Information Regarding Change Healthcare Data Breach

Background

Nufactor takes the privacy and confidentiality of patient information very seriously. Nufactor is aware of the cyberattack on Change Healthcare that occurred on February 21, 2024. Change Healthcare is a provider of revenue and payment cycle management that connects payers, providers, and patients within the U.S. healthcare system, reportedly handling 15 billion transactions annually. It processes about 50% of medical claims in the United States for around 900,000 physicians, 33,000 pharmacies, 5,500 hospitals and 600 laboratories. Through pharmacy management software, Nufactor utilizes Change Healthcare's systems to, among other things, process insurance claims and billing, receive pre-authorizations, and get cost estimates. **Nufactor was not responsible for the breach.**

The information below includes potential questions and answers to address your concerns.

1. **What Happened?**

We have learned of a security breach, which was identified on February 21, 2024, by Change Healthcare when it discovered a threat actor gained access to one of its environments. According to reports from Change Healthcare, once it became aware of the outside threat, it took immediate action to disconnect its systems to prevent further impact. According to Change Healthcare, their security team, along with law enforcement and independent experts, began working to address the matter. On April 15, 2024, UnitedHealth Group, the parent company of Change Healthcare, confirmed that "the data [that was accessed] had some quantity of personal health information and personally identifiable information." On April 22, 2024, UnitedHealth Group issued an updated statement saying that a breach involving protected health information was indeed confirmed, and that the compromise "could cover a substantial proportion of people in America." NuFactor was not responsible for the breach and has confirmed there was no direct access to our systems by the threat actor.

Nufactor has been diligently monitoring the situation surrounding the reported security breach and actively requesting regular updates to determine if any Nufactor patient data was compromised as part of the data breach. Although we are not aware of any misuse of your health information, we are providing this information about the incident out of an abundance of caution.

2. **Was my information included in the data breach?**

At this time, we have not received notice from Change Healthcare or any of our mutual business associates that any Nufactor patient data was compromised. We continue to diligently monitor the situation and actively seek regular updates regarding Nufactor patient data. Should we receive confirmation that any Nufactor patient data has been compromised, you will promptly be notified.

On April 15, 2024, UnitedHealth Group, the parent company of Change Healthcare, stated that "the data [that was accessed] had some quantity of personal health information and personally identifiable information. [They] are working to determine the quantity of impacted data, and [ ] are fully committed to providing notifications to impacted individuals when determinations are able to be made…." On April 22, 2024, UnitedHealth Group issued an updated statement saying that a breach involving protected

health information was indeed confirmed, and that the compromise "could cover a substantial proportion of people in America."

UnitedHealth Group maintains a Frequently Asked Questions page on its website that you may want to visit for more information. Frequently Asked Questions
https://www.unitedhealthgroup.com/ns/changehealthcare/faq.html

3. What personal information is involved?

We have not received confirmation that any specific Nufactor patient data was compromised, so we can't identify any specific personal information. However, the personal information shared with Change Healthcare may include:

- Patient Name
- Patient Address
- Patient Phone number
- DOB
- ID #
- Group #
- Insured's Name, Address, DOB
- Relationship
- Diagnosis
- Drug/Service Provided
- Prescription #
- Dates (prescription fill date, prescription infusion date)

4. Was Nufactor responsible for the breach?

No. Change Healthcare reported a security breach, which was identified on Feb. 21, 2024, when it discovered a threat actor gained access to one of its environments. Change Healthcare, a third-party service provider of revenue and payment cycle management that connects payers, providers, and patients within the U.S. healthcare system, reportedly handles 15 billion transactions annually. It processes about 50% of medical claims in the United States for around 900,000 physicians, 33,000 pharmacies, 5,500 hospitals and 600 laboratories. Through pharmacy management software, Nufactor (and numerous other pharmacies) use Change Healthcare's systems to, among other things, process insurance claims and billing, receive pre-authorizations, and get cost estimates.

5. Were Nufactor's systems breached?

Upon learning of the security breach at Change Healthcare, Nufactor promptly took steps to ensure the threat actor did not access Nufactor's systems. We have confirmed based on our current investigations, there was no direct access by the threat actor to Nufactor's systems.

6. What is Nufactor doing to find out if my data was breached?

Nufactor has confirmed that there was no direct access to our systems by the threat actor. However, we currently do not know if any Nufactor patient information was compromised within Change Healthcare's systems. At this time, neither Change Healthcare nor any of our mutual business associates have reported any Nufactor patient data was compromised. We continue to diligently monitor the situation

and actively seek regular updates regarding Nufactor patient data. We are committed to maintaining the highest standards of data protection and will promptly notify you if we receive confirmation your information was compromised.

7. **When will I find out if my data was breached?**

UnitedHealth Group, the parent company of Change Healthcare, has committed to providing notifications to impacted individuals once it is able to determine which data were compromised. Federal law provides 60 days from the time an entity discovers a breach of Protected Health Information to notify those impacted. However, given the magnitude of the breach and the challenges in identifying the impacted data, UnitedHealth Group may not be able to comply with this time period.

8. **Where can I get more information?**

UnitedHealth Group has established a dedicated call center to offer additional resources and information to people who are concerned they may have been affected by this incident. People can visit a dedicated web site at **changecybersupport.com** to get more information and details on these resources. A dedicated call center has also been established to offer free credit monitoring and identity theft protections for two years to anyone in the U.S. who requests it. The call center will also include trained clinicians to provide emotional support services to those who request it. According to UnitedHealth Group, given the ongoing nature and complexity of 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.

9. **What else can I do to protect myself?**

The Federal Trade Commission offers the following tips to help protect yourself if your personal information has been compromised:

- If a company responsible for exposing your information offers you free credit monitoring, take advantage of it.
- Get your free credit reports from annualcreditreport.com. Check for any accounts or charges you don't recognize.
- Consider placing a free credit freeze. A credit freeze makes it harder for someone to open a new account in your name.
- If you place a freeze, be ready to take a few extra steps the next time you apply for a new credit card or cell phone – or any service that requires a credit check.
- If you decide not to place a credit freeze, at least consider placing a fraud alert.
- Try to file your taxes early — before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.
- Don't believe anyone who calls and says you'll be arrested unless you pay for taxes or debt — even if they have part or all of your Social Security number, or they say they're from the IRS.
- Continue to check your credit reports at annualcreditreport.com. You can check your reports every week for free.

10. Will I receive compensation if my data was breached?

While Nufactor is not responsible for the data breach, we understand the concerns of our patients regarding the impact of this incident. Any decision regarding compensation for affected individuals would be made by Change Healthcare and UnitedHealth Group, as they are managing the response to this breach. We will provide updates regarding compensation as we receive them from Change Healthcare. Additionally, if Change Healthcare determines your data has been breached, Change Healthcare will notify you, and such notification may include additional information on measures or compensation offered in relation to the breach.

11. Who can I contact for more information or to report suspicious activity related to this breach?

If you believe your personal information has been misused, we recommend contacting the Federal Trade Commission through their website at Identitytheft.gov. We also recommend that you notify your bank and credit card companies to monitor for any unusual activity and contact the major credit bureaus—Equifax, Experian, and TransUnion—to place a fraud alert on your credit reports. For additional information or any questions about the data security incident, please contact the UnitedHealth Group call center at 1-866-262-5342. For questions about these questions and answers or Nufactor, please contact us at 951-296-2528 ext. 1623.