UNITEDHEALTH GROUP
9900 Bren Road East | MN008-T904
Minnetonka, MN 55343

November 9, 2018

National Telecommunications and
Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4275
Washington, DC 20230

Submitted Electronically: privacyrfc2018@ntia.doc.gov

Re: Developing the Administration's Approach to Consumer Privacy

Dear Sir/Madam:

UnitedHealth Group (UHG) is writing in response to a Request for Comments (RFC) from the National Telecommunications and Information Administration (NTIA) entitled *Developing the Administration's Approach to Consumer Privacy* published in the Federal Register on September 26, 2018.[1] The RFC is seeking public input on potential federal government actions and goals to protect the privacy of consumer information collected and used by businesses in the delivery of products and services. UHG supports efforts by the NTIA to develop a consistent policy framework for safeguarding consumer data while promoting the appropriate use of information within the digital environment.

UHG is dedicated to helping people live healthier lives and making the health care system work better for everyone through two distinct business platforms -- UnitedHealthcare, our health benefits business, and Optum, our health services business. Our workforce of 285,000 people serves the health care needs of nearly 140 million people worldwide, funding, arranging and providing health care for individuals, employers, and the government. As America's most diversified health and well-being company, we not only serve many of the country's most respected employers, we are also the nation's largest Medicare health plan - serving nearly one in five seniors nationwide - and one of the largest Medicaid health plans, supporting underserved communities in 28 States and the District of Columbia. We also serve over 14 million people through more than 30,000 aligned physicians and 7,000 advanced practice clinicians, as well as working with 4 out of 5 hospitals, 200 plus health plans, and 80 life sciences organizations.

Using Health Information to Promote Better Care

Health information is critical to the delivery of services and products to our health plan members, patients, and consumer and business customers. In accordance with our policies and applicable state and

[1] 83 Fed. Reg. 48600.

federal laws and regulations, we exchange data and information throughout the health care system to ensure that individuals have access to the care they need and that care providers are reimbursed appropriately. UHG receives data from medical and prescription claims submitted by providers and pharmacies, eligibility and clinical information, and from patients and consumer themselves through the normal course of our day-to-day business and clinical operations.

Combined with our deep knowledge and expertise in health care, we use this data and information to gain better clinical insights that help our members and patients better manage their health and the health care they receive. We also use this knowledge and insight to drive innovation and develop tools that enable UHG to facilitate and deliver more effective, efficient care and help improve patient health outcomes.

UHG maintains strict policies and protections around the data and information entrusted to us. Permitted data analysis and research – to help advance and support the needs of the people we serve – is conducted in a secure and compliant manner consistent with applicable state and federal laws and regulations.

Safeguarding Consumer Information

As noted in the RFC, there are a number of existing comprehensive standards governing the collection, use, and sharing of information. UHG is subject to the privacy and data security rules established under the Health Insurance Portability and Accountability Act (HIPAA).[2] Depending on the circumstances, our use of information may also be governed by other federal requirements including the Children's Online Privacy Protection Act,[3] Fair Credit Reporting Act,[4] Genetic Information Nondiscrimination Act,[5] and the Gramm-Leach-Bliley Act.[6] In addition, UHG operates in compliance with an extensive structure of state privacy and data security laws and regulations as well as international privacy standards, such as the European Union General Data Protection Regulation adopted in 2016 by the European Parliament and other international privacy standards.

UHG strongly supports the statement by NTIA in the RFC that it "does not propose changing current sectoral federal laws."[7] UHG primarily operates under the HIPAA privacy, security, and data breach notification rules, all of which are enforced by the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS). These rules have been in place for 15 years and provide substantial protections for protected health information entrusted to health plans, health care providers, and clearinghouses (including business associates of these "covered entities") yet provide the flexibility needed to improve healthcare and reduce costs. When necessary, both Congress and HHS have acted to amend the rules to enable additional data safeguards and information sharing in order to improve the delivery of health care.[8]

---

[2] The HIPAA health information privacy, security and data breach rules are set out at 45 CFR Part 164, Subpart C, §§164.302 *et seq.*, 45 CFR Part 164, Subpart D, §§164.400 *et seq.*, and 45 CFR Part 154, Subpart E, §§164.500 *et seq.*
[3] 16 CFR §§312.1 *et seq.*
[4] 16 CFR §§604.1 *et seq.*
[5] 29 CFR §§1635.1 *et seq.*
[6] 16 CFR §§313.1 *et seq.*
[7] 83 Fed. Reg. 48601.
[8] *See e.g.*, The Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 USC §§1301 *et seq.*

We believe that covered entities should continue to be regulated by HIPAA. Any efforts to replace the protections outlined in HIPAA could have significant unintended consequences that will unduly restrict the sharing of patients' health information among covered entities including doctors, hospitals, and other caregivers. In its policy development, NTIA should not disturb existing federal privacy standards. UHG urges the NTIA to consider harmonizing protection of non-HIPAA health data with similar protections as are found in the HIPAA privacy, security, and data breach notification rules, along with similar enforcement mechanisms. As discussed below, we believe that the HIPAA privacy provisions establish a number of important principles that should be considered by NTIA in its development of consumer information privacy policies and goals.

