

**Congress of the United States**  
**House of Representatives**  
Washington, DC 20515

March 21, 2024

The Honorable Chiquita Brooks-LaSure  
Administrator  
Center for Medicare and Medicaid Services  
200 Independence Ave, S.W.  
Washington, D.C. 20201

Dear Administrator Brooks-LaSure:

We write to express concern regarding the Change Healthcare ransomware attack that has impacted a significant portion of the American health care system. On February 21st, UnitedHealth Group, and its division, Optum, Inc., reported that their subsidiary, Change Healthcare, had fallen victim to a ransomware cyberattack. This attack has disrupted the lives of patients, doctors, pharmacists, and countless other health industry professionals due to outages in systems used for medical billing and insurance claims. If not addressed quickly, alarming reports of the negative implications for our health care system, threats to patient care, access to critical medications, and the ability of physicians to operate their practices will continue. We urge the Center for Medicare and Medicaid Services (CMS) to use existing statutory authorities to hold relevant actors accountable to ensure promised support is delivered to America's providers.

The Change Healthcare disruption is significant given the current challenges physicians are already facing, such as low reimbursement, ongoing regulatory burden, rising practice costs, and burnout. Many practices, particularly small and independent practices in rural and underserved areas, will not be able to survive without timely help. According to an estimate from Compass Point analyst, Max Reale, based on the volume of impacted health care claims, providers are losing between \$500 million and \$1 billion in daily revenue compared to 2023,<sup>1</sup> posing severe financial challenges for medical practices already strained for liquidity. Change Healthcare impacts 1 in 3 patient records in the United States<sup>2</sup>, these delays in claims processing compounded with ongoing workforce shortages and rising inflation will have a severe impact on patient access to timely care.

---

<sup>1</sup> Health Care Providers losing up to \$1b a day from Cyberattack. Accessed March 11, 2024.  
<https://www.axios.com/2024/03/11/hospitals-doctors-cyberattack-losses>.

<sup>2</sup> "Healthcare Technology & Business Solutions Company." Change Healthcare. Accessed March 11, 2024.  
<https://www.changehealthcare.com/>.


While we acknowledge the Department of Health and Human Services and CMS have put out multiple statements recognizing the disruption and indicating they would work with the Medicare Administrative Contractors (MACs) and insurers to provide some resources and administrative flexibility for providers, we urge immediate action to ensure all, not just some, providers are getting the resources and information they need. Additionally, we have been made aware that the commercial insurer payments provided have been inadequate, unpredictable, and slow, with little support for providers in the process. Therefore, we encourage CMS to use their existing authority to ensure timely resolution by ensuring physicians have the information and resources they need and communicating with affected payers to accomplish that goal.

Our health care system is and will remain a critical infrastructure, and the risks of cybersecurity attacks are a domestic and international threat to the ecosystem at large. The result of the breach has far-reaching implications for providers, patients, health systems, health plans, and vendors. This situation sets a dangerous precedent for potential impacts moving forward if our health systems are not adequately protected. It is critical that Change Healthcare operations are reestablished safely as soon as possible, and CMS should work to communicate with providers and inform them of the resources available to them.

Sincerely,



Michael C. Burgess, M.D.  
Member of Congress



Gregory F. Murphy, M.D.  
Member of Congress



Brad R. Wenstrup, D.P.M.  
Member of Congress



A. Drew Ferguson IV  
Member of Congress



---

Earl L. "Buddy" Carter  
Member of Congress



---

Brian Babin, D.D.S.  
Member of Congress



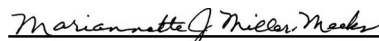
---

John Joyce, M.D.  
Member of Congress



---

Diana Harshbarger, Pharm.D.  
Member of Congress



---

Mariannette Miller-Meeks,  
M.D.  
Member of Congress



---

Jefferson Van Drew  
Member of Congress



---

Neal P. Dunn, M.D.  
Member of Congress



---

Andy Harris, M.D.  
Member of Congress



---

Michael K. Simpson  
Member of Congress



---

Rich McCormick, MD, MBA  
Member of Congress

*Larry Bucshon*

---

Larry Bucshon, M.D.

