WindRose Health Network

*Leading you to better health!*

# Notice of Data Security Incident

WindRose Health Network recently learned about a security incident that involved our computer network. The incident involved a previously undisclosed vulnerability in a remote-management tool that is used by one of our vendors. This remote-management tool can be used to access some of WindRose's systems. Upon learning of the incident, we promptly began working with our vendor and cybersecurity experts to investigate. We are providing this notice to share information about what happened and what we are doing in response.

## WHAT HAPPENED?

On August 4, 2026, we were informed by one of our vendors about a previously undisclosed vulnerability in the remote-management tool it maintains and uses to access our network. We immediately took steps to secure our environment and began working with cybersecurity experts to assist us in the investigation. Based on the investigation, we believe that an unauthorized third party used this vulnerability to gain access to one of our servers from August 3 to August 4, 2026. This incident did not have any impact on the systems that host our electronic medical records.

## WHAT INFORMATION WAS INVOLVED?

The investigation determined that the following types of information were present in some of the affected files: patient name, patient identification number, health insurance information, date of service, and the name of the medical provider.

## WHAT WE ARE DOING.

We hired third-party experts to help us perform an investigation into the unauthorized activity and further secure our systems and the information we maintain. To those impacted individuals for whom WindRose has a current address, we are now in the process of mailing individual letters to them to let them know about the incident.

## WHAT YOU CAN DO.

For individuals who receive a letter from us about the incident, we encourage them to read the information in that letter carefully, as it contains important steps that they can take. We encourage individuals to (1) remain vigilant for unauthorized financial activity by reviewing their account statements and free credit reports, (2) consider placing a fraud alert or security freeze on their credit file (which individuals can do for free), and (3) immediately report any suspicious activity or suspected incidents of identity theft to their financial institutions and to law enforcement. Additional steps can also be found at www.IdentityTheft.gov/.

## FOR MORE INFORMATION.

Should you have any questions, you can contact us at privacyincident@windrosehealth.org, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.