communications. Consumers should also continue to have the opportunity to decline solicitations as provided by existing sectoral laws. We also note that sensitive data is difficult to define and indeed is defined differently in various jurisdictions.

[2] Report at 53-57.

[3] Report at 54-55.

ii. *Data enhancement:* In response to the Commission's request for comment regarding the level of choice that should be given to consumers regarding the practice of data enhancement, we believe it is important for data enhancement practices to be set forth in a privacy notice, but that such practices should not require a specific consent. As the Commission has noted, requiring choice sometimes can be more burdensome than beneficial, and data enhancement is such a circumstance. Prohibiting the combining of publicly available data with data held by a first party marketer may unduly restrict the exchange and use of data that benefits consumers.

2. Do Not Track

Within the theme of simplifying consumer choice, the Commission proposes a "Do Not Track" mechanism that could be advanced either by legislation or through enforceable industry self-regulation. Such a mechanism would require businesses to comply with a consumer's centralized opt-out of online behavioral tracking. UnitedHealth Group supports the Commission's approach to an enforceable industry-developed solution to Do Not Track technology. Industry already is working to create solutions, and it is important that any solutions allow for evolving technologies that respond to and promote consumer choice. We believe that an industry-led solution will provide the best combination of consumer protection and innovative technology, and we understand that browser suppliers are working to enhance these functions. We agree with the Commission that it will be important for browser mechanisms to be more accessible and understandable. We also believe that an important component of Do Not Track efforts is consumer education. Significant efforts should be made to educate consumers on how to utilize their browser settings to increase privacy during their online sessions.

The Report suggests that a Do Not Track mechanism would be applied in the context of behavioral advertising but does not offer a description of the scope of practices that constitute "behavioral advertising." We believe that a Do Not Track mechanism should be directed at consumers' principle privacy concerns, typically the practice of tracking users across third party web sites in order to deliver targeted advertising to the consumer. At the same time, as the Commission notes, Do Not Track mechanisms "should not undermine the benefits that online behavioral advertising has to offer."[4] Thus, a Do Not Track mechanism that shuts down all tracking activities may in fact not be consistent with consumer preferences or choice. Instead, permitting consumers to choose a Do Not Track option that applies to third party tracking and targeting – or that permits more granular choice under which consumers can control the types of third party advertising they would like to receive – provides consumers the option to benefit from behavioral advertising. At the same time, we believe that first party tracking and targeting should not fall within the scope of Do Not Track mechanisms. This is consistent with the Commission's recommendations that first party marketing be an exception to any requirement for affirmative consumer choice. Consumers have the ability to control first party tracking and targeting by simply choosing not to visit the website that offers such tracking. We urge the Commission to clarify that Do Not Track efforts should be focused at behavioral advertising in the context of third party tracking and targeting.

D. Increasing the Transparency of Data Practices

UnitedHealth Group supports the Commission's position that companies should increase the transparency of their data practices, such as by clarifying, shortening and standardizing privacy notices; providing reasonable access to the consumer data they maintain; providing prominent disclosures and obtaining affirmative express consent before using consumer data in a materially different manner than claimed when the data was collected; and working to educate consumers about commercial data privacy practices. In particular, we support the Commission's recommendations that companies simplify consumer choice in part by providing a notice of privacy practices, and we support efforts to provide

[4] Report at 67.

guidance to companies on how to simplify and provide more meaningful information to consumers about privacy practices. We believe it is important that consumers be put on notice of an entity's privacy practices, yet at the same time we appreciate the concerns that such notices not be overly confusing to consumers.

Privacy notices are a routine and required part of HIPAA compliance, and HIPAA covered entities already are governed by a regulatory system that imposes very specific privacy notices. We encourage the Commission to ensure that any guidance it provides on privacy notices makes clear that it is not intended to apply where another specific regulatory system already governs privacy notices. Again, we note the importance of having a single regulatory authority apply in a particular context. In our capacity as a HIPAA covered entity, we already must adhere to very similar principles with respect to the protected health information we maintain. We believe that it is important that an additional regulatory scheme not be imposed on information protected by HIPAA. We urge the Commission to make clear that HIPAA governs with respect to its covered entities and to provide a safe harbor for HIPAA covered entities and their business associates.

* * *

We appreciate the opportunity to submit comments on the Report. Should you have any questions regarding our suggestions, please do not hesitate to contact me.

Sincerely,

Gaye Adams Massey
Senior Deputy General Counsel
and Acting Privacy Officer

Ann Tobin
Senior Privacy Counsel