June 14, 2018

The Honorable Greg Walden
Chairman
Energy and Commerce Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
Energy and Commerce Committee
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Walden and Ranking Member Pallone:

The Confidentiality Coalition appreciates the opportunity to respond to the House Energy and Commerce Committee's request for information on legacy technology challenges to address cybersecurity threats in the healthcare sector. The Confidentiality Coalition is a broad group of organizations working to ensure that policies are implemented to appropriately balance the protection of confidential health information with the efficient and interoperable systems needed to provide high quality healthcare.

The Confidentiality Coalition is comprised of hospitals, medical teaching colleges, health plans, pharmacies, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacy benefit managers, health information and research organizations, clinical laboratories, and others. Through this diversity, we develop a nuanced perspective on the impact of any legislation or regulation affecting the privacy and security of health consumers. The Confidentiality Coalition is pleased to provide our thoughts regarding two potential methods to incentivize solutions to current cybersecurity vulnerabilities in healthcare.

Legacy technologies introduce a complex set of cybersecurity challenges in healthcare organizations, as explained in the Committee's Request for Information. These cybersecurity issues can have an adverse impact on healthcare delivery, finances, data integrity, and trust. The federal government should help organizations to manage these risks by encouraging private entities to invest in and adopt strong cybersecurity policies and practices. Federal incentives to implement and maintain reasonable and appropriate cybersecurity safeguards should include effective regulatory safe harbors or affirmative defenses under privacy laws including HIPAA.

As the Committee knows, the HIPAA Security Rule (at 45 CFR Part 164.302-318) lays out general categories – administrative, physical and technical safeguards – that Covered Entities (CEs) and Business Associates (BAs) must implement, on a required or addressable basis, in order to demonstrate protection of protected health information (PHI) in electronic form. All CEs and BAs are currently required to determine through a risk analysis and risk management process the specific safeguards that are "reasonable and appropriate" for the CE or BA to implement in order meet the required standards and implementation specifications, and mitigate potential threats and vulnerabilities identified.

As a result of a lack of guidance from the Office for Civil Rights (OCR) on the specific safeguards that the agency believes are reasonable and appropriate with respect to each of the Security Rule's implementation specifications (e.g., the appropriate level of encryption to use, or when it is reasonable and appropriate to implement multi-factor authentication), CEs and their BAs have been left to consider a wide range of safeguards, without any assurance that what they are implementing will be considered "reasonable and appropriate" if a violation of the Security Rule or certain provisions of the Privacy and Breach Reporting rules occurs. Layered on top of this uncertainty is the fact that with the promulgation of the final Enforcement Rule in 2013 (as called for by the HITECH Act in 2009) HHS has had the authority to impose civil monetary penalties (CMPs) of up to $1.5 million for a range of violations, including "unknowing" violations – which might be best exemplified by a CE's or BA's loss of access to and/or control over the PHI it creates, maintains, uses or transmits secondary to a ransomware or other cybersecurity attack.

Representing Covered Entities, Business Associates and other stakeholders in the healthcare ecosystem, including biopharmaceutical and health research companies, the Confidentiality Coalition believes that levying a CMP against a CE or BA that has suffered a cyberattack by an outside entity, (e.g., a hacker or other criminal enterprise, or a state actor,) would in no way ameliorate a breach of PHI or other violation of a requirement of Part 164, but instead would only "re-victimize the victim" – *assuming that the CE or BA could <u>demonstrate</u> having made adequate efforts to be in compliance with Part 164 <u>and</u> a cybersecurity program that reasonably complies with a recognized cybersecurity framework developed by the National Institute of Standards and Technology (NIST).*

The Confidentiality Coalition recommends to the Energy & Commerce Committee a piece of legislation that has advanced toward passage in the General Assembly of Ohio. S.B. 220:

- Would establish a legal safe harbor…to a cause of action…that alleges or relates to the failure to implement reasonable security controls, resulting in a data breach. The safe harbor shall apply to all businesses that implement, on a voluntary basis, a cybersecurity program that meets the requirements of the act.
- Is intended to be an incentive and to encourage businesses to achieve a higher level of cybersecurity through voluntary action. The act does not, and is not intended to, create a minimum cybersecurity standard that must be achieved, nor shall it be read to impose liability upon businesses that do not obtain or maintain practices in compliance with the act.

Beyond the compliance with the requirements of Part 164 that is already required of CEs and BAs, and their voluntary subscription to the standards and best practices of the cybersecurity framework published by NIST, the Coalition believes that a safe harbor should be available to CEs and BAs that have had their HIPAA compliance and cybersecurity programs and/or processes audited by a 3rd party and certified/accredited by an organization determined by the Secretary.

<u>Potential Methods for the Implementation of a Safe Harbor</u>:

There are two ways that Congress could direct HHS to help raise the level of CE and BA preparation for cybersecurity attacks, while also leaving flexibility for such safeguards to evolve to address ever-changing threats and vulnerabilities.

First, Congress could require HHS (OCR) to develop a government-recognized certification program for compliance with the information security requirements of Part 164 <u>and</u> the standards of the NIST cybersecurity framework that would help provide certainty for CEs and

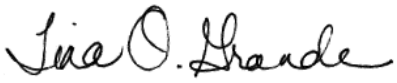
BAs. Under such a program, either CEs or BAs could voluntarily seek a certification or accreditation from an entity recognized by the Secretary and thereby be able to assert a legal safe harbor against HIPAA CMPs in the event of a cyberattack.

Congress could direct HHS (OCR) to issue regular guidance that provides a baseline of cybersecurity safeguards, incorporating the standards and best practices of the NIST framework, and suggest or require that OCR use enforcement discretion and not impose CMPs in the event of a cyberattack against CEs or BAs that have documented the implementation of the named safeguards. This approach would not provide the same level of certainty as the first safe harbor proposal but would give CEs and BAs greater clarity about their obligations to secure PHI against cyberattack.

In part because of the daunting technology and fiscal challenges outlined in the Committee's white paper, the Confidentiality Coalition strongly believes that healthcare entities must be incentivized to update technologies and to fix cyber vulnerabilities. The Confidentiality Coalition recommends developing certification programs to ensure CEs and BAs will comply under the NIST framework and/or issue guidance to provide clear language on CE and BA responsibilities to protect PHI against potential cyberattacks. We believe these two recommendations will help to ensure healthcare stakeholders are held accountable in adhering to current cybersecurity safeguards to protect electronic health information. We do not believe that the "stick" of CMPs should be any part of the solution and have instead proposed a "carrot" to upgrade systems and processes in meaningful and voluntary (and audited) ways.

We thank you for your attention and would be happy to expand upon the ideas in this brief response at any time. Please contact Tina Grande, Senior Vice President for Policy at the Healthcare Leadership Council on behalf of the Confidentiality Coalition at tgrande@hlc.org or at (202) 449-3433 if there are any comments or questions about this letter.

Sincerely,



Tina Grande
Healthcare Leadership Council on behalf of the Confidentiality Coalition