[Company Logo]

[Return Address Line 1]
[Return Address Line 2]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

[Date]

RE: Important Security Notification. Please read this entire letter.

Dear [First Name] [Last Name]:

G.I. Medicine Associates, P.C. ("GIMA"), is providing this Notice to inform you about a data security incident that involved unauthorized access to personal information of its patients maintained by one of its vendor's, Aesto, LLC ("Aesto"). Aesto provides healthcare data migration and archiving services for its Covered Entity clients, including GIMA. GIMA takes its patients' privacy seriously, and it is important to us that you and the community that we serve are made fully aware of this recent security incident.

What Happened? On June 26, 2026, Aesto notified GIMA about a cyber incident it experienced on or about December 18, 2025, that impacted a portion of its Amazon Web Services ("AWS") infrastructure that stores GIMA's archived medical records. Upon detecting the unauthorized activity, Aesto immediately contained the incident and commenced a thorough investigation. As part of Aesto's investigation, it engaged leading cybersecurity experts to identify what personal information, if any, was involved.

After an extensive forensic investigation and manual document review, on May 26, 2026, Aesto's forensic experts confirmed that between on or about December 2, 2025, and December 18, 2025, certain protected health information belonging to patients of various Covered Entity clients, including GIMA, stored within Aesto's network may have been accessed and/or acquired by an unauthorized actor.

What Information Was Involved? On or about July 15, 2026 GIMA received the list of patients whose medical records were potentially impacted by Aesto's data breach. Upon further review of this information, GIMA discovered its patients' information, which varied per individual, included full names and one or more of the following elements: address, telephone number, dates of birth, medical record number and Social Security numbers.

What Are We Doing? We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. While Aesto has advised GIMA that there is no evidence of any identity theft or financial fraud related to this incident, out of an abundance of caution, GIMA is offering **complimentary** access to Experian IdentityWorks^{SM} for [##] months to help protect your identity.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [##] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [##]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** [Enrollment End Date] by 11:59 pm UTC (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [Enrollment URL]
- Provide your **activation code**: [Activation Code]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team by [Enrollment End Date] at [TFN] Monday – Friday, 8 am – 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide engagement number [B######] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [##]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call [Experian TFN] toll-free Monday through Friday from 8 am to 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide your engagement number [B######]. Aesto has also created a dedicated and confidential toll-free response line that it has set up to respond to questions at **833-918-8060,** which is staffed with professionals familiar with this incident. Aesto's response line is available Monday through Friday, 8 am – 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide the following Aesto engagement number: **B167683**. Further information about the incident is also posted on Aesto's website at: Notice of Data Security Incident-12-18-25 | Aesto Health. For additional information about what you can do to protect yourself, please review the attached **Information About Identity Theft Protection.**

Sincerely,

[Your Signature Graphic]

[Organization Contact, Title]
[Organization Name]

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.
[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a **free copy** of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three nationwide consumer reporting agencies listed below.

Equifax:	P.O. Box 740241, Atlanta, GA 30374, 1-800-685-1111, www.equifax.com
Experian:	P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion:	P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. We also recommend that you place either a **Fraud Alert** or **Security Freeze** or both to further protect your identity, **at no charge**, as further detailed below.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report **at no cost** to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three nationwide consumer reporting agencies listed below. As soon as the credit bureau confirms your fraud alert, it will notify the others. ***You do not need to contact all three credit bureaus to place a fraud alert on your credit file.***

Equifax	P.O. Box 105069 Atlanta, GA 30348	1-888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	fraud.transunion.com

Security Freezes: You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file **at no cost**. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. ***Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually***. For more information on security freezes, you may contact the three nationwide consumer reporting agencies (listed above) or the FTC as described above.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Complete Address
- Prior Addresses (where you lived over the past five years)
- A legible copy of a government-issued identification card (such as a state driver's license or ID Card, military ID card, birth certificate, etc.)
- Proof of your current residential address (such as a current utility bill or account statement)
- If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (1-877-438-4338), www.ftc.gov/idtheft.

ADDITIONAL STATE-SPECIFIC DISCLOSURES & PROTECTIONS.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

> **Office of the Attorney General of Iowa,** Hoover State Office Building,1305 E. Walnut Street, Des Moines, IA 50319; (515) 281-5164; www.iowaattorneygeneral.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

> **Maryland Office of the Attorney General,** Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us.

Massachusetts residents: You have the right to obtain a police report with respect 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.

New Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following: (1) The unique personal identification number, password, or similar device provided by the consumer reporting agency; (2) Proper identification to verify your identity; and (3) Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report. A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone. A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act. If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act. To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; 1-800-771-7755.

North Carolina residents: You may obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

> **North Carolina Attorney General's Office**, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-5-NO-SCAM (1-877-566-7226) or 1-919-716-6000 (outside NC); www.ncdoj.gov.

Oregon Residents: You may report suspected identity theft to the Federal Trade Commission (as noted above) or the Oregon Department of Justice at:

> **Oregon Department of Justice,** 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392 (toll-free in Oregon), (503) 378-4400, http://www.doj.state.or.us .

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Office of the Attorney General at:

> **Rhode Island Office of the Attorney General,** Consumer Protection Unit, 150 South Main Street, Providence, RI 02903; 1-401-274-4400; http://www.riag.ri.gov.

As noted above, you may obtain a **Security Freeze** on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency as noted above and provide all of the following: (1) The unique personal identification number or password provided by the consumer reporting agency, (2) Proper identification to verify your identity, and (3) The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion, using the contact information and providing the requested information detailed above.

There were Rhode Island __residents impacted by this incident.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001; https://oag.dc.gov/consumer-protection, 1-202