Clinical Registry Solutions
c/o Cyberscout
<<Return Address>>
<<City>>, <<State>><<Zip>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

NOTICE OF <<Custom Field 1>>

Dear <<First Name>> <<Last Name>>:

Clinical Registry Solutions ("CRS") is notifying you of a data security incident that may have involved your protected health information and/or personal information. CRS is a vendor that provides registry support services to Dignity Health – St. Mary's Medical Center ("St. Mary's"). As part of those services, CRS maintains certain information relating to St. Mary's patients. This notice explains what happened, our response, and additional steps you may consider to protect your information.

What Happened? On April 9, 2026, CRS discovered suspicious activity within its network. Upon discovery, CRS took immediate steps to secure its network and conducted an investigation into the nature and scope of the incident. The investigation determined that CRS's network suffered an unauthorized access on April 9, 2026, and that certain files containing St. Mary's patient information was acquired.

What Information Was Involved? The information included your first and last names, medical record number, and procedure date. The information **did not** include your Social Security number, diagnosis, or treatment plan. We have no evidence of misuse of any protected health information and/or personal information, including for fraud or identity theft, as a result of this incident.

What We Are Doing. Upon learning of the incident, we took immediate action by reviewing the data involved to determine whether it contained any protected health information or sensitive personal information, identify to whom the information belonged, and promptly notify those individuals.

What You Can Do. We reiterate that we have no reports of identity fraud or fraudulent activity involving your information as a result of this incident. However, as a general matter, it is best practice to remain vigilant for incidents of identity theft and fraud, from any source, by reviewing and monitoring your account statements and credit reports for suspicious activity and errors. If you discover any suspicious or unusual activity on your accounts, promptly contact your financial institution or service provider.

For More Information. Should you have any questions or concerns, we have established a dedicated assistance line through TransUnion to assist with any inquires regarding this incident. Please contact Cyberscout, a TransUnion company call center at 1-800-405-6108, Monday through Friday, 8:00 a.m. to 8:00 p.m. EST, excluding major U.S. holidays. We remain committed to protecting your trust in us and continue to be thankful for your support and understanding.

Sincerely,

Clinical Registry Solutions

Enclosure: *Steps You Can Take to Help Protect Your Information*

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts and Credit Reports: Generally speaking, it is good practice to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors.

You May Obtain a Free Credit Report: Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit https://annualcreditreport.com, call toll-free at 1-877-322-8228, complete the Annual Credit Report Request Form on the Federal Trade Commission's (FTC) website at https://ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact one of the credit reporting bureaus.

Fraud Alert Services: You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified below.

Credit Freeze Instructions: As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address information from the prior two to five years;
5. Proof of current address, such as current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, you may contact a major credit reporting bureau listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information: This notice has not been delayed by law enforcement. If you experience identity theft or fraud, you have the right to file a police report with your local law enforcement agency. When filing a report, you may be required to provide documentation showing that you have been a victim, and you are entitled to obtain a copy of the report for your records. If you discover suspicious activity on your credit reports or otherwise believe your information is being misused, you should promptly contact local law enforcement to file a report.

Instances of known or suspected identity theft should also be reported to your state Attorney General and the FTC. A complaint may be filed with the FTC online at https://ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Complaints submitted to the FTC are added to its Identity Theft Data Clearinghouse and made available to law enforcement for investigative purposes. The FTC also provides information about fraud alerts and security freezes.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or https://oag.dc.gov/consumer-protection.

For New York residents, the New York Attorney General may be contacted at The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; or https://ncdoj.gov.

For Oregon residents, the Oregon Attorney General may be contacted at Justice Building, 1162 Court St. NE, Salem, OR 97301; 1-877-877-9392; or https://doj.state.or.us.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. [# of RI] residents had their data impacted by this incident.

You also have rights under the federal Fair Credit Reporting Act (FCRA) and Identity Security Act, which governs the collection and use of information pertaining to you by consumer reporting agencies. These rights include the right to access the information in your file, dispute incomplete or inaccurate information, and request correction or deletion of inaccurate, incomplete, or unverifiable information. For more information about the FCRA and your rights, you may visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf. or https://ftc.gov.

You may contact Clinical Registry Solutions by mail at 306 Gold St, Suite 31E, Brooklyn, NY 11201.