



A business advisory and advocacy law firm®

Spencer Pollock
Direct Dial: 1.410.917.5189
Email: spollock@mcdonaldhopkins.com

McDonald Hopkins LLC
1820 Lancaster Street
Suite 200
Baltimore, MD 21231

P 1.410.917.5189

June 26, 2026

Re: Aesto LLC Security Incident

To Whom it May Concern:

McDonald Hopkins PLC represents Aesto LLC. We are writing to provide information about a security incident impacting Aesto, which involved data owned by HIPAA Covered Entity Clients. By providing this information, Aesto does not waive any rights or defenses regarding the applicability of law or personal jurisdiction.

On or about December 18, 2025, Aesto experienced a network security incident that impacted a limited portion of their Amazon Web Services (“AWS”) infrastructure. Upon learning of the issue, Aesto commenced a prompt and thorough investigation. As part of Aesto’s investigation, Aesto worked very closely with external cybersecurity professionals experienced in handling these types of incidents.

After an extensive forensic investigation and manual document review, on May 26, 2026, Aesto confirmed that between on or about December 2, 2025, and December 18, 2025, a limited amount of sensitive information pertaining to Covered Entities, which was stored Aesto’s network, may have been accessed and/or acquired by an unauthorized actor. On June 26, 2026, Aesto notified Covered Entities with impacted information of the incident. Aesto has no evidence that any of the information has been misused.

Aesto is committed to maintaining the privacy of sensitive information in its possession and has taken many precautions to safeguard it. Please note, this incident was contained to a limited portion of Aesto’s AWS infrastructure and did not affect the systems of Covered Entities.

Should you have additional questions, please contact McDonald Hopkins at **AestoOptIn@mcdonaldhopkins.com**.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Spencer Pollock".

Spencer Pollock

Baltimore | Chicago | Cleveland | Columbus | Detroit | West Palm Beach

mcdonaldhopkins.com



Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line

<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

RE: NOTICE OF DATA BREACH

Dear <<Full Name>>:

Aesto, LLC ("Aesto") provides healthcare data migration and archiving services for Iroquois Memorial Hospital and writes with important information regarding a recent data security incident at Aesto involving some of your protected health information. The privacy and security of the information we maintain is of the utmost importance to Aesto and Iroquois Memorial Hospital. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened? On or about December 18, 2025, Aesto experienced a network security incident that impacted a limited portion of their Amazon Web Services infrastructure.

What We Are Doing. Upon learning of the issue, Aesto commenced a prompt and thorough investigation. As part of Aesto's investigation, Aesto worked very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, on May 26, 2026, Aesto confirmed that between on or about December 2, 2025, and December 18, 2025, a limited amount of your protected health information pertaining to Iroquois Memorial Hospital, which was stored within Aesto's network, may have been accessed and/or acquired by an unauthorized actor. Aesto has no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved? The information potentially impacted includes your full name, as well as your <<Breached Elements>>.

What You Can Do. Aesto has no evidence that any protected health information has been or will be misused for identity theft or financial fraud as a direct result of this incident. However, out of an abundance of caution, to help protect your identity, Iroquois Memorial Hospital is offering a complimentary <<CM Duration>> month membership of Epiq Privacy Solutions ID 3B Credit Monitoring. For more information on identity theft prevention and Epiq Privacy Solutions ID 3B Credit Monitoring, including instructions on how to activate the complimentary <<CM Duration>> - month membership, please see the additional information provided in this letter. This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. To the extent that it is helpful, we are also suggesting steps you can take to protect your medical information on the following pages.

For More Information. Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. **If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED].** This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 8 AM – 8 PM Central Standard Time (excluding major U.S. holidays). Be prepared to provide **your engagement number B167683.**

Sincerely,

Aesto LLC, *on behalf of*
Iroquois Memorial Hospital



Activation Code: <<Full Name>>
<<ACTIVATION CODE>>
Enrollment Deadline: <<ENROLLMENT DEADLINE>>
Coverage Length: <<CM Duration>> Months

Epiq - Privacy Solutions ID 3B Credit Monitoring

How To Enroll:

- 1) Visit www.privacysolutionsid.com and click “Activate Account”
- 2) Enter the following activation code, <<Activation Code>> and complete the enrollment form
- 3) Complete the identity verification process
- 4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
- 5) Enter your log-in credentials
- 6) You will be directed to your dashboard and activation is complete!

Product Features:

3-Bureau Credit Monitoring with Alerts

Monitors your credit file(s) with each of the 3 Credit Bureaus for key changes, with alerts such as credit inquiries, new accounts, and public records.

VantageScore® 3.0 Credit Score with Score Tracker¹

1-Bureau VantageScore®3.0 (monthly) and Credit Score Tracker.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)

Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring

Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Change of Address Monitoring

Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users’ current or past addresses.

Credit Protection

3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Personal Info Protection

Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

Identity Restoration & Lost Wallet Assistance

Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Up to \$1M Identity Theft Insurance²

Provides up to \$1,000,000 (\$0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT²

Provides up to \$1,000,000 (\$0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 3B Credit Monitoring, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

1 The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore® credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

2 Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. or American Bankers Insurance Company of Florida, an Assurant company. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Security Freeze: A security freeze can be placed without any charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

To place a security freeze on your credit report, you must place your request for a freeze with each of the three major consumer reporting agencies, Equifax, Experian, and TransUnion. To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below or through each of the reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze
1-888-298-0045
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
<https://www.experian.com/freeze/center.html>
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
<https://www.transunion.com/credit-freeze>
P.O. Box 160
Woodlyn, PA 19094

In order to request a security freeze, you may need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. Social Security Card, pay stub, or W2; and
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and should provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you may need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you make a request to the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and may be required to provide the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have between one (1) hour (for requests made online or by phone) or three (3) business days (for requests made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Credit Reports: By law, you may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies. The three national credit reporting agencies have also agreed to provide free weekly online credit reports. You can obtain your free credit report by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>. Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 1000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Protecting Medical Information: We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft:

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

This notification was not delayed by law enforcement.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports.

District of Columbia Residents: District of Columbia residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at 400 6th Street NW, Washington, DC 20001, 202-727-3400, oag@dc.gov, <https://oag.dc.gov/>. The District of Columbia law also allows consumers to place a security freeze on their credit reports without any charge.

Iowa Residents: Iowa residents can contact the Office of the Attorney General to obtain information about steps to take to avoid identity theft from the Iowa Attorney General’s office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General’s office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New Mexico Residents: Individuals have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General’s Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/publications/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Oregon Residents: Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 503-378-4400; <https://www.doj.state.or.us/>.

Rhode Island Residents: We believe that this incident affected <<RI Count>> Rhode Island residents. Rhode Island residents can contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).