AMERICA'S HOSPITALS AND HEALTH SYSTEMS

May 8, 2024

Andrew P. Witty
Chief Executive Officer
UnitedHealth Group
P.O. Box 1459
Minneapolis, MN 55440-1459

Dear Mr. Witty:

On behalf of our member health systems and hospitals, we write to urge UnitedHealth Group (UHG) to formalize its intentions regarding any breach notifications following the cyberattack on Change Healthcare. On May 1, you acknowledged during a Senate Finance Committee hearing that "maybe a third" of Americans had Protected Health Information (PHI) and Personally Identifiable Information (PII) stolen. Despite this staggering figure, it is important to emphasize that hospitals, health systems and other providers were not the direct targets of this cyberattack, nor were they responsible for the potential release of private patient information. UHG/Change Healthcare, as the targets of the attack and source of any potential breach, are in the best position to make any necessary breach notifications.

Thankfully, UHG appears to agree with this assessment. We are encouraged that UHG announced in an April 22, 2024, press release that the company will "provide appropriate notifications when the company can confirm the information involved" and "make notifications and undertake related administrative requirements on behalf of any provider or customer." **It is important, however, that UHG officially inform the Department of Health and Human Services Office for Civil Rights (OCR) and state regulators that UHG will be *solely* responsible for all breach notifications required under law and provide them with a timeline for when those notifications will occur.**

This is important in light of information included on OCR's new webpage, entitled "Change Healthcare Cybersecurity Incident Frequently Asked Questions." In particular, OCR stated:

> [W]ith respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, **the covered entity may delegate the responsibility of providing individual notices to the business associate**. Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may vary, depending on the circumstances.

See https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html (Apr. 19, 2024) (emphasis in original). UHG has already correctly recognized that it—not covered entities like health systems and hospitals—is in the "best position" to notify individuals of any breach. **Accordingly, we urge UHG to immediately notify OCR, state regulators, Congress, the media, and other relevant stakeholders that it is formally accepting a delegation from *all* covered entities to make breach notifications on their behalf**.

As you are aware, our members have been acutely affected by the unprecedented cyberattack. It will take many months for health systems and hospitals to address the fallout from this attack and return to standard operations. In the meantime, our members remain committed to safeguarding the privacy and security of their patients' medical information, claims and billing information and personal information. To that end, our members are concerned about protecting individuals whose PHI and PII may have been improperly disclosed because of the cyberattack.

Although your website states that it will take "several months" to identify and notify those individuals who were impacted by any breach, you informed the Senate Finance Committee that UHG is working with regulators to make the timely notifications required by law. We are grateful for that. Without a unified notification process, patients, the media, state regulators and OCR could possibly face multiple notifications of this same breach. This would: 1) cause public confusion, misunderstandings and added stress; 2) unnecessarily increase burden on OCR and other regulators; and 3) impose unnecessary costs on hospitals, which already have suffered greatly from this attack. Hospitals have already experienced extraordinary reductions in cash flow, thereby threatening their ability to make payroll and acquire the medical supplies needed to provide care to patients. As you have acknowledged, they should not have to make a duplicative breach notification on top of these other added costs.

We thank you for your attention to these urgent matters. We continue to stand ready to work with you to minimize any further disruption to patient care as a result of this attack.

Sincerely,

America's Essential Hospitals
American Hospital Association
Association of American Medical Colleges
Children's Hospital Association
Federation of American Hospitals
National Association for Behavioral Healthcare