March 22, 2019

The Honorable Mark Warner
United States Senate
703 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Warner:

The Healthcare Leadership Council (HLC) applauds your efforts to work with industry stakeholders to reduce cybersecurity vulnerabilities in the healthcare sector.

HLC is a coalition of chief executives from all disciplines within American healthcare. It is the exclusive forum for the nation's healthcare leaders to jointly develop policies, plans, and programs to achieve their vision of a 21st century healthcare system that makes affordable high-quality care accessible to all Americans. Members of HLC –hospitals, academic health centers, health plans, pharmaceutical companies, medical device manufacturers, laboratories, biotech firms, health product distributors, post-acute care providers, home care providers, and information technology companies – advocate for measures to increase the quality and efficiency of healthcare through a patient-centered approach.

As you know, cybersecurity is a significant challenge for the entire healthcare system. Cybersecurity attacks can have an adverse impact on healthcare safety and delivery, finances, data integrity, and trust. We face the same challenges as other sectors of the economy while simultaneously embarking on a critical mission to transform to a value-based system, drive electronic health information exchange across systems, and engage patients more proactively in their care. We strongly believe the federal government must be a partner and clear supporter of healthcare organizations to effectively counteract cybersecurity threats. HLC members, who are leaders in every healthcare field, agree that cybersecurity is critical to the transformational changes underway in the healthcare industry. The movement to value-based care requires efficient interoperation of health information technology, an engaged and active patient, and trust among all participants.

HLC appreciates the opportunity to work with you to develop a national strategy that improves the safety, resilience, and security of our healthcare industry and offers the following comments:

In response to Question 7

Has the federal government established an effective national strategy to reduce cybersecurity vulnerabilities in the health care sector? If not, what are your recommendations for improvement?

Leadership and Governance

Various state and federal agencies, including the Department of Homeland Security, the Department of Health and Human Services (HHS), the Federal Trade Commission, the Federal Bureau of Investigation, and others have a role to play in helping protect health information held by private sector organizations. It is critical that healthcare organizations, in a time of crisis, have a single trusted partner within HHS to which they can turn – as well as an assurance that cooperation with one agency will not lead to penalties from another.

The Health Insurance Portability and Accountability Act Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) creates an established model for healthcare entities to approach cybersecurity protections. HIPAA's 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 specific safeguards that are "reasonable and appropriate" for the CE or BA to implement to meet the required standards and implementation specifications, and mitigate potential threats and vulnerabilities identified.

The healthcare sector would benefit from additional 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. CEs and BAs seek 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. Concurrent with 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 CEs' or BAs' loss of access to and/or control over the PHI it creates, maintains, uses or transmits secondary to a ransomware or other cybersecurity attack.

HLC 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 not ameliorate a breach of PHI, but instead would only "re-victimize the organizational victim" – assuming that the CE or BA could demonstrate having made adequate efforts to be in compliance with 45 CFR Part 164 and a cybersecurity program that reasonably complies with a recognized cybersecurity framework developed by the National Institute of Standards and Technology (NIST).

Beyond the compliance with the requirements of 45 CFR Part 164 that are already required of CEs and BAs, and their voluntary subscription to the standards and best practices of the cybersecurity framework published by NIST, HLC 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 third party and certified/accredited by an organization determined by the HHS Secretary (e.g., HITRUST or EHNAC).[1] Lack of an HHS deemed or certified third party to assess, audit and accredit the risk posture of an organization contributes to increased risk and costs in the healthcare industry.

[1] Private, non-profit certification and accreditation entities currently exist and work extensively with security agencies, but the Department of Health and Human Services lacks an accreditation or deeming program.

Potential Methods for the Implementation of a Safe Harbor:

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 45 CFR Part 164 and the standards of the NIST cybersecurity framework that would help provide certainty for CEs and BAs. Under such a program, CEs and BAs could voluntarily seek a certification or accreditation from an entity recognized by the HHS Secretary and thereby be able to assert a legal safe harbor against HIPAA CMPs in the event of a cyberattack.

Alternatively, 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 and runs the risk of slow adoption of new standards that is inherent in the federal regulatory process, but would give CEs and BAs improved clarity about their obligations to secure PHI against a cyberattack compared to the current policy.

HLC believes that healthcare entities must be incentivized to update technologies and to fix cyber vulnerabilities. We recommend 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.

In response to Question 8

Are there specific federal laws and/or regulations that you would recommend Congress consider changing in order to improve efforts to combat cyberattacks on health care entities?

Federal Fraud and Abuse Laws

Federal fraud and abuse laws should be modernized to allow healthcare organizations to assist in the acquisition of cybersecurity software without fear of violating the Physician Self-Referral (Stark Law) and the Anti-Kickback Statute. Congress should expand the regulatory exception of the Stark Law and the safe harbor of the Anti-Kickback Statute for donation and financial support of EHR software to cover technology related cybersecurity and information sharing.

HHS Breach Portal

In recognition of the shift to fight cyber threats, Congress and the administration should revisit section 13402(e)(4) of the HITECH Act, requiring the Secretary of HHS to post a list of breaches of unsecured protected health information affecting 500 or more individuals. In revisiting this provision, Congress should maintain consumer notifications of breaches, but should differentiate organizations that use appropriate security practices and were simply unfortunate victims of cyberattacks.

The presence of a company on the public-facing reporting breach website undermines consumer confidence in specific healthcare organizations and the healthcare system as a whole. This penalty should be reserved for organizations that have not adequately protected

their healthcare information – not those who took appropriate precautions but were overcome by major attacks that virtually no organization would have been able to stop. Similarly, HHS should develop a mechanism for healthcare organizations to remove their name from this list by demonstrating that they have resolved security issues and have implemented appropriate information security tools and protocols.

In response to Question 9

Are there additional recommendations you would make in establishing an industry wide strategy to improve cybersecurity in the health care sector?

HLC supported provisions in the Cybersecurity Information Sharing Act (CISA) which encouraged private sector companies to share cyber-related information with each other and the federal government which, in turn, provided necessary liability and anti-trust protections to enable these open lines of communication. However, fear of penalties and unwelcomed publicity can result in a lack of transparency of information on security breaches and ongoing cybersecurity threats. Candid and transparent collaboration among security practitioners in healthcare on best practices, tools, solutions, and threats can have a profound, positive impact on improving risk posture. A national security strategy to improve cybersecurity in healthcare should incentivize the industry to collaborate.

HLC was also supportive of section 405 of CISA which aimed to improve cybersecurity in the healthcare industry. For entities in healthcare, but not currently regulated by the HIPAA Security Rule, we encourage that a national security strategy to improve cybersecurity ensures that these entities apply a consistent set of security standards for the protection of patients and the healthcare industry in general.

Finally, a well-trained, fully resourced, strategically deployed cybersecurity workforce is vital for identifying, assessing, and preventing cyber-related attacks within the healthcare industry. The security of PHI can be improved, and the cost to the healthcare system reduced, through an adequate cybersecurity workforce and expanded training of health professionals in basic cyber hygiene.

Thank you for working on this important issue within healthcare. We look forward to working with you and your staff. Please contact Tina Grande, Senior Vice President for Policy at the Healthcare Leadership Council, at (202) 449-3433 or tgrande@hlc.org with any questions or for additional details on any of the topics mentioned above.

Sincerely,

Mary R. Grealy
President