

<https://www.hfma.org/technology/cybersecurity/cyberattack-on-change-healthcare-brings-turmoil-to-healthcare-operations-nationwide/>

## Data Assessment and Support for Impacted Individuals

Given the ongoing nature and complexity of the data review, it is **likely to take several months of continued analysis before enough information will be available to identify and notify impacted customers and individuals**. As the company continues to work with leading industry experts to analyze data involved in this cyberattack, it is immediately providing support and robust protections rather than waiting until the conclusion of the data review.

People can visit a dedicated website at <http://changeybersupport.com/> to get more information and details on these resources. A dedicated call center has been established to **offer free credit monitoring and identity theft protections for two years to anyone impacted**. The call center will also include trained clinicians to provide support services. Given the ongoing nature and complexity of the data review, the call center **will not be able to provide any specifics on individual data impact at this time**.

The call center can be reached at **1-866-262-5342** and further details can be found on the website.

The company, along with leading external industry experts, continues to monitor the internet and dark web to determine if data has been published. **There were 22 screenshots, allegedly from exfiltrated files, some containing PHI and PII, posted for about a week on the dark web by a malicious threat actor. No further publication of PHI or PII has occurred at this time.**

While this comprehensive data analysis is conducted, the company is in communication with law enforcement and regulators and will provide appropriate notifications when the company can confirm the information involved. **This is not an official breach notification**. The company will reach out to stakeholders when there is sufficient information for notifications and will be transparent with the process.

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.**

**Temporary funding** assistance is being provided through Optum Financial Services for provider organizations impacted by the payer system outage. Eligible providers can register at [www.optum.com/temporaryfunding](https://www.optum.com/temporaryfunding), using an Optum pay account without incurring fees or interest.

## **General Info:**

<https://www.unitedhealthgroup.com/changehealthcarecyberresponse>

## **4/22 Press Release:**

<https://www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html>

## **Incident Support:**

<https://www.unitedhealthgroup.com/ns/health-data-breach.html>

## Change Healthcare Assistance Program – Sponsored by the Mass Collaborative

<https://masscollaborative.org/>

<https://www.mahealthdata.org/chap?hsCtaTracking=41f9bf82-799b-46f4-9a65-ba36289191c1%7C928a09ef-959f-4ea6-8974-d8258ec06192>

**NEW Open Office Hours:** Fourth Thursday of the month, 12-1pm ET, via Zoom. Register [HERE](#).

Open Office slides - [April 11, 2024](#)

Key links shared in Open Office sessions, 4/11 & 4/17:

[Change Healthcare Impacted Payer Status](#)  
[NEHEN/TriZetto Impacted Payer Status](#)

**Need Personal Assistance?** Call 888-402-3550 or email [CHAP@mahealthdata.org](mailto:CHAP@mahealthdata.org)

**MA Health Information Sessions Provider Services:** (800) 849-2900 or [provider@masshealthquestions.com](mailto:provider@masshealthquestions.com)

Latest updates from the [American Medical Association](#) and the [American Hospital Association](#)

[Change Healthcare FAQ](#) - US Dept. of Health & Human Services (Office for Civil Rights)

**Key forms:** [Health Insurance Claim Form CMS1500](#) and [MassHealth Electronic Claims Waiver Request](#)

**Claims:** As of 4/3/24, TPS will begin sending claims to Change Healthcare's Relay Exchange. The payer list is currently limited, but Change Healthcare is working daily to restore payer connections. TPS will continue to update our payer list with reroute dates. In the meantime, we remain actively engaged with many impacted payers to find alternate solutions for new connections. TPS will continue to communicate updates on our website via the Message Center.

[CHC\\_Impacted\\_Payers\\_-\\_4.23.2024.xlsm.xlsx](#)

**TPS will also continue to reject any claim that has not yet been rerouted.** The following rejection message will be displayed to assist in recognizing affected claims: The route to this payer has been impacted by the Change Healthcare cyber incident. Providers will need to submit by paper, hold, or utilize the payer's portal for claims submission. This solution allows clients to submit claims by paper, hold, or utilize the payer's online portal.

TPS can print and mail claims for clients who currently have our Paper Claim product. To utilize this paper process, please use the payer ID 00000 when submitting impacted claims. This unique payer ID will bypass any systematic attempt to send them electronically and route them via paper. Note: **Clients may also opt to download claims from their software, print them, and mail them directly to the payer.**

**Eligibility Inquiries:** Any eligibility transactions sent to impacted payers **will not receive a response.** Until a new route is established for these transactions to the impacted payers, clients will want to verify coverage with the payer directly when needed.

