



July 31, 2024

The Honorable Xavier Becerra
Secretary
Department of Health & Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Secretary Becerra,

AARP, which advocates for the more than 100 million Americans aged 50 and older, is reaching out to you to share our concern over the serious threat cyberattacks are posing to America's health care system, as evidenced by recent incidents such as the hack of Change Health Care, Ascension, and others. Persistent vulnerabilities in the American health care system are putting our sensitive personal, financial, and health information at risk of being exposed and exploited.

Millions of Americans have had their private data hacked in cyberattacks on health insurance companies and providers. These attacks must serve as a wakeup call for the entire health care industry. Maintaining the integrity of data should be at the forefront when developing and deploying increasingly complex online-based platforms. Current laws and regulations should also be examined to ensure that they are sufficient to protect patients and health care providers alike. We appreciate the steps that the Administration is already taking, as outlined in the June 10 fact sheet, and urge continued efforts to protect the sensitive data in our health care system.

We are particularly concerned that after the recent attacks, some consumers have still not been directly notified or encouraged to take steps to protect themselves. People cannot afford to wait months until an investigation verifies that their data was compromised. We urge HHS to work with the entities targeted in cyberattacks to quickly notify all consumers who may have been impacted. This should include efforts to widely publicize any offers for potential victims to sign up for credit monitoring and identity theft protection. After notification, we ask that HHS continue to work with UnitedHealth Group, Ascension, and other entities to provide any additional support necessary to mitigate the negative impacts that a breach may have on consumers' personal or financial security.

Beyond the immediate impacts and fallout of the recent cyberattacks, these incidents underscore the ongoing risks that patients bear of having their personal health and financial information compromised. We recommend HHS/CMS conduct a holistic analysis of IT vulnerabilities both within federally-administered health care systems and commercial entities that handle such data. The goal should be not only protecting against future attacks but developing notification and contingency plans to minimize impact when such attacks do occur. We are deeply troubled by the many stories of patients who have faced disruptions in their care or have had to inappropriately pay large out-of-pocket expenses to receive care during recent attacks on processing systems without sufficient contingency plans.

Thank you for the opportunity to share our thoughts on this major threat to our nation's health care system. While there is no single answer for how to protect against cyberattacks, America's consumers are counting on the commitment and focus of every part of the health care sector to do better. AARP is ready to help in any way that we can. If you have any questions, please feel free to reach out to me directly or have your staff contact Brendan Rose (brose@aarp.org) on Government Affairs team.

Sincerely,

A handwritten signature in purple ink that reads "Bill Sweeney". The signature is fluid and cursive, with a long horizontal stroke at the end.

Bill Sweeney
Senior Vice President
Government Affairs