June 4, 2010

The Honorable Rick Boucher
Chairman
Subcommittee on Communications,
Technology and the Internet
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Cliff Stearns
Ranking Member
Subcommittee on Communications,
Technology and the Internet
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Re: Confidentiality Coalition Comments on Proposed Privacy Legislation

Dear Chairman Boucher and Ranking Member Stearns:

The Confidentiality Coalition respectfully submits these comments in connection with draft privacy legislation distributed by Congressmen Boucher and Stearns. In these comments, we (i) provide background on the Confidentiality Coalition; and (ii) offer our concerns about the potential impact of this legislation on the healthcare industry and its business partners, who already are regulated on privacy and security issues by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the recent amendments from the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the "HITECH Act").

The proposed legislation, while focused primarily on areas (like Internet marketing) that are outside the most common activities of the healthcare industry and for which privacy standards are a laudable goal, likely would have extremely disruptive (and presumably unintended) effects on the normal business activities of healthcare providers and health plans, by altering current and accepted practices across the industry. Moreover, the legislation would create a parallel enforcement mechanism for the healthcare industry, which is already subject to extensive privacy and security regulation at both the federal and state levels. In addition, and of greater concern, these provisions would duplicate regulations that are already in place for this industry, and would create overlapping and largely inconsistent requirements on the healthcare industry. These new provisions will not only unfairly burden the healthcare industry and create substantial new inefficiencies, but will also threaten patient health and safety by altering longstanding industry practices.

Accordingly, we encourage a clear statement in this legislation that exempts healthcare companies who are covered entities under HIPAA and their business associates (to the extent they are holding data on behalf of covered entities that already is regulated by HIPAA and HITECH) from the reach of this new legislation. This statement would preserve the careful lines drawn by the HIPAA rules and would permit the healthcare industry to continue to provide its services to members and patients without the need to dramatically alter its current (and already

heavily regulated) arrangements. We view these steps as appropriate to avoid substantial disruption of the healthcare industry and risks to patients, while still permitting the legislation to focus on areas (such as the core Internet marketing area) that are largely unregulated today.

Background

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health produce distributors, pharmacy benefit managers, pharmacies, health information and research organizations, patient groups, and others[1] founded to advance effective patient confidentiality protections.

The Coalition's mission is to advocate policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enabling the essential flow of information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions. The Confidentiality Coalition is committed to ensuring that consumers and thought leaders are aware of the privacy protections that are currently in place. And, as healthcare providers make the transition to a nationwide, interoperable system of electronic health information, the Confidentiality Coalition members believe it is essential to replace the current mosaic of sometimes conflicting state privacy laws, rules, and guidelines with a strong, comprehensive national confidentiality standard.

Discussion

The Confidentiality Coalition applauds Congress' effort to evaluate appropriate practices for the collection and distribution of personal information through the Internet. We understand and support the primary goals of this legislation. For example, as Representative Boucher noted in his comments upon the release of the legislation, "[o]ur goal is to encourage greater levels of electronic commerce by providing to Internet users the assurance that their experience online will be more secure. That greater sense of privacy protection will be particularly important in encouraging the trend toward the cloud computing." In addition, Representative Boucher noted the bill's focus on advertising and marketing practices. As he described, "[o]nline advertising supports much of the commercial content, applications and services that are available on the Internet today without charge, and this legislation will not disrupt this well established and successful business model. It simply extends to consumers important baseline privacy protections."

While we understand and support these goals in connection with the largely unregulated internet marketing area, these goals - and the consumer risks they are designed to address - make little sense (or have already been addressed) for the healthcare industry. Unlike much of the online industry, the healthcare industry already is heavily regulated in its privacy and security

[1] A list of the Confidentiality Coalition members is attached to this letter.

obligations. These obligations have been in place since 2003 under HIPAA, and recently have been revised and expanded through the HITECH Act. These HIPAA/HITECH provisions impose specific requirements on covered entities (mainly healthcare providers and health plans) to provide notice to patients and members of all uses and disclosures of personal information obtained in the course of providing services to these individuals (along with a wide variety of other notice provisions). Obviously, most healthcare information is not exchanged using the Internet, but some clearly is. Accordingly, legislation that focuses on online collection of information - and addresses issues of specific importance to internet marketing activities - distorts the practices of the healthcare industry.