**Electronic Remittance Advice:** Change Healthcare has indicated that ERA data was cleared from their server, but **some payers have submitted ERA files upon the 3/24 reconnection.** While we do not have full visibility into what will be made available, TPS is committed to passing along any received information as expected. If you have missing remittance advice, we recommend that clients utilize payer portals or other means to obtain remittance advice until service is fully restored.

TPS has decided to start transitioning ERA payers through alternative routes to reduce the impact on our providers. We are working closely with payers and trading partners on enrollment requirements. In some cases, we can enroll our providers in bulk, but in many cases, new enrollment is required. **Once an alternative route is established, we will update our message center with any enrollment instructions.**

## NEHEN/TriZetto Impacted Payer Status

Payer ID	Payer Name	Claims Impacted	Claim Type	Claims Connection Rerouted Date - you may resume sending electronically if there is a date listed	TPS Notes
13162	1199 LOCAL BENEFIT FUND	Y	Professional	3/13/2024	Claims rerouted - you may resume sending claims electronically
R6845	1-888-OHIOCOMP	Y	Professional		This payer requires enrollment for claims submission. We are researching the best approach for payers requiring enrollment to minimize our providers' impact. For now, please submit claims on paper or via the payer portal
R7627	1-888-OHIOCOMP - UB	Y	Institutional/UB		This payer requires enrollment for claims submission. We are researching the best approach for payers requiring enrollment to minimize our providers' impact. For now, please submit claims on paper or via the payer portal
29076	1st MEDICAL NETWORK	Y	Professional	3/4/2024	Claims rerouted - you may resume sending claims electronically
U7205	360 Alliance UB - Gilsbar	Y	Institutional/UB		Until the Change Healthcare issue is resolved, please submit claims on paper or via the payer portal
20446	6 Degrees Health Incorporated	Y	Professional		Until the Change Healthcare issue is resolved, please submit claims on paper or via the payer portal
11370	A G Administrators LLC	Y	Professional	4/9/2024	Claims rerouted - you may resume sending claims electronically
U1370	A G Administrators LLC UB	Y	Institutional/UB	4/9/2024	Claims rerouted - you may resume sending claims electronically
84129	Access Behavioral Care	Y	Professional		Until the Change Healthcare issue is resolved, please submit claims on paper or via the payer portal
COACC	Access Behavioral- Care	Y	Professional		Until the Change Healthcare issue is resolved, please submit claims on paper or via the payer portal
S7815	Acordia National - UB	Y	Institutional/UB		Until the Change Healthcare issue is resolved, please submit claims on paper or via the payer portal
59141	Administrative Services, Inc.	Y	Professional		Until the Change Healthcare issue is resolved, please submit claims on paper or via the payer portal
U9141	Administrative Services, Inc. UB	Y	Institutional/UB		Until the Change Healthcare issue is resolved, please submit claims on paper or via the payer portal
U8056	Advantage Plan - UB	Y	Institutional/UB		Until the Change Healthcare issue is resolved, please submit claims on paper or via the payer portal
68056	Advantage Plan by Bridgeway	Y	Professional		Until the Change Healthcare issue is resolved, please submit claims on paper or via the payer portal

## Change Healthcare Impacted Payer Status



Intelligent EDI (iEDI) Claims Payer List for Legacy Emdeon (OKC) Submitters

Enrollment Key	
Y	You must re-enroll with this payer.
Y*	If you were previously enrolled with this payer through Legacy Emdeon (OKC), you do not have to re-enroll to submit claims.
N	Enrollment is not required.

Payer Name	Payer ID	Professional		Institutional		Dental	
		Available	Enrollment	Available	Enrollment	Available	Enrollment
(UCS) Masonry Industry Trust	60230	Y	N				
1199 SEIU National Benefit Fund	13162	Y	N	Y	N		
2020 Eye Care	2020E	Y	N	Y	N		
21st Century Insurance and Financial Services	51028	Y	N				
3P ADMIN	20413	Y	N	Y	N		
6 Degrees Health, Inc.	20446	Y	N	Y	N	Y	
8th Distric Electrical	74234	Y	N	Y	N		
A.G. Administrators	11370	Y	N	Y	N		
AARP Medicare Supplement Plans insured by UnitedHealthcare Insurance Company	36273	Y	N	Y	N		
ABMG	A0701	Y	N				
Abrazo Advantage Health Plan	03443	Y	N	Y	N		
Abri Healthplan	ABR11	Y	N	Y	N		
Access Administrators	12T33			Y	N		
Access Administrators	AHS01	Y	N	Y	N		
Access Administrators	TH067	Y	N				
Access Behavioral Care	COACC	Y	N	Y	N		
Access Integra	INTEG	Y					
Access Medical Group	AMG02	Y	N	Y	N		
ACCLAIM	64071	Y	N	Y	N		
Accountable HC IPA (Customer Service (562) 435-3333 for claims with DOS prior to 5 1 15)	AHIPA	Y	N				
Accountable Healthcare IPA	MPM23	Y	N				
ACS Benefits Payer Compass	PA331	Y	N	Y	N		
Activa Benefits Services LLC	38254	Y	N	Y	N		
ActivHealthcare	AHC01	Y	N				
Administrative Concepts Inc.	22384	Y	N	Y	N		
ADN Administrators	CXADN					Y	
Adv Benefit Mgmt Systems USA	66457	Y	N				

