

## **Notice of Data Security Incident**

### **What happened:**

On June 1, 2024, Special Health Resources of Texas, Inc. (“SHRT”) learned of a data security incident which may have impacted the Protected Health Information (“PHI”) of a limited number of patients. As soon as SHRT learned of the incident, it began an internal investigation to identify what occurred and what patient data may be at risk. SHRT also began working with independent cybersecurity specialists to help determine what had occurred and whether any information was at risk. The investigation is ongoing, but SHRT believes that an unauthorized actor gained access to a limited number of SHRT systems for a brief period of time and that a limited amount of PHI was impacted. The investigation into this incident is ongoing, and SHRT intends to provide notice to individuals when it learns more information. At this time, there is no indication that any PHI has been misused.

### **What We Are Doing:**

SHRT has taken steps to prevent a similar incident from occurring in the future, including putting additional security controls in place and is conducting a thorough review of its existing security controls. SHRT respects the privacy and confidentiality of all information entrusted to it and will remain vigilant in its efforts to safeguard and protect all information within our control. SHRT is working to identify impacted individuals and will be mailing letters to any impacted individual for whom there is contact information. This letter will contain more information about the incident, steps taken in response, and resources that will be made available to impacted individuals. If an individual’s Social Security number was affected, credit monitoring and identity restoration services will be provided at no cost.

### **What You Can Do:**

Individuals should remain vigilant for incidents of identity theft or fraud by reviewing bank accounts and other financial statements, as well as credit reports, for suspicious activity. Incidents of identity theft should be reported to law enforcement or the attorney general. Recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on a credit file can be found at [www.identitytheft.gov](http://www.identitytheft.gov). Individuals should monitor credit reports and financial statements for suspicious activity.

### **For more Information**

Please call **1-833-531-1829** Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time with any questions. We take very seriously the need to protect the privacy and security of all information in our respective care, and deeply regret any inconvenience or concern that this matter may cause.