In addition to the detailed privacy notice obligations (which overlap to some extent, but also contain significant differences with the proposed legislative requirements), the HIPAA/HITECH rules impose specific consent obligations, with certain areas where consent is assumed (primarily, the core healthcare purposes of treatment, payment, and healthcare operations), certain areas where use and disclosure is permitted without the need for consent (such as certain public health disclosures or disclosures in connection with litigation), and other areas – essentially, all other disclosures – where a specific, detailed individual "authorization" is required. "Marketing" in connection with the healthcare industry also is heavily regulated and limited – both through the original HIPAA rules and through new – and stricter – provisions from the HITECH Act. These rules address the specific operations of healthcare companies, rather than applying more general principles to a healthcare business. Under these rules, most marketing activities require a specific patient authorization. The only marketing activities that are permitted without authorization are those that the Department of Health and Human Services (HHS) have deemed to be useful and appropriate for consumers in the healthcare industry. The HHS Office for Civil Rights has jurisdiction to enforce these provisions (including expanded new penalties created by the HITECH Act). In addition, the HITECH Act authorized state Attorneys General to enforce the HIPAA rules as well.

The HIPAA Privacy and Security Rules have created comprehensive regulation on privacy and security for HIPAA covered entities (healthcare providers, health plans, and healthcare clearinghouses). Initially, "business associates" under HIPAA – those companies that provided services to HIPAA covered entities – were regulated only through contracts with these covered entities. Now, as a result of the HITECH law, these business associates also are directly subject to privacy and security requirements, subject to primary enforcement by the Department of Health and Human Services, and face the same penalties as covered entities for non-compliance.

Accordingly, while HIPAA does not apply to all entities that might collect, use, or disclose health-related information,[2] HIPAA does create a comprehensive set of standards and an overall enforcement protocol for those entities – both covered entities and business associates –

[2] The Coalition supports efforts by Congress and the Federal Trade Commission to evaluate appropriate privacy and security obligations for these unregulated healthcare entities or for uses and disclosures of sensitive healthcare information that are outside the scope of HIPAA.

who are regulated directly under the HIPAA rules. Moreover, as a result of the HITECH law, both covered entities and business associates face significantly increased exposure for violations of these rules, as well as the ongoing possibility of criminal penalties.

Therefore, for these covered entities and business associates, regulation under HIPAA/HITECH is both comprehensive and substantial. HIPAA/HITECH incorporates a wide range of standards for the use and disclosure of health information, creating specific rules for all aspects of the operations of the covered entities and their business associates. Moreover, the HIPAA Security Rule imposes perhaps the most significant set of security–related requirements imposed by law under any standard.

With these standards in place, we have significant concerns about the risks and burdens of creating additional and largely inconsistent obligations related to notice and consent for healthcare entities. The proposed legislation would create a new and inconsistent set of obligations on both notice and consent for the healthcare industry. We recognize that there is language addressing HIPAA in the legislation (in the section entitled "Effect on Other Laws"), but the effect of this language as drafted is unclear. Therefore, to the extent that this legislation applies to healthcare entities and their business associates, we believe strongly that these provisions would require fundamental changes in the healthcare industry without any identified need or specific rationale. The risks and burdens from these provisions are particularly high here, as virtually all information held by healthcare entities would be considered "sensitive" information under the proposed bill, with even higher compliance requirements.

Moreover, in the context of how the healthcare industry operates, the legislation would prove exceedingly difficult to implement, because of the routine and ongoing disclosures of information between "unaffiliated" entities (such as doctors, hospitals, and insurance companies), where such disclosure of information is a routine, expected, and necessary part of the healthcare industry (for example, for treatment, payment, and healthcare operations). While we recognize the value of these notice and consent principles in areas that are unregulated today, and where much of the collection and disclosure of information is invisible to individuals and consumers, neither of these premises is true for the healthcare industry. This area is heavily regulated, and the use and disclosure of information is both visible (in most situations) to the individual and appropriate for the functioning of the healthcare industry.

In addition, to the extent that this proposed legislation seeks to set standards that apply to the use or disclosure of health related information, we have great concerns if these standards are applied to information that already is protected and regulated under the HIPAA rules. HIPAA covered entities and their business associates already face significant and detailed regulation of their activities – ranging from how they use and disclose information to individual rights of patients and insureds to specific details for training, sanctions, and documentation related to privacy and security practices. It is unfair, unreasonable, and unnecessary to create new and/or different standards that would be applied to this same information. The HIPAA Rules – particularly with the additional (and still being defined) obligations imposed by the HITECH Act – create a challenging set of standards for any affected healthcare entity. To impose different or

additional standards for this information would create significant additional cost and unneeded complexity.