Informing Consumers How Their Information is Used

Consumers today share their personal information with a wide variety of organizations. As such, they need to be aware how information is used and when it may be shared with others as part of the delivery of a product or service. We support easily understood disclosures by information users to consumers on how and when their data is accessed. For example, our health plan members receive an annual HIPAA notice of privacy practices that spells out the situations where we use their data and when it is shared in connection with treatment, payment or health care operations, and our health care providers post a similar notice and provide it on the date of the patient's first service and upon request.[9]

It is important that such notices be provided in a manner that will be easily understood. Mandated information provisions, lengthy disclosure language, and requirements to include notices with all transactions, especially when these are not directly related to privacy, can detract from transparency and present consumers with information overload that is ultimately ignored. Transparency policies need to carefully weigh the goal of keeping consumers informed with adding complex disclosure requirements that may not adequately educate consumers on how their information is used.

Ensuring Reasonable Use of Consumer Information

Our members and their care providers provide us with information so we may pay their claims, coordinate their care, and carry out health care operations such as fraud prevention and quality assurance. Our patients provide information directly to their doctors and other health care professionals. Members and patients have a reasonable expectation that we use their data for the purposes for which we collected it – and only use the data necessary to provide their health coverage, treatment, and other related services. Under the HIPAA privacy rule we may use this member and patient personal health information of treatment, payment, and designated health care operations.[10] However, we must obtain patient and member authorization for any other data use or sharing such as marketing.[11] These requirements apply both to us and any of our business associates.

Since its passage, HIPAA's controls have been proven to protect member and patient health information while at the same time allow for health care innovation. We believe similar, reasonable controls imposed on organizations that are not subject to HIPAA appropriately balances a member's or patient's privacy and security interests with the provision of innovative products and services.

---

[9] 45 CFR §164.520. Similar consumer disclosures are provided under the Gram-Leach-Bliley Act regulations, 16 CFR §313.4.
[10] 45 CFR §164.506.
[11] 45 CFR §164.508.

Consumer Rights to Data

Providing individuals with easy access to their health information empowers them to be more in control of decisions regarding their health and well-being. For example, individuals with access to their health information are better able to monitor chronic conditions, adhere to treatment plans, find and fix errors in their health records, and track progress in wellness or disease management programs. For these reasons, consumers should have the ability to review their data and to ask for corrections where appropriate. The HIPAA privacy rules provide standards for an individual to access their information and request changes. However, businesses need the ability to challenge correction requests if they believe that such action will result in inaccurate or incomplete information. Under the HIPAA privacy rules, an individual can request access to and amendment of their personal health information and the covered entity may decline the request to amend if the information is in fact accurate and complete or was not originally created by the covered entity.[12]

Organizations also should not be required to delete data that is still needed in the usual course of operations or where deletion would be infeasible due to legal, regulatory, or other reasons. In the context of health care data, prematurely removing information from data systems poses significant risk to business systems and operational credibility.

Protecting Health Information

Health information is too valuable and the risk of misuse is far too great, and, as a result, individuals have the right to expect that their health information will be used appropriately and held securely by an organization regardless of whether HIPAA or a different law applies. As discussed above, we recommend that the current HIPAA standards remain for covered entities and their business associates subject to those requirements. Organizations not subject to HIPAA should be required to conform to similar privacy, security, and data breach notification requirements. Moreover, we believe HHS' Office for Civil Rights has the expertise and focus to enforce all requirements applicable to the use and sharing of health information, whether under HIPAA or a similar health information privacy law.

Harmonizing Privacy Standards

As noted, there are a growing number of state and federal laws governing the collection and use of consumer information. As a result, organizations face a complex and potentially conflicting set of requirements when they use consumer data to provide products and services. The complicated web of privacy laws leads to confusion on the part of individuals and organizations and adds to the costs incurred by consumers.

The NTIA should look at ways to harmonize these various laws and consider how they might be applied across all organizations, particularly with respect to health information. Members and patients that provide protected health information subject to the HIPAA privacy rules benefit from a comprehensive set of privacy safeguards and information use standards that are not available if their health information is collected and used by organizations not governed by HIPAA. We encourage NTIA to convene a group of stakeholders in health care and those that support health care to examine how different health

[12] 45 CFR §164.526.

privacy standards are applied and develop a policy approach that will lead to more uniformity in both what is required and how the requirements are enforced.

UHG appreciates the opportunity to provide feedback to NTIA as it works on this critical issue. We look forward to contributing additional support in the future to this initiative. Please feel free to contact us if you have any questions.

Sincerely,

Michelle Huntley
Chief Privacy Officer, UnitedHealth Group