May 2, 2024

The Honorable Xavier Becerra
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Secretary Becerra:

Thank you for your strong leadership to resolve the myriad challenges the healthcare system has faced from the Change Healthcare cyber incident. With the private sector and government leaders working together, we have made real progress the past two months. Important work remains, including on the critical aspect of data breach notifications.

United Healthcare has acknowledged that "files containing protected health information (PHI) or personally identifiable information (PII)" were compromised for a "substantial proportion of people in America." Their data review is "likely to take several months of continued analysis before enough information will be available to identify and notify impacted customers and individuals."

While the lack of specificity and timeline is challenging, it gives federal officials the opportunity to evaluate HIPAA's breach notification obligations within the context of this unique situation. Specifically, HIPAA's rules apply to all Covered Entities, which includes providers, payers and clearinghouses. Applying these rules to this situation, all three types of Covered Entities may have obligations to notify individuals regarding this situation. This situation presents the very real likelihood of a "significant portion" of the American public receiving numerous breach notification letters.

At yesterday's hearing held by the House Energy & Commerce Committee, United CEO Andrew Witty said, "we are offering to take full responsibility for all notification obligations for everyone involved in this." We support this approach and agree that guidance from the Office of Civil Rights should clearly state that only Change has an obligation to perform breach notification in this context. That clarity would avoid tens of millions of Americans being left confused, frustrated and inundated by multiple notifications. For example, a patient with diabetes could be notified by their primary care physician and endocrinologist; an EHR company; their local hospital; their local pharmacy; a specialty pharmacy; their employer; and their health plan's administrator – with many other possible notifications as well. All regarding the one data breach at Change.

It is critical that regulators, working closely with Change, obtain specific information and clearly define all Covered Entities' notification obligations regarding this situation. Updated federal guidance that outlines a single, straight-forward notification by Change would be an effective approach to avoid confusion.

We appreciate your consideration – and your continued partnership with industry leaders.

Sincerely,

AHIP
Alliance of Community Health Plans
American Medical Association
American Academy of Family Physicians
Association for Community Affiliated Plans
Blue Cross Blue Shield Association

Cc: Chiquita Brooks-LaSure, Administrator, Center for Medicare & Medicaid Services
Andrea Palm, Deputy Secretary, Department of Health and Human Services
Melanie Fontes Rainer, Director, Office for Civil Rights, Department of Health and Human Services