November 12, 2021

Chairman Gary Peters
Senate Committee on Homeland Security
& Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC, 20510

Ranking Member Rob Portman
Senate Committee on Homeland Security
& Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC, 20510

Chairman Mark Warner
Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, D.C. 20510

Ranking Member Marco Rubio
Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, D.C. 20510

Chairman Jack Reed
Senate Committee on Armed Services
Russell Senate Building, Room 228
Washington, D.C. 20510

Ranking Member James Inhofe
Senate Committee on Armed Services
Russell Senate Building, Room 228
Washington, D.C. 20510

Chairman Bennie Thompson
House Committee on Homeland Security
H2-176 Ford House Office Building
Washington, D.C. 20515

Ranking Member John Katko
House Committee on Homeland Security
H2-117 Ford House Office Building
Washington, DC 20515

Chairman Adam Smith
House Armed Services Committee
2216 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member Mike Rogers
Committee on Armed Services
2216 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Peters, Ranking Member Portman, Chairman Warner, Ranking Member Rubio, Chairman Reed, Ranking Member Inhofe, Chairman Thompson, Ranking Member Katko, Chairman Smith, and Ranking Member Rogers:

On behalf of the Healthcare Information and Management Systems Society (HIMSS) and the American Health Information Management Association (AHIMA), we are writing to provide some thoughts on the Cyber Incident Reporting Act, which would require private sector entities, including those in healthcare, to report certain cyber incidents to the U.S. government. We appreciate the fundamental interests of the government to enhance

the nation's cybersecurity and the vital contributions of public-private collaboration in this endeavor. We also recognize lawmakers' efforts—including Sens. Warner, Rubio, Collins, Peters, and Portman and Reps. Clarke and Katko—and their staff in developing the cyber incident reporting legislation over the last few months and engaging the various stakeholders during this process, which has led to the latest improved amendment that was introduced last week.

HIMSS is a global advisor and thought leader supporting the transformation of the health ecosystem through information and technology. As a mission-driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research, and analytics to advise global leaders, stakeholders and influencers on best practices in health information and technology. Through our innovation engine, HIMSS delivers key insights, education and engaging events to healthcare providers, governments, and market suppliers, ensuring they have the right information at the point of decision. Our members include more than 100,000 individuals, 480 provider organizations, 470 non-profit partners and 650 health services organizations.

AHIMA is a global nonprofit association of health information (HI) professionals. AHIMA represents professionals who work with health data for more than one billion patient visits each year. AHIMA's mission of empowering people to impact health drives our members and credentialed HI professionals to ensure that health information is accurate, complete, and available to patients and clinicians. Our leaders work at the intersection of healthcare, technology, and business, and are found in data integrity and information privacy job functions worldwide.

The legislation would create a compulsory cyber incident notification program to impose additional obligations on the healthcare community. The need for incident notification is clear. As the Senate begins consideration of the FY2022 National Defense Authorization Act (NDAA) next week, we want to make sure the final legislation and ensuing rulemaking provide heightened attention to be given to the following few keys factors critical for the healthcare sector. The most recent bipartisan amendment offer by Senators Gary Peters (D-MI), Rob Portman (R-OH), Susan Collins (R-ME), and Mark Warner (D-VA) clearly addressed the following issues, and our organizations want to reiterate our support for the inclusion of these provisions in final legislation.

- **Patient Safety.** No matter the size or type of the healthcare organization which has been the target of a cyberattack, whether it is a large multi-state health system, small rural practice, medical device manufacturer, or laboratory, patient safety cannot be compromised in providing government notification as the organization responds to the attack. The stress put on healthcare providers during or just after a cyberattack will be extremely high, therefore the requirement around any notifications should be minimal. Time taken away from patient care

may indeed have a negative impact on patient care as well as the quality of care.

