Secretary Robert F. Kennedy, Jr.
Department of Health and Human Services
200 Independence Ave., SW
Washington, D.C. 20201

Acting Director Anthony Archeval
Office of Civil Rights, Department of Health and Human Services
200 Independence Ave., SW
Washington, D.C. 20201

Submitted via www.regulations.gov

Re: HIPAA Proposed Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information

Dear Secretary Kennedy, and Acting Director Archeaval,

Innovation in cybersecurity practices is critical as attacks on the health care industry continue to rise. The Alliance of Community Health Plans (ACHP) appreciates the Administration freezing the *HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information*, which does not yield meaningfully improved cybersecurity. This Biden Administration proposed rule would introduce unnecessary and duplicative processes, jeopardizing protected health care systems and information. **ACHP urges the Trump Administration to rescind this proposed rule in accordance with the 'Unleashing Prosperity Through Deregulation' Executive Order**.

ACHP is the only national organization advancing a unique payer-provider aligned model of health care that fosters true competition, delivering both high-quality coverage and care. As regional and non-profit insurers, ACHP member companies provide affordable coverage options to tens of millions of Americans in nearly 40 states and D.C., remaining in their markets even when other health plans exit. The sustainability of regional health plans is of paramount importance to an innovative and competitive insurance industry, ensuring consumers are free to select the coverage they want.

ACHP member companies confront cyberattacks on a daily basis and need meaningful support from the Administration. During the cyberattack on UnitedHealth Group's Change Healthcare, ACHP's members acted quickly to minimize disruptions for providers and patients, ensuring timely payments, prompt determinations and reducing administrative processes. To prevent future incidents like this, we encourage the Trump Administration to prioritize strengthening cybersecurity and look forward to working together to create commonsense improvements.

The Biden Administration's proposed rule is overly prescriptive and would impose compliance burdens that do not translate to stronger protections for electronic protected health information. The financial burden of compliance would delay and divert resources from more effective security investments.

Improvements must be commonsense, cost-effective and tailored to individual circumstances/needs of industry partners. ACHP is excited to collaborate with the Trump Administration on commonsense requirements that strengthen cybersecurity standards, rather than jeopardizing health care systems.

The Biden proposed rule also introduces risks rather than meaningful protections. The requirement for HIPAA covered entities to create technology asset inventories and network maps of ePHI flow could serve as a "roadmap" to a company's most vulnerable access points if the information falls into the hands of bad actors. The proposed rule extends beyond a payer's own system and would require a map of the technology assets of business associates of the covered entity. While an inventory and map may be helpful for recovery or auditing purposes, the risk of exposing health plans and their business associates' infrastructure to bad actors outweighs the benefits.

Additionally, the frequency with which these resources should be updated is unrealistic. It may take a health plan months to create these inventories. A health plan would be required to update the inventory any time there is a system change, including any software updates or even minor changes to technology assets. As a result, these resources could become outdated before health plans even finish creating the first iteration. This frequency of updates required would make implementation nearly impossible.

The proposed rule also includes provisions that require covered entities to create written procedures to "restore both its critical relevant electronic information systems and data within 72 hours of the loss." HHS OCR also asked whether it should require covered entities to make those system restorations within 72 hours or otherwise face penalties. **Both proposals are misguided. In the event of a cybersecurity incident, any health care organization is going to work as hard as possible to restore its system as fast as safely possible.** Industry experience consistently shows that the systems and processes necessary to recover from a large-scale cyberattack are significantly greater and more time consuming than those required to recover from a natural disaster. Rushing a covered entity to do so any faster than deemed safe may lead to additional risks of exposure.

We look forward to sharing additional recommendations on how the Administration can strengthen health care cybersecurity and privacy while reducing regulations and fostering innovation. Please contact Michael Bagel, Associate Vice President of Federal Affairs, ACHP (mbagel@achp.org) with any questions.

Regards,

Dan Jones

Dan Jones
Senior Vice President of Federal Affairs
Alliance of Community Health Plans (ACHP)

cc: The Honorable Russell Vought
Amy Gleason, Acting Administrator, Department of Government Efficiency