United States Senate
WASHINGTON, DC 20510

November 15, 2019

The Honorable Alex M. Azar II
Department of Health and Human Services
Office of the Secretary
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Secretary Azar:

I am writing regarding the proposed rule from the Center for Medicare and Medicaid Services (CMS) on Interoperability and Patient Access that would enable third party consumer applications to access sensitive patient and health plan data through application programming interfaces (APIs) [1]. I share the goals of advancing interoperability in patient health information and believe that – implemented appropriately – this proposal could represent a significant step in that direction. However, I urge CMS to take additional steps to address the potential for misuse of these features in developing the rules around APIs. In just the last three years, technology providers and policymakers have been unable to anticipate – or preemptively address – the misuse of consumer technology which has had profound impacts across our society and economy. As I have stated repeatedly, third-party data stewardship is a critical component of information security, and a failure to ensure robust requirements and controls are in place is often the cause of the most devastating breaches of sensitive personal information.

Congress passed the *21st Century Cures Act (P.L. 114-255)* with a key objective of improving the protected exchange of electronic health records across the care continuum. Notably, Section 4003 and 4004 included specific provisions to establish a trusted health information exchange framework and reduce information blocking; it stated that there should be regulation over unreasonable practices to interfere with, prevent, or materially discourage access, exchange, or use of a patient's electronic health records. While your agency has taken substantial steps to implement fundamental aspects of this legislation, it is critical that there are proper safeguards are in place to protect patient privacy and sensitive health information. Moreover, there should be more work done by HHS to facilitate greater access to, and transfer of, electronic health information that does not inadvertently enable dominant IT providers to leverage their control over user data outside of the health care context into nascent markets for personalized health products.

In your proposed rule CMS would specifically require Medicare Advantage (MA) organizations, state Medicaid and Children's Health Insurance Program (CHIP) Fee-for-Service (FFS) programs, Medicaid managed care plans, CHIP managed care entities, and qualified health plans (QHPs) on the federally-facilitated exchanges (FFEs) to allow patients to access their personal health information electronically through an open application programming interface (API). Data

should be made available through an API so that third party software applications can connect to, process, and make the data available to patients.

I agree that patients should have an ability to easily acquire their health information. The rule is in many ways consistent with bipartisan legislation I have introduced in Congress – *the Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act*, which requires our nation's largest social media companies to make user data portable, and make their services interoperable with other platforms.

Common to both my bill and the proposed rule is a recognition that consumers should have a right to possess their data – and share it with authorized third parties that will protect it. Both proposals also seek to address the control over consumer data that incumbents wield, often to the detriment of new, innovative providers. Across all sectors – including health care – innovative products and services, increasingly dependent upon machine learning, rely on user data as the single most important productive input to innovation and customization. Importantly, however, any approach must balance innovation and ease of access with privacy, security, and a commitment to robust competition. Further, any effort must ensure that such access redounds to the benefit of *patients* – and that data, once shared with new providers, is not commercialized in ways that benefit those providers without direct benefits or compensation to users.

As CMS and HHS move forward with this needed rule – I urge you to include clear standards and defined controls for all stakeholders that ensure third party software applications accessing patient data through APIs are effectively protecting patient information and that patients are appropriately (and routinely) informed, in clear and particularized ways, how their data is used. Such standards in a final rule should include at a minimum:

- Patient Access to Data – A guarantee that patients will have ready access to their personal health data and an ability to regularly monitor and ensure the accuracy of such information. Patients should be informed of all commercial uses of their data, including any third parties their data has been shared with (even if it has alleged to have been anonymized). Patients should also have the right to withhold consent for their data to be shared with third parties, or used in new ways without their consent. Patients should also reserve the right to have third party users dispose of their data upon request.
- Adequate Privacy and Security Safeguards – Ensure participating stakeholders can adequately safeguard patient information by using existing best practices for secure storage and complying with applicable breach notification requirements. Moreover, HHS must work with the FTC and state attorneys general to develop mechanisms to report, supervise, and prosecute privacy and security lapses.
- Documentation of the open API specifications and required security controls – Provide clear attestation of the open API specifications as defined for patient data, the security requirements and controls imposed on healthcare providers, and the third-party platform obligations in managing patient data.
- Patient Consent and Terms of Use – CMS and HHS should work proactively with the patient, provider and payer community to ensure users have informed proactive consent when user data is shared with a third party. In addition – there should be clear protections in place to ensure third party vendors use patient data solely for purposes in

which the patient has expressly given informed proactive consent, including cases where patient information may be sold, and that patients retain the right to direct any party that has acquired their data to delete it upon request. Further, those accessing patient data should be prohibited from conditioning continued access on agreement by the patient to share their data with third parties.

Thank you for your consideration your commitment to advancing interoperability to improve patient care. I believe the outline I have shared would strengthen and ensure the rule achieves its intended purpose. It is my hope and belief that we can achieve both a higher level of interoperability and patient access to their data, as well as, strong protections for that information. I look forward to continued work with you on this important issue and our shared goals.

Sincerely,

Mark R. Warner
United States Senator