NOTICE OF DATA SECURITY INCIDENT

Eduro Healthcare ("Eduro") recently learned about a data security incident that may have impacted your Protected Health Information ("PHI"). Specifically, the incident in question may have resulted in the disclosure of your name and medical information. At Eduro, we respect the privacy and security of all information within our control, and sincerely apologize for any concern this may cause you.

Eduro Healthcare operates transitional care and skilled nursing facilities throughout the United States, including New Mexico and South Dakota.

What happened?

On March 2021, Eduro Healthcare experienced a security incident involving suspicious activity on its network. Upon discovery, Eduro took immediate action to disconnect external access to the network, contain the threat, and implemented a well-coordinated incident response plan to quickly restore the network. All systems were restored within and Eduro remained fully operational. Eduro was of the belief that it had caught and stopped a security event from occurring and had no knowledge that any information on its systems were accessed or removed as part of this event. However, Eduro was made aware that some of its data had been posted on the dark web. On August 24, 2021, Eduro learned that PHI was present in the posted dataset. Eduro continued its investigation to determine the identity of those individuals affected by the incident, the information associated with them that was involved, and addresses for the same. This process took considerable time and only concluded on October 21, 2021.

What information was involved?

On August 24, 2021, the review concluded and Eduro determined PHI was present in the posted dataset, which may include patients' first and last name, date of birth, treatment information, provider name, dates of service, Social Security number, and health insurance information.

What are we doing?

To help reduce the risk of fraud or identity theft, we are offering complimentary credit monitoring and identity restoration services for twelve months, at no charge. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

Additionally, in response to this incident, we deployed additional security controls, conducted a complete audit of all accounts, strengthened password protocols, and reconfigured our firewall. We also enforced a system wide password reset, implemented multi-factor authentication for email, and evaluated and updated network security protocols and procedures.

What can you do?

It is always a good idea to carefully monitor your bank account and other financial statements, and immediately contact your financial institution if you identify any suspicious activity. We also recommend that patients keep

an eye on their benefits statement and report any unusual activity. All individuals whose information may have been involved in this incident are being offered complimentary identity protection services through IDX for 12 months. We encourage you to contact IDX with any questions and, if your information was present in the impacted dataset, take full advantage of the IDX service offering. To determine whether you were affected by this incident, please call 1-833-989-3935, Monday through Friday from 7 am - 7 pm Mountain Time.

For more information

If you have any questions or concerns, please call 1-833-989-3935, Monday through Friday from 7 am - 7 pm Mountain Time. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you. Individuals can also contact the Federal Trade Commission at 600 Pennsylvania Avenue NW, Washington, D.C. 20580, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261 or visit www.ftc.gov/idtheft/ for more information on protecting their identity.