

Notice of a Data Incident

On November 10, 2025, Iroquois Memorial Hospital (“IMH”) discovered suspicious activity in its computer network. Upon discovering the incident, IMH promptly began an internal investigation, worked to secure its systems, and communicated with law enforcement. IMH also engaged a forensic security firm to assist with its investigation and ensure the security of its computer network. The forensic investigation determined that an unauthorized third party accessed portions of the IMH computer network at times between October 8, 2025, and November 15, 2025. The investigation also determined that the third party may have accessed and acquired certain IMH files during the incident.

Based on the results of its investigation, IMH engaged a dedicated eDiscovery vendor to conduct a comprehensive review of the involved files to determine if the third party may have accessed or acquired any personal information. On August 28, 2026, IMH received the results of the review and determined that the files contained personal information of certain individuals. IMH then worked to validate the results and locate current contact information for those individuals. Depending on the individual, the personal information may include their name, address, date of birth, Social Security number, driver’s license or state ID card number, passport number, financial account number, medical treatment information, and/or health insurance information. On October 14, 2026, IMH mailed notification letters to those individuals whose information was in the files for whom IMH has a valid mailing address.

Notified individuals should refer to the notice they will receive in the mail regarding steps they can take to protect themselves. Although IMH has no evidence that any information may have been misused as a result of this incident, as described in those letters, IMH has arranged for complimentary identity theft protection services for those individuals whose Social Security numbers and/or driver’s license numbers were involved in the incident. As a precautionary measure, individuals should remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing their account statements and monitoring credit reports closely. If individuals detect any suspicious activity on an account, they should promptly notify the financial institution or company with which the account is maintained. They should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and their state’s attorney general. Notified individuals may also wish to review the tips provided by the Federal Trade Commission (“FTC”) on fraud alerts, security/credit freezes and steps that they can take to avoid identity theft. For more information and to contact the FTC, please visit www.IdentityTheft.gov or call 1-877-ID-THEFT (1-877-438-4338). Notified individuals may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

IMH is committed to maintaining the privacy and security of the information entrusted to it. IMH has taken, and is taking, additional steps to help reduce the likelihood of a similar event from happening in the future, including enhancing its technical security measures. Individuals seeking additional information may contact 888-752-8551 from 9:00 a.m. - 9:00 p.m. Eastern time, Monday through Friday, excluding major U.S. holidays.