Also, there is no need for an additional regulator to oversee these obligations. The HIPAA rules govern healthcare covered entities and their business associates. The Department of Health and Human Services has primary authority under these rules, with a significant new set of enforcement tools in its arsenal. There is no need for the Federal Trade Commission to enter this arena to provide additional (and potentially inconsistent) regulatory oversight. To the extent that Congress wants the Federal Trade Commission (FTC) to have any involvement at all in the regulation of health information, it should limit this involvement (if any) to those entities who are outside the HIPAA/HITECH structure. Congress should not permit the FTC to regulate those companies – whether a covered entity or a business associate – who already face regulation by the Department of Health and Human Services and the Attorneys General around the country.

Therefore, we encourage Congress to include in this proposed legislation a clear and explicit exemption from these new requirements for personal information held by covered entities and their business associates that is already protected and regulated by HIPAA. Specifically, Congress should ensure that there is either an explicit statement in the legislation that entities covered by HIPAA and their business associates are exempt to the extent that the information they hold is protected and regulated by HIPAA, or a specific statement that the new notice and consent obligations imposed by this legislation do not apply to these entities to the extent the information they hold is protected and regulated by HIPAA. We propose language below to include in the legislation. This specific language, however, is less important than the overall principle – the privacy and security practices of the healthcare industry already are heavily regulated, with principles designed to facilitate the appropriate use and disclosure of healthcare information for appropriate purposes. Any change to these rules in legislation that is not focused on the activities of the healthcare industry will be duplicative at best and disruptive and damaging at worst. There is no need for these changes, and the changes (as addressed in the proposed legislation) will have significant negative effects on both healthcare companies and their patients and members.

Proposed Language:

- Amend the definition of "covered entity" in section (B) to add (iii) or any entity that is a "covered entity" under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 or a "business associate" under 45 C.F.R. Section 160.103.

- Section 3(a)(1) – Add new paragraph C – Such notice and consent obligations shall not apply to an entity that is a "covered entity" under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 or a "business associate" under 45 C.F.R. Section 160.103.

Please let us know if there are any comments or questions about the comments in this letter or the language we have proposed. We also would be happy to address our concerns in more detail if that would be helpful. We look forward to working with you on these important issues.

Sincerely,

Mary R. Grealy
President, Healthcare Leadership Council
On Behalf of the Confidentiality Coalition

Enclosure

CONFIDENTIALITY COALITION

Advancing Health Care. Safeguarding Trust.

2010 Steering Committee Membership

Aetna
American Hospital Association
America's Health Insurance Plans
Association of Clinical Research Organizations
Blue Cross Blue Shield Association
CVS Caremark
Federation of American Hospitals
Greenway Medical Technologies
Gundersen Lutheran
Health Dialog
Healthcare Leadership Council
IMS Health
Marshfield Clinic
McKesson Corporation
Medco
National Association of Chain Drug Stores
Pharmaceutical Care Management Association
Pharmaceutical Research and Manufacturers of America
Premier, Inc.
Prime Therapeutics
Texas Health Resources
VHA
Walgreens
Wellpoint

General Membership

ACA International
Adheris
American Academy of Nurse Practitioners
American Benefits Council
American Clinical Laboratory Association
American Electronics Association
American Managed Behavioral Healthcare Association
Amerinet
AstraZeneca
American Pharmacists Association
Ascension Health
Association of American Medical Colleges
Baxter Healthcare
BlueCross BlueShield of Tennessee
Catalina Health Resource
CIGNA Corporation
Cleveland Clinic
College of American Pathologists
DMAA: The Care Continuum Alliance
Eli Lilly
ERISA Industry Committee
Food Marketing Institute
Fresenius Medical Care
Genentech, Inc.
Genetic Alliance
Genzyme Corporation
Health Care Service Corporation
Humana, Inc.
Integrated Benefits Institute
Intermountain Healthcare
Johnson & Johnson
Kaiser Permanente
Mayo Clinic
Medical Banking Project
Merck
MetLife
National Association of Health Underwriters
National Association of Manufacturers
National Association of Psychiatric Health Systems
National Community Pharmacists Association
National Rural Health Association
Novartis
Pfizer
Quest Diagnostics
SAS
Siemens Corporation
Society for Human Resource Management
State Farm
TeraDact Solutions Inc.
Trinity Health
U.S. Chamber of Commerce
Wal-Mart
Wolters Kluwer Health