



# THE AHA RESPONDS

The cyberattack against UnitedHealth Group’s Change Healthcare that began on Feb. 21 represents the most serious incident of its kind leveled against a U.S. health care organization.

In response to this crisis, the AHA and its member hospitals and health systems joined together to alert the government, media and public about the seriousness of the situation. Together, we secured needed support for patients and hospitals caring for them, as well as shined a light on the issues that led to the massive scope of the impact.

## AHA MEMBER CALL

More than 3,000 hospital and health system executives join an AHA member call with representatives from HHS, CISA and the FBI.

## MEDIA OUTREACH

We take our story to the national media, appearing on multiple news programs and in influential publications.

## AHA URGES CONGRESS TO ACT

AHA asks Congress to get involved and help minimize fallout from attack.

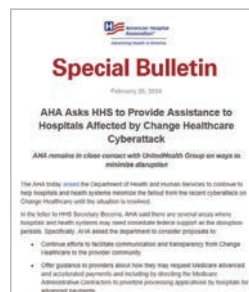
## SURVEYING IMPACT & APPLYING PRESSURE

We maintain focus on the issue – releasing a survey documenting the impact of the attack and bringing the issue to the stage at the 2024 AHA Annual Membership meeting in mid-April.



## CHANGE HEALTHCARE'S CYBERATTACK

Change Healthcare is hit with a cyberattack and begins to disconnect its systems. AHA becomes aware of the network disruptions and reaches out to the FBI, Department of Health and Human Services (HHS), and Cybersecurity and Infrastructure Security Agency (CISA). AHA is in direct contact with Change and UnitedHealth Group to obtain information on the scope and anticipated duration of the impact.



## ALERTING HHS

AHA contacts Xavier Becerra, HHS Secretary, to emphasize the implications of the attack on patient care, and to ask for continued support.



## ADDRESSING FINANCIAL RELIEF

And in early March when Change describes its temporary funding program, the AHA quickly points out its flaws. Change makes improvements to its program.



## CMS'S PAYMENT PROGRAM

CMS formally announces an accelerated and advance payment program, which the AHA welcomes and shares with the field.







## BRIEFING CONGRESS & ALERTING THE MEDIA

In advance of House and Senate hearings with UnitedHealth Group CEO, the AHA executes a strategic campaign to inform both media and Congressional members about the challenges members continue to face.

“It is long past time to do a comprehensive scrub of United Health’s anti-competitive practices.”

**- Sen. Ron Wyden**  
D-Ore.

“The reality that hospitals and providers are facing is wildly different from the rosy picture that you have painted.”

**- Sen. Marsha Blackburn**  
R-Tenn.



# IT'S BECAUSE OF YOU THAT THIS WAS POSSIBLE.

## AHA'S TESTIMONY IN DC

John Riggi, AHA's national advisor for cybersecurity and risk and a former FBI agent, testifies in front of Congress on the need for support.

## CONGRESS REACTS

Congressional lawmakers hold two hearings with UnitedHealth Group CEO at which they hold the organization accountable and criticize its response to the attack. The hospital perspective comes through loud and clear via lawmakers' comments.

Later that month, our continued work behind the scenes ensures that Change Healthcare, not providers, must notify affected patients.

UnitedHealth Group is having to answer for this crisis, and long overdue questions about its outsized power and influence are finally being raised. The AHA continues to closely monitor the landscape for any new threats.

“How did consolidation in the health insurance industry reach such a state where a single ransomware attack on one company cripple the flow of payments and claims for months?”

**- Rep. Morgan Griffith**  
R-Va.

“It's almost a too big to fail insurer.”

**- Sen. Bill Cassidy**  
R-La.

“It is wrong that health care providers, pharmacists and patients bear the brunt of a failure by a corporation that earned \$371 billion last year to even prevent or quickly remedy the situation.”

**- Rep. Frank Pallone**  
D-N.J.



The AHA stands ready to support our members in their work on this critical issue. Our Cybersecurity and Risk Advisory Services, led by John Riggi, former FBI cyber executive and expert on health care cybersecurity, provides consultation and strategy in a range of areas to help defend against cyber and physical threats.

Let us know how we can help you. Contact John Riggi at [jriggi@aha.org](mailto:jriggi@aha.org).