March 21, 2024

Melanie Fontes Rainer
Director
Office for Civil Rights
U.S. Department of Health and Human Services
Hubert H. Humphrey Building
200 Independence Avenue, S.W., Room 515F
Washington, DC 20201

Dear Director Fontes Rainer:

The American Hospital Association (AHA) and Federation of American Hospitals (FAH) write in response to your March 13 letter regarding the cyberattack on Change Healthcare.

America's hospitals and health systems are committed to safeguarding the privacy and security of their patients' medical information, claims and billing information, and personal information. As such, the AHA and FAH appreciate the Department of Health and Human Services' (HHS) Office for Civil Rights' (OCR) efforts to determine whether a breach of protected health information occurred in connection with this cyberattack, as well as Change Healthcare's and UnitedHealth Group's compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules. We also are grateful that OCR recognizes, as you wrote in your March 13 letter, that this cybersecurity incident "is disrupting health care and billing information systems nationwide" and "poses a direct threat to critically needed patient care and essential operations of the health care industry." The fallout from this attack is ongoing and will continue for many months.

The AHA and FAH also appreciate your clarification that OCR is not prioritizing investigations of health care providers and that your interest in "other entities that have partnered with Change Healthcare and UHG is secondary." **We remain concerned, however, that OCR may require hospitals to make breach notifications to HHS and affected individuals, if it is later determined that a breach occurred.**

In that event, presumably UnitedHealth Group and Change Healthcare will be required to make breach notifications. **We are seeking additional clarification that hospitals and other providers do not have to make *additional* notifications if UnitedHealth Group and Change Healthcare are doing so already.** Providing duplicative notifications is inconsistent with Change Healthcare's regulatory obligations. In most situations, Change Healthcare is acting as a clearinghouse and is a covered entity in this capacity. As a covered entity, Change Healthcare has the duty to notify OCR and the impacted individuals. Even where Change Healthcare acts as a business associate, HIPAA authorizes Change Healthcare to issue these notifications for a more streamlined approach. **Given the scope and scale of the cyberattack on Change Healthcare, without a unified notification process, patients could possibly face multiple notifications of this same breach, which could unnecessarily increase public confusion, misunderstandings and added stress.**

To be clear: America's hospitals and health systems have long honored HIPAA's core privacy objectives. Our concern is simply that requiring breach notifications in these

circumstances will confuse patients and impose unnecessary costs on hospitals, particularly when they have already suffered so greatly from this attack. Indeed, in response to a recent AHA survey of hospitals with nearly 1,000 responses, hospitals, health systems and other providers are experiencing extraordinary reductions in cash flow, threatening their ability to make payroll and to acquire the medical supplies needed to provide care. In the same survey, 94% of hospitals reported that the Change Healthcare cyberattack was impacting them financially, with more than half reporting the impact as "significant or serious." A third of the survey respondents indicated that the attack has disrupted more than half of their revenue.

Now is not the time to impose additional costs on America's health care providers and the patients they serve. This is particularly true because hospitals, health systems, and other providers were *not* the direct targets of this cyberattack. As your March 13 letter recognizes, the target of this attack — and the source of any potential breach — was Change Healthcare and its parent corporation, UnitedHealth Group. They are in the best position to make this notification.

We therefore urge OCR to exercise its enforcement discretion and clarify that Change Healthcare and UnitedHealth Group will be required to make any breach notifications — *not* hospitals, health systems and other downstream victims of this attack. **Given what you rightly describe as the "unprecedented magnitude" of this attack, we urge OCR to preemptively relieve hospitals and other providers of any potential breach notification burdens, which would cause significant patient confusion and undoubtedly be costly and resource-intensive.**

We thank OCR, HHS, and others in the Administration for their ongoing support. We continue to stand ready to work with you, Change Healthcare and its corporate ownership to minimize any further disruption to patient care as a result of this attack. Please contact us if you have questions.

Sincerely,

Chad Golder

/s/

General Counsel
American Hospital Association

Katie Tenoever

/s/

General Counsel
Federation of American Hospitals