- **Clearly Understanding the Impact of a Reported Cyberattack.** To meet the proposed notification requirements, healthcare providers must have time to assess the impact of any cyberattack, especially as it relates to potential patient safety issues. Healthcare providers must have an appropriate and realistic timeframe to investigate an intrusion before being mandated to report to an agency, such as the Cybersecurity and Infrastructure Security Agency (CISA). For this reason, we support a timeline of no less than 72 hours after the cyberattack. Healthcare providers should report an incident after conducting initial mitigation and response efforts. Even relatively minor cyber incidents can require hundreds of personnel hours to assess accurately.

- **Notification Must be High Level in Nature**. We ask that in rulemaking the notification that is required by the government remains at a high level. The need for notification cannot interfere with the ongoing response to the cyberattack. We would re-emphasize that the stress around a cyberattack and concern for patient safety means that the notification should focus simply on:
    - When did the attack occur?
    - What is the scope and impact of the attack, if known?
    - What is currently being done to resolve the issue?

- **Harmonize Federal Reporting Requirements**. Obligations to report significant data breach incidents of Protected Health Information (PHI) at the federal and state levels are already in place and constantly evolving. Congress must align federal and state reporting requirements to ensure that industry resources can combat malicious cyber threats efficiently, rather than creating multiple reports on the same incident for multiple agencies. A single report to one agency should suffice to meet legislative and regulatory mandates. Reporting should be made either to CISA or the appropriate sector risk management agency (SRMA), and subsequently uses its resources to disseminated necessary information to other relevant agencies.

- **Ensure Compliance is Supportive, Not Punitive**. A final bill must create a compliance regime that treats cyberattack victims as victims. A regulatory-based approach that focuses on punitive actions, such as fines or penalties, rather than mutual gains would counter creating a strong national partnership model to address the increasing cyber threats facing the U.S. A reporting program should encourage cooperation and strengthen trust between the public and private sectors, not serve as the basis for later imposing a penalty.

- **Treat Reporting as Bidirectional Sharing and Collaboration.** Cybersecurity information sharing must be bidirectional. Information reported to government

needs to be promptly aggregated, anonymized, analyzed, and shared to foster future cyber incident mitigation and prevention strategies. Lack of timely and effective action or feedback on cyber incidents and events from government is a common shortcoming in the healthcare sector. We need legislation that pushes all parts of the healthcare sector to work together so that they are receiving actionable data and assistance from CISA, HHS, law enforcement, and other agencies to enhance industry groups' security postures.

- **Promote Opportunities to Support Cyber Workforce Development.** Congress and the Administration should look for every opportunity to support and fund the growth of the cyber workforce, not just in healthcare, but in all industries. The proposed additional reporting requirements will not matter if organizations lack qualified cyber professional talent to take the necessary actions in response to an incident. Education programs to increase the diversity in cyber field, encouragement to veterans to enter the cyber workforce, and providing incentives through tuition reimbursement for cyber graduates to move and work in rural healthcare or critical access care settings, could go a long way to meet the cyber-workforce challenges.

HIMSS and AHIMA are committed to working with lawmakers, their staff, and the Administration on cyber incident reporting legislation to strengthen our national security and the protection and resilience of the U.S. healthcare sector. We also believe that this legislation and eventual rulemaking can and must address the healthcare sector concerns with forced notifications. Once passed the law needs to enhance agencies' situational awareness if government is to better inform and partner with healthcare providers and businesses that become cyberattack targets or victims. We thank you for all your efforts and work on this legislation, and if you have questions, or would like additional information, please contact David Gray, HIMSS Director, Government Relations & Connected Health Policy, at dgray@himss.org, Amanda Krzepicki, HIMSS Manager, Government Relations at akrzepicki@himss.org, or Kate McFadyen, AHIMA Director, Government Affairs, at kate.mcfadyen@ahima.org.

Sincerely,

Healthcare Information and Management Systems Society (HIMSS)

American Health Information Management (AHIMA)