NOTICE OF DATA SECURITY INCIDENT

Date: April 4, 2025

Loretto Hospital ("Loretto") is providing notice of a data security incident. This notice provides information about the incident, Loretto's response to date, and the resources available to individuals to help protect their information from possible misuse, should they feel it appropriate to do so. The confidentiality, privacy, and security of information in our care is one of our highest priorities and we take this incident very seriously.

What Happened? We became aware of suspicious activity involving our computer network and promptly began an investigation. The investigation determined that the network had been accessed by an unknown actor between January 17, 2025 and February 1, 2025, and during this time files were copied. We are reviewing the files to determine the content and to whom it relates.

Additionally, certain data that was input into the electronic medical record system between the evening of February 2, 2025, through the afternoon of February 3, 2025, was not saved. We worked diligently to restore and capture as much data and patient records as possible during this downtime, but some records may not have been recovered or fully recreated.

What Information Was Involved? The review of the files is ongoing and at the conclusion of the review, we will notify those who are potentially affected by this incident. In general, as an employer and healthcare provider we do store certain types of personal information on our systems. For this reason, we are providing this notice out of an abundance of caution while we complete our investigation.

What We Are Doing. We take this incident and the security of information in our care very seriously. We moved quickly to respond and investigate the suspicious activity, assess the security of our network, and notify potentially impacted individuals. As part of our ongoing commitment to information security, we are currently reviewing our policies and procedures, as well as assessing new cybersecurity tools, to reduce the risk of a similar incident occurring in the future. We also notified federal law enforcement and will be notifying relevant regulators, as required.

What You Can Do. In general, individuals should remain vigilant against incidents of identity theft and fraud by reviewing account statements, explanation of benefits statements, and monitoring free credit reports for suspicious activity and to detect errors. Suspicious activity should be promptly reported to relevant parties including an insurance company, healthcare provider, and/or financial institution. Additional information and resources may be found below in the *Steps You Can Take to Protect Personal Information* section of this notice.

For More Information. For questions on this notice you may contact cyber.incident@lorettohospital.org or write to Loretto at 645 South Central Avenue, Chicago, IL 60644; Attn: Information Systems CIO.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent.

However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

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

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/get-credit-report https://www.transunion.com/credit-freeze https://www.transunion.com/fraud-alerts
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, PO Box 2000 Chester, PA 19016

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General.