

May 20, 2024

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

Dear Secretary Becerra:

The undersigned organizations, representing a broad range of clinicians and providers nationwide, write to you today for further clarification about how the U.S. Department of Health & Human Services' (HHS) Office for Civil Rights (OCR) intends to enforce the Health Insurance Portability and Accountability Act (HIPAA)-related reporting requirements involving the Change Healthcare cyber incident announced on February 21<sup>st</sup>. **We are writing to request more clarity around reporting responsibilities and assure affected providers that reporting and notification obligations will be handled by Change Healthcare.**

**OCR should publicly state that its breach investigation and immediate efforts at remediation will be focused on Change Healthcare, and not the providers affected by Change Healthcare's breach.**

Healthcare clinicians and providers take seriously their responsibility to safeguard and protect their patients' data. Since the attack became known, concerns among our members have mounted related to what could – from all indications – amount to the largest breach of the healthcare sector. Change Healthcare processes claims on behalf of hundreds of thousands of clinicians and providers, and several terabytes of possibly protected health information are alleged to have been stolen and held for ransom.

On April 22<sup>nd</sup>, United Health Group (UHG), of which Change Healthcare is a business unit, issued a [press release](#) offering limited details that stated, “Based on initial targeted data sampling to date, the company has found files containing protected health information (PHI) or personally identifiable information (PII), which could cover a substantial proportion of people in America. To date, the company has not seen evidence of exfiltration of materials such as doctors' charts or full medical histories among the data.” Contrary to media reports – as well as information we have heard from our respective members – there are indications that certain data may indeed have been compromised, resulting in a perplexing situation for providers tasked with ensuring the privacy and security of PHI and PII.

This unprecedented cyberattack raises the question of how OCR plans to reassure the provider community regarding breach reporting obligations under HIPAA, and to clarify that is the responsibility of the covered entity which experienced the breach—UHG—to fulfill its obligations in regard to reporting the breach to OCR, notifying each affected individual, as well as any further HIPAA breach reporting requirements that may be applicable, such as notifying state Attorneys General and media outlets. Numerous providers continue to grapple with the far-reaching consequences of this incident, and financial recovery remains elusive as the situation continues to get fully resolved. This has been exacerbated by a lack of clarity and definitive information offered by UHG and Change Healthcare.

OCR has said they have initiated investigations of Change Healthcare and UHG, and they issued a set of [frequently asked questions](#) (FAQs) on April 19<sup>th</sup> referencing the “unprecedented magnitude of this cyberattack.” While a breach report is still forthcoming from UHG, they have said that “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, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.”

UHG has stated they “are committed to doing everything possible to help and provide support to anyone who may need it” and has pledged “To help ease reporting obligations on other stakeholders whose data may have been compromised as part of this cyberattack, UnitedHealth Group has offered to make notifications and undertake related administrative requirements on behalf of any provider or customer.” While we appreciate these statements, **we are concerned that without further guidance from OCR, clinicians and providers have not received sufficient confirmation from OCR that HIPAA breach reporting and notification requirements related to this incident are the responsibility of UHG/Change Healthcare as the HIPAA covered entity which experienced the breach of unsecured PHI.**

Providers affected by this breach are so numerous that a specific number is not readily available. A simple affirmation from OCR, as requested herein, that UHG, as the covered entity which experienced the breach is responsible for fulfilling the attendant breach reporting and notification requirements, is badly needed to address the lack of clarity among the community of affected providers. Given UHG’s statement that it is prepared to fulfill these reporting and notification requirements, it appears that it would be a quick and straightforward matter for OCR to confirm publicly that the HIPAA breach notification and reporting requirements are applicable to UHG and not to the affected providers. Given the well documented state of chaos in the provider community in the wake of this breach, OCR’s silence on this point is disappointing.

In addition, **OCR must affirm its position that the breach was perpetrated upon Change Healthcare, whose status as a health care clearinghouse makes them a covered entity under HIPAA and thus responsible for the breach of any PHI which it processes or facilitates the processing of.** Because Change Healthcare experienced impermissible access to unsecured PHI that it processed on behalf of other covered entities, no entity other than Change Healthcare, its parent company, UnitedHealth Group, and their corporate affiliates such as Optum, bears responsibility for this breach and is under any legal reporting or notification obligation as a result of it.

Given the statement by UHG that, “UnitedHealthGroup has offered to make notifications and undertake related administrative requirements on behalf of any provider or customer,” **OCR should confirm that any affected provider may rely upon that statement and, as UHG bears sole responsibility for the breach, no breach notification requirements apply to any affected medical provider.**

While we appreciate OCR’s FAQs, **OCR should publicly state that their breach investigation and immediate efforts at remediation will be focused on Change Healthcare, and not the providers affected by Change Healthcare’s breach.**

For medical providers affected by the UHG ransomware attack, their chief responsibility patient care. These providers may lack clarity regarding what is required of them under HIPAA in this instance and so we call upon HHS-OCR to take the simple step of confirming the above, to publicly to ease concerns in the provider community. We appreciate the opportunity to bring this matter to your attention as we navigate the fallout from this assault on patient care and the privacy of their medical information.

Sincerely,

College of Healthcare Information Management Executives (CHIME)  
American Health Information Management Association (AHIMA)  
American Medical Association  
Medical Association of the State of Alabama  
Alaska State Medical Association

Arizona Medical Association  
Arkansas Medical Society  
California Medical Association  
Colorado Medical Society  
Connecticut State Medical Society  
Medical Society of Delaware  
Medical Society of the District of Columbia  
Florida Medical Association Inc  
Medical Association of Georgia  
Hawaii Medical Association  
Idaho Medical Association  
Illinois State Medical Society  
Indiana State Medical Association  
Iowa Medical Society  
Kansas Medical Society  
Kentucky Medical Association  
Louisiana State Medical Society  
Maine Medical Association  
MedChi, The Maryland State Medical Society  
Massachusetts Medical Society  
Michigan State Medical Society  
Minnesota Medical Association  
Mississippi State Medical Association  
Missouri State Medical Association  
Montana Medical Association  
Nebraska Medical Association  
Nevada State Medical Association  
New Hampshire Medical Society  
Medical Society of New Jersey  
New Mexico Medical Society  
Medical Society of the State of New York  
North Carolina Medical Society  
North Dakota Medical Association  
Ohio State Medical Association  
Oklahoma State Medical Association  
Oregon Medical Association  
Pennsylvania Medical Society  
Rhode Island Medical Society  
South Carolina Medical Association  
South Dakota State Medical Association  
Texas Medical Association  
Utah Medical Association  
Vermont Medical Society  
Medical Society of Virginia  
Washington State Medical Association  
West Virginia State Medical Association  
Wisconsin Medical Society  
American Academy of Allergy, Asthma & Immunology  
American Academy of Dermatology Association  
American Academy of Emergency Medicine  
American Academy of Facial Plastic and Reconstructive Surgery (AAFPRS)  
American Academy of Family Physicians

American Academy of Neurology  
American Academy of Ophthalmology  
American Academy of Pediatrics  
American Academy of Physical Medicine and Rehabilitation  
American Academy of Sleep Medicine  
American Association of Neurological Surgeons  
American Association of Neuromuscular & Electrodiagnostic Medicine  
American Association of Orthopaedic Surgeons  
American College of Allergy, Asthma and Immunology  
American College of Cardiology  
American College of Emergency Physician  
American College of Gastroenterology  
American College of Obstetricians and Gynecologists  
American College of Physicians  
American College of Radiology  
American College of Rheumatology  
American Gastroenterological Association  
American Geriatrics Society  
American Orthopaedic Foot & Ankle Society  
American Osteopathic Association  
American Psychiatric Association  
American Society for Dermatologic Surgery Association  
American Society for Radiation Oncology  
American Society of Anesthesiologists  
American Society of Cataract and Refractive Surgery  
American Society of Clinical Pathology  
American Society of Nephrology  
American Society of Neuroradiology  
American Society of Plastic Surgeons  
American Society of Regional Anesthesia and Pain Medicine  
American Society of Retina Specialists  
American Society of Transplant Surgeons  
Association for Clinical Oncology  
Association of American Medical Colleges (AAMC)  
College of American Pathologists  
Congress of Neurological Surgeons  
Medical Group Management Association  
North American Neuromodulation Society  
North American Spine Society  
Renal Physicians Association  
Society for Pediatric Dermatology  
Society for Vascular Surgery  
Society of Interventional Radiology  
The American Academy of Otolaryngology - Head and Neck Surgery  
The American College of Radiation Oncology, Inc.

cc: Melanie Fontes Rainer, Director, Office for Civil Rights, Department of Health and Human Services