

BERNARD SANDERS, VERMONT, CHAIR

PATTY MURRAY, WASHINGTON  
ROBERT P. CASEY, JR., PENNSYLVANIA  
TAMMY BALDWIN, WISCONSIN  
CHRISTOPHER MURPHY, CONNECTICUT  
TIM Kaine, VIRGINIA  
MARGARET WOOD HASSAN, NEW HAMPSHIRE  
TINA SMITH, MINNESOTA  
BEN RAY LUJÁN, NEW MEXICO  
JOHN W. HICKENLOOPER, COLORADO  
EDWARD J. MARKEY, MASSACHUSETTS

BILL CASSIDY, LOUISIANA  
RAND PAUL, KENTUCKY  
SUSAN M. COLLINS, MAINE  
LISA MURKOWSKI, ALASKA  
MIKE BRAUN, INDIANA  
ROGER MARSHALL, KANSAS  
MITT ROMNEY, UTAH  
TOMMY TUBERVILLE, ALABAMA  
MARKWAYNE MULLIN, OKLAHOMA  
TED BUDD, NORTH CAROLINA

## United States Senate

COMMITTEE ON HEALTH, EDUCATION,  
LABOR, AND PENSIONS

WASHINGTON, DC 20510-6300

WARREN GUNNELS, MAJORITY STAFF DIRECTOR  
AMANDA LINCOLN, REPUBLICAN STAFF DIRECTOR

[www.help.senate.gov](http://www.help.senate.gov)

March 20, 2024

### VIA ELECTRONIC TRANSMISSION

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

Dear Secretary Becerra:

Cybersecurity attacks pose a grave risk to patients and payers. As the Sector Risk Management Agency (SRMA) for the Health and Public Health (HPH) sector, the Department of Health and Human Services (HHS) is the primary coordinating body for cybersecurity incidents. However, recent cyberattacks raise questions about HHS' ability to effectively execute this role.

The recent cyberattack involving Change Healthcare has been enormously disruptive to the health care sector, and has hindered patients from accessing timely care. HHS' response to this incident has been inadequate, as the agency has not provided sufficient information to Congress about the attack at a time when the health care sector faces record cybersecurity incidents.<sup>1</sup> For example, Change Healthcare first reported the cyberattack on February 21, yet HHS only released its first formal statement outlining steps for affected parties on March 5 — nearly two weeks later. This incident has impacted providers across the country, potentially putting as many as 25% of practices on the verge of bankruptcy.<sup>2</sup> The breadth of this situation requires regular communication and immediate action, especially with members of Congress.

Providing up-to-date information and coordination about cybersecurity incidents is one of HHS' key duties as SRMA. It is troubling that HHS has failed in this critical area. As such, in an effort to better understand the facts surrounding Change Healthcare's cybersecurity incident, I ask that you answer the following questions, on a question-by-question basis, by **April 3, 2024**:

---

<sup>1</sup> Emily Olsen, *Patient records exposed in data breaches doubled in 2023*, HEALTHCARE DIVE (Jan. 18, 2024), <https://www.healthcaredive.com/news/patient-records-exposed-healthcare-data-breaches-double-fortified-health-security/704917/>.

<sup>2</sup> Dan Diamond and Daniel Gilbert, *Officials rush to help hospitals, doctors affected by Change Healthcare hack*, THE WASHINGTON POST (Mar. 5, 2024), <https://www.washingtonpost.com/health/2024/03/05/change-healthcare-insurance-hack-hhs-plan/>.

1. When did HHS receive notification from Change Healthcare that a cyberattack occurred?
2. Change Healthcare first reported that a cyberattack had occurred on February 21. However, HHS did not issue a formal statement outlining steps for affected parties until March 5.
  - a. Why did HHS wait 13 days to issue this statement?
  - b. How does HHS intend to improve its role in providing regular updates to Congress?
3. Has HHS identified any unauthorized access or breach of any federal systems as a result of the cyberattack?
4. What steps is HHS taking to ensure that affected providers do not suffer from any secondary cybersecurity intrusions as a result of the original incident?
5. What tools has HHS offered to affected entities to identify and patch any cybersecurity vulnerabilities?
6. What steps is HHS taking to ensure that there are adequate flexibilities for providers to submit claims for reimbursement to UnitedHealth Group (UHG) or other private payers in light of the Change Healthcare attack?
7. Will HHS provide an extension for the submission of claims to the federal Independent Dispute Resolution (IDR) process under the No Surprises Act for providers and payers affected by the Change Healthcare attack?
8. What steps is HHS taking to ensure that prevailing parties under the No Surprises Act receive timely payment by entities affected by the Change Healthcare attack?
9. The Administration for Strategic Preparedness & Response (ASPR) is designated to serve as the SRMA on behalf of HHS. ASPR, however, has thus far shared limited information about the cyberattack.
  - a. What specific steps has ASPR taken to coordinate the response to this incident?
  - b. How does it intend to communicate additional details to Congress?
10. How is HHS coordinating its immediate response with other federal agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Securities and Exchange Commission (SEC)?
11. ASPR has stated that it intends to make improvements to its cybersecurity reporting and monitoring systems for future cybersecurity incidents. Please provide specific improvements it intends to make, the anticipated timeline for making such improvements, and any limitations ASPR has identified that need improvements.

Sincerely,

*Bill Cassidy, M.D.*

---

Bill Cassidy, M.D.  
Ranking Member  
U.S. Senate Committee on Health,  
Education, Labor, and Pensions



---

Tommy Tuberville  
United States Senator