DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Director

Office for Civil Rights

Washington, D.C. 20201

March 13, 2024

Re: Cyberattack on Change Healthcare

Dear Colleagues:

The Office for Civil Rights (OCR) is aware that Change Healthcare, a unit of UnitedHealth Group (UHG), was impacted by a cybersecurity incident in late February that is disrupting health care and billing information systems nationwide. The incident poses a direct threat to critically needed patient care and essential operations of the health care industry.

OCR administers and enforces the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules, which establish the minimum privacy and security requirements for protected health information and breach notification requirements that covered entities (health care providers, health plans, and clearinghouses) and their business associates must follow. We are committed to ensuring access to care while enforcing laws that bolster patient privacy and security.

Given the unprecedented magnitude of this cyberattack, and in the best interest of patients and health care providers, OCR is initiating an investigation into this incident. OCR's investigation of Change Healthcare and UHG will focus on whether a breach of protected health information occurred and Change Healthcare's and UHG's compliance with the HIPAA Rules.

OCR's interest in other entities that have partnered with Change Healthcare and UHG is secondary. While OCR is not prioritizing investigations of health care providers, health plans, and business associates that were tied to or impacted by this attack, we are reminding entities that have partnered with Change Healthcare and UHG of their regulatory obligations and responsibilities, including ensuring that business associate agreements are in place and that timely breach notification to HHS and affected individuals occurs as required by the HIPAA Rules.

Safeguarding protected health information is a top priority. OCR would also like to share the following resources to assist you in protecting your records systems and patients from cyberattacks:

- **OCR HIPAA Security Rule Guidance Material** – This webpage provides educational materials to learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic protected health information. Materials include a Recognized Security Practices Video, Security Rule Education Paper Series, HIPAA Security Rule Guidance, OCR Cybersecurity Newsletters, and more.

- **OCR Video on How the HIPAA Security Rule Protects Against Cyberattacks** – This video discusses how the HIPAA Security Rule can help covered entities and business associates defend against cyberattacks. Topics include breach trends, common attack vectors, and findings from OCR investigations.
- **OCR Webinar on HIPAA Security Rule Risk Analysis Requirement** – This webinar discusses the HIPAA Security Rule requirements for conducting an accurate and thorough assessment of potential risks and vulnerabilities to electronic protect health information and reviews common risk analysis deficiencies OCR has identified in its investigations.
- **HHS Security Risk Assessment Tool** – This tool is designed to assist small- to medium-sized entities in conducting an internal security risk assessment to aid in meeting the security risk analysis requirements of the HIPAA Security Rule.
- **Factsheet: Ransomware and HIPAA** – This resource provides information on what is ransomware, what covered entities and business associates should do if their information systems are infected, and HIPAA breach reporting requirements.
- **Healthcare and Public Health (HPH) Cybersecurity Performance Goals** – These voluntary, health care specific cybersecurity performance goals can help health care organizations strengthen cyber preparedness, improve cyber resiliency, and protect patient health information and safety.

OCR is committed to helping health care entities understand health information regulations and to collaboratively working with entities to navigate the serious challenges we face together. OCR encourages all entities to review the cybersecurity measures they have in place with urgency to ensure that critically needed patient care can continue to be provided and that health information is protected.

Sincerely,

/s/

Melanie Fontes Rainer

Director, Office for Civil Rights