Clinical Registry Solutions (CRS) Notice for Data Security Incident

This substitute notice provides information about a security incident experienced by one of our service providers, Clinical Registry Solutions (CRS), that occurred in April 2026 involving protected health information. CRS, on our behalf, began notifying impacted patients on Sept 4, 2026. This notice is meant to provide information about the incident and CRS's response.

What Happened

Clinical Registry Solutions facilitates the abstraction and submission of patient data to clinical data registries for various health care organizations, including CommonSpirit. On April 9, 2026, CRS was a victim of a ransomware attack. Upon discovering the unauthorized activity, CRS hired a cybersecurity forensic firm to investigate and conduct a review of the data involved. Through this investigation, CRS found evidence that an unauthorized actor obtained a copy of some information impacting the following facilities: Colorado facilities include CommonSpirit Mercy Regional Hospital (Durango), CommonSpirit St. Francis, and CommonSpirit Penrose. California facilities involved include St. Joseph's Medical Center (Stockton) and Sequoia Hospital (Redwood City). This disclosure serves to update the prior notification, which originally was limited to a specific patient population at St. Mary's Long Beach.

What Information Was Involved

CRS has determined that some of the data involved in the security incident may have included names and information in one or more of the following categories: First Name, Last Name, Medical Record Number (MRN), dates of service, and some clinical health information.

For More Information

Clinical Registry Solutions (CRS) has hired Transunion to answer any questions about this event. If you have questions, please call 800–405–6108, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for any unauthorized or suspicious activity. Any such activities should be reported to your financial institutions immediately.

We take this matter seriously and are committed to protecting the privacy and security of the information entrusted to us and our service providers.