American Hospital Association™
Advancing Health in America

Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100

November 15, 2021

Lisa J. Pino, JD
Director, Office for Civil Rights
U.S. Department of Health and Human Services
Humbert H. Humphrey Building
200 Independence Avenue, SW
Washington, DC 20201

Dear Director Pino:

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, our clinician partners – including more than 270,000 affiliated physicians, 2 million nurses and other caregivers – and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) offers our sincere congratulations on your appointment as Director of the Department of Health and Human Services (HHS) Office for Civil Rights (OCR). The AHA has a long history of working with OCR on a variety of issues critical to hospitals and health systems and the patients and communities they serve, and we look forward to continuing this fruitful relationship during your leadership.

As you consider the work of OCR in the coming weeks and months, we urge you to prioritize implementation of H.R. 7898, which requires HHS to consider certain recognized security practices of covered entities and business associates when making determinations related to Health Insurance Portability and Accountability Act (HIPAA) audits, fines and resolution agreement terms. H.R. 7898 in January 2021 was passed with strong bipartisan support in Congress and signed into law. The law appropriately recognizes that covered entities and business associates, like all entities including the Federal Government, can never fully eliminate the risk of cyber attacks. When the inevitable attack occurs, entities should not be penalized, but rather treated as the victims of a crime. The law translates this concept by allowing certain measures of regulatory relief if the HIPAA-covered entity or business-associate victim had in place federally recognized security practices, such as those defined under the National Institute of Standards and Technology (NIST) Cybersecurity Framework and developed under Section 405(d) of the Cybersecurity Act of 2015.

The spirit of this law recognizes that health care organizations should be incentivized to adopt cybersecurity best practices and therefore provided regulatory relief when breaches do occur. This also will encourage cooperation and information sharing with

law enforcement agencies, who need information from the victims to advance their cyber investigations, identify the perpetrators and prevent additional cyber attacks from occurring. Absent the implementation of this law, there may be continued reluctance by health care victims of cyber attacks to cooperate with law enforcement, due to a fear of regulatory repercussions.

Hospitals and health systems invest significant resources to protect patients and their health information from cyber threats, which continue to grow in volume, severity and sophistication. The pandemic and the influx of COVID-19 patients required hospitals and health systems to rapidly expand and deploy network-connected and remote technologies. Unfortunately, this created a vastly expanded attack surface upon which international cyber criminals and foreign spies can leverage against hospitals, health systems and patients.

During the pandemic, hospitals and health systems, already under the stress of caring for COVID-19 patients, suffered a dramatic increase in cyber attacks. Most concerning, there has been a significant increase in high-impact, regionally disruptive ransomware attacks, which have interfered with care delivery and placed patient safety at risk.

Given the continued wave of cyber and ransomware attacks targeting health care, along with this law's importance as a means to incentivize increased adoption of recognized cybersecurity practices and cooperation with the government, we urge OCR to quickly initiate full notice and comment rulemaking, rather than embark on a pre-rulemaking phase as listed in the current version of the Unified Regulatory Agenda.

The AHA and our members stand ready to serve as resources for you and the OCR throughout this process. Thank you for your leadership and again, congratulations on assuming this important role at such a pivotal time in health care. Please contact me if you have questions or feel free to have a member of your team contact Samantha Burch, AHA's director for health IT policy, at sburch@aha.org.

Sincerely,

/s/

Stacey Hughes
Executive Vice President