



UnitedHealth GroupSM

Ann E. Tobin, JD
Senior Privacy Counsel
UnitedHealth Group
9900 Bren Road East, MN008-T700
Minnetonka, MN 55343

January 28, 2011

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave., N.W., Room 4725
Washington, D.C. 20230

**RE: Commercial Data Privacy and Innovation in the Internet Economy: A
Dynamic Policy Framework, RIN 0660-XA22**

Dear Internet Policy Task Force:

UnitedHealth Group is pleased to provide the U.S. Department of Commerce our comments on the Department's report entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" (the "Green Paper"). We support the efforts of the Department and its Internet Policy Task Force to propose a comprehensive national framework for commercial data privacy.

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 Task Force's recommendation calling for a stronger U.S. commercial data privacy framework. We believe that a strong privacy framework is important for protecting consumer trust in electronic information as well as for promoting innovation. We support the Task Force's recommendation for adoption of a comprehensive set of Fair Information Practice Principles to protect the privacy of personal information in commercial contexts not covered by an existing industry specific law. We also support the

recommendation to allow adherence to voluntary industry codes of conduct as a mechanism for implementation of a national privacy framework. We are particularly concerned that any national privacy framework takes into account existing sector-specific privacy laws, such as those governing the use and disclosure of patient information in the health care context. We strongly urge the Task Force to continue to recognize the existence of these laws and to foster recommendations that will not have the effect of subjecting health care companies to an additional, competing set of compliance obligations. We have described our specific recommendations and concerns below.

I. A Single Framework Should Apply to the Health Sector

We appreciate the Task Force's decision not to make recommendations with respect to data privacy laws and policies that cover specific industry sectors, such as health care. The careful coordination of any federal privacy framework with existing industry-specific laws will be critical for commercial entities subject to those specific laws. It will be important to the compliance activities of such entities that any federal framework recognizes these existing laws.

a. HIPAA provides a robust privacy and security framework for health care entities.

The Health Insurance Portability and Accountability Act of 1996 (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 as part of the American Recovery and Reinvestment Act of 2009, by enacting the HITECH Act, which created a federal data breach notification law for HIPAA covered entities. The law 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; however, that efforts to create a national privacy framework may result in two distinct sets of requirements for HIPAA covered entities. We urge the Department to recommend that HIPAA covered entities not be required to comply with any such national framework in addition to HIPAA. Instead, we support the Task Force's acknowledgment of existing sector-specific laws and urge the Department to continue to support a framework that does not require entities already subject to industry specific privacy and security requirements also to come into compliance with a different set of standards. Duplicate and overlapping sets of requirements will have the effect of increasing compliance costs – and thus health care costs – without providing consumers with greater protection.

b. State law

With respect to the Task Force's recommendation for consideration of a federal commercial data security breach notification law, we believe it is important to provide clear rules for state law preemption. As the Green Paper notes, the current patchwork of different state laws "present[s] undue costs to American businesses" while at the same time results in a lack of clarity to consumers as to how their information is being used.¹ We suggest that any federal data security breach notification law preempt state laws addressing the same subject matter. This

¹ Green Paper at 7.

would provide greater uniformity for commercial entities as well as for consumers. This also would allow businesses to comply with one set of legal requirements, avoiding unnecessary compliance costs that do not clearly increase privacy protection. Absent complete preemption, it is critical that – at a minimum – contrary state law be preempted by any federal security breach notification rules. The preemption of contrary state laws allows companies experiencing a breach to apply the same legal standard consistently when trying to assess state and federal notification requirements. This also ensures that consumers are provided only a single notification in the event of a breach rather than different communications about the same security breach that may be required in order to comply with contrary laws. This will reduce anxiety and confusion among affected individuals who may otherwise receive multiple notices of a single breach.

c. Federal law

We also appreciate the Task Force’s recommendation that any new federal data security breach notification law not preempt existing federal security breach laws that apply to specific industries, such as healthcare. We believe it is important that any such federal standard provide a safe harbor for any security breaches that would be subject to an industry specific law, ensuring that any new federal standard does not apply where a breach already is subject to the requirements of an existing federal industry-specific law. Any federal commercial privacy policy, including any federal data security breach notification, should act in conjunction with those laws so that companies already subject to robust industry-specific standards need only comply with a single legal framework.

II. A National Security Breach Framework Should Include a Risk-Based Trigger

UnitedHealth Group strongly believes that any national security breach framework should be based on a risk assessment of the potential harm from the breach. A risk of harm standard is a critical component of the effective implementation of breach notification. The purpose of a federal breach notification requirement should be to alert individuals so that they may take precautions to mitigate harm. Providing notice to individuals for whom there is no reasonable likelihood of harm may create needless anxiety among the recipients of the notices without serving any real benefit to the individuals being notified. Notifying individuals in such circumstances ultimately may result in more harm than if no notice had been provided.

The federal government currently provides guidance on the parameters of conducting a risk assessment in OMB Memorandum M-07-16,² and it instructs federal agencies to undertake a risk of harm assessment before notifying individuals of a breach. This memorandum provides guidance for federal agencies to safeguard against and respond to breaches of personally identifiable information. It serves as a useful framework for commercial entities to establish a meaningful process for identifying situations in which the security or privacy of information has been compromised, and thus where a risk of harm exists. The establishment of a risk assessment process in any federal security breach notification legislation would be consistent with the federal government’s approach to security breaches to date. A risk of harm trigger for a security breach notification – combined with a robust framework for protecting individual privacy, audits, and other mechanisms to ensure stronger and more comprehensive privacy protections – can help to ensure that consumers receive notice of security breaches that present a risk of identity theft or

² See 74 Fed. Reg. at 42744.

other harm without notifying individuals of circumstances in which their information is not likely to be compromised.

III. Conclusion

UnitedHealth Group appreciates the opportunity to submit our thoughts and recommendations to the Department on the Green Paper. We look forward to working with you to aggressively support adoption of a robust privacy framework that recognizes existing industry-specific framework.

Should you have any questions regarding our suggestions, please do not hesitate to contact me.

Sincerely,

A handwritten signature in cursive script, appearing to read "Ann E. Tobin".

Ann Tobin
Senior Privacy Counsel