

April 15, 2024

The Honorable Brett Guthrie
Chairman
Subcommittee on Health
Energy and Commerce Committee
United States House of Representatives
Washington, DC 20515

The Honorable Anna Eshoo
Ranking Member
Subcommittee on Health
Energy and Commerce Committee
United States House of Representatives
Washington, DC 20515

The Honorable Larry Bucshon, MD
Vice Chair
Subcommittee on Health
Energy and Commerce Committee
United States House of Representatives
Washington, DC 20515

Dear Chairman Guthrie, Vice Chair Bucshon, and Ranking Member Eshoo:

Thank you for reaching out to the National Association of Insurance Commissioners (NAIC) for comments on the Change Healthcare ransomware attack, and we commend the Committee for examining this important issue. The NAIC represents the lead insurance regulators in the 50 states, the District of Columbia, and 5 United States Territories.

When news broke that Change Healthcare's systems were down due to a cyberattack there was great concern among state regulators, but our concerns only grew as the significance of the event quickly became apparent. What initially seemed to be an incident limited to United Health Group (UHG) soon became a crisis that impacted the operations of insurance companies, providers, and pharmacists - and thus consumers - nationwide. There were also questions about whether private information was obtained by the criminals responsible for this attack. As state regulators collaborated with each other, and engaged UHG and Change Healthcare, we gained an understanding of the growing issue and began reaching out to insurance carriers for more information and encouraged them to provide immediate assistance and flexibilities to providers to ensure care and access to prescription drugs continued without significant delay.

States issued official bulletins and memos to their carriers urging them to take actions to keep funds flowing to providers, allow prior authorization flexibility, and provide timely updates on the status of their various systems.

To be clear, Change Healthcare was the victim of a crime, but also has a responsibility to follow applicable rules and laws of the states for data security that may apply to it. We are currently working to determine the applicability of state rules and laws to Change Healthcare, which itself is not a risk-bearing insurance entity, and determining whether additional protections and contingencies are necessary to ensure consumers receive care and providers receive reimbursement in a timely manner and that regulators have the authority they need to enforce such requirements.

State regulators are now working together to determine if impacted carriers complied with all existing state cybersecurity and consumer protections regulations. For example, the NAIC developed cybersecurity and claims settlement regulations that some states have adopted. You can find those here:

Cybersecurity:

<https://content.naic.org/sites/default/files/inline-files/MDL-668.pdf>

Unfair Claims Settlement:

<https://content.naic.org/sites/default/files/inline-files/MDL-900.pdf>

The NAIC has created a multi-state Steering Group to look at how the cyberattack unfolded, assess how insurance carriers and other impacted entities reacted, and facilitate discussions about the response and recovery efforts with UHG's and Change Healthcare's senior management. The Steering Group, which is in the early stages of their work, can keep the Subcommittee updated on their progress and findings. While corporate protocols, IT security, and appropriate regulatory requirements can minimize the risk of a ransomware attack, we acknowledge that such attacks can and will still occur, and some will be successful. We are committed to examining whether UHG and Change Healthcare lived up to their obligations under the law, communicating with impacted stakeholders, and in the weeks ahead analyzing what we can do better to assist consumers and mitigate the damage from ransomware and cyber security threats to the insurance sector.

As we look forward, state regulators hope to learn from this attack and be more prepared should it happen again. One overarching concern is how an attack on a single entity could impact the delivery and reimbursement of healthcare nationwide. Regulators and policy makers may need to consider the significance of this event and whether additional redundancies or contingency plans need to be developed to prevent such a crisis in the future. Part of our collective work should be to assess whether state and federal regulators have sufficient authority during a cyberattack or comparable emergency to require certain actions by health insurers and healthcare providers. What flexibilities, consumer protections, notifications, liability protections, etc., are necessary to avoid distributions in care? We intend to focus on these important questions, and welcome engagement with this Subcommittee as our work progresses.

We applaud the Subcommittee for holding this hearing and look forward to working with you and other Members of Congress and the Administration to improve the resilience of the health insurance sector for the benefit of its policyholders.

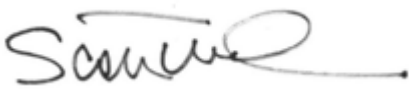
Sincerely,



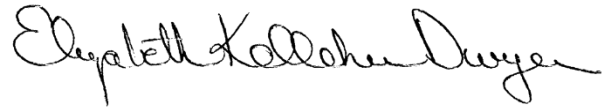
Andrew N. Mais (He/Him/His)
NAIC President
Commissioner
Connecticut Insurance Department



Jon Godfread
NAIC President-Elect
Commissioner
North Dakota Insurance Department



Scott White
NAIC Vice President
Commissioner
Virginia Insurance Department



Elizabeth Kelleher Dwyer
NAIC Secretary-Treasurer
Director
Rhode Island Department of Business
Regulation