Member of Congress

**Congress of the United States**  
**House of Representatives**  
Washington, DC 20515

March 21, 2024

The Honorable Chiquita Brooks-LaSure  
Administrator  
Center for Medicare and Medicaid Services  
200 Independence Ave, S.W.  
Washington, D.C. 20201

Dear Administrator Brooks-LaSure:

We write to express concern regarding the Change Healthcare ransomware attack that has impacted a significant portion of the American health care system. On February 21st, UnitedHealth Group, and its division, Optum, Inc., reported that their subsidiary, Change Healthcare, had fallen victim to a ransomware cyberattack. This attack has disrupted the lives of patients, doctors, pharmacists, and countless other health industry professionals due to outages in systems used for medical billing and insurance claims. If not addressed quickly, alarming reports of the negative implications for our health care system, threats to patient care, access to critical medications, and the ability of physicians to operate their practices will continue. We urge the Center for Medicare and Medicaid Services (CMS) to use existing statutory authorities to hold relevant actors accountable to ensure promised support is delivered to America's providers.

The Change Healthcare disruption is significant given the current challenges physicians are already facing, such as low reimbursement, ongoing regulatory burden, rising practice costs, and burnout. Many practices, particularly small and independent practices in rural and underserved areas, will not be able to survive without timely help. According to an estimate from Compass Point analyst, Max Reale, based on the volume of impacted health care claims, providers are losing between \$500 million and \$1 billion in daily revenue compared to 2023,<sup>1</sup> posing severe financial challenges for medical practices already strained for liquidity. Change Healthcare impacts 1 in 3 patient records in the United States<sup>2</sup>, these delays in claims processing compounded with ongoing workforce shortages and rising inflation will have a severe impact on patient access to timely care.

---

<sup>1</sup> Health Care Providers losing up to \$1b a day from Cyberattack. Accessed March 11, 2024.  
<https://www.axios.com/2024/03/11/hospitals-doctors-cyberattack-losses>.

<sup>2</sup> "Healthcare Technology & Business Solutions Company." Change Healthcare. Accessed March 11, 2024.  
<https://www.changehealthcare.com/>.


While we acknowledge the Department of Health and Human Services and CMS have put out multiple statements recognizing the disruption and indicating they would work with the Medicare Administrative Contractors (MACs) and insurers to provide some resources and administrative flexibility for providers, we urge immediate action to ensure all, not just some, providers are getting the resources and information they need. Additionally, we have been made aware that the commercial insurer payments provided have been inadequate, unpredictable, and slow, with little support for providers in the process. Therefore, we encourage CMS to use their existing authority to ensure timely resolution by ensuring physicians have the information and resources they need and communicating with affected payers to accomplish that goal.

Our health care system is and will remain a critical infrastructure, and the risks of cybersecurity attacks are a domestic and international threat to the ecosystem at large. The result of the breach has far-reaching implications for providers, patients, health systems, health plans, and vendors. This situation sets a dangerous precedent for potential impacts moving forward if our health systems are not adequately protected. It is critical that Change Healthcare operations are reestablished safely as soon as possible, and CMS should work to communicate with providers and inform them of the resources available to them.

Sincerely,



Michael C. Burgess, M.D.  
Member of Congress



Gregory F. Murphy, M.D.  
Member of Congress



Brad R. Wenstrup, D.P.M.  
Member of Congress



A. Drew Ferguson IV  
Member of Congress

*Earl L. "Buddy" Carter*

---

Earl L. "Buddy" Carter  
Member of Congress

*Brian Babin*

---

Brian Babin, D.D.S.  
Member of Congress

*John Joyce*

---

John Joyce, M.D.  
Member of Congress

*Diana Harshbarger*

---

Diana Harshbarger, Pharm.D.  
Member of Congress

*Mariannette Miller Meeks*

---

Mariannette Miller-Meeks,  
M.D.  
Member of Congress

*Jefferson Van Drew*

---

Jefferson Van Drew  
Member of Congress

*Neal P. Dunn*

---

Neal P. Dunn, M.D.  
Member of Congress

*Andy Harris M.D.*

---

Andy Harris, M.D.  
Member of Congress

*Michael K. Simpson*

---

Michael K. Simpson  
Member of Congress

*Rich McCormick*

---

Rich McCormick, MD, MBA  
Member of Congress



---

Larry Bucshon, M.D.

Member of Congress