<https://www.hhs.gov/sites/default/files/cyberattack-change-healthcare.pdf>



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

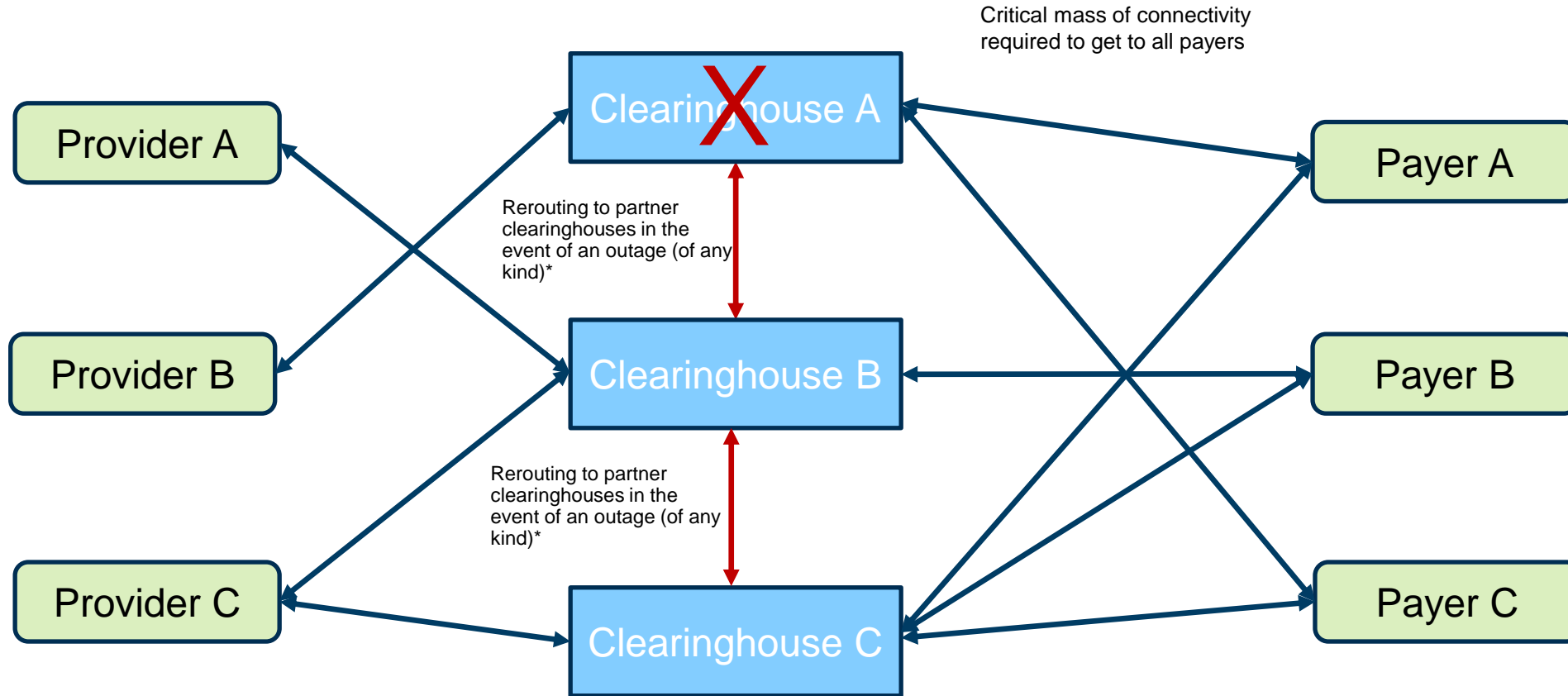
• [OCR HIPAA Security Rule Guidance Material](#) – This webpage provides educational materials to learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic protected health information. Materials include a Recognized Security Practices Video, Security Rule Education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

• [OCR Video on How the HIPAA Security Rule Protects Against Cyberattacks](#) – This 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.



\* Requires strong (hardened) front-end transaction intake and re-routing systems – Possibly air-gapped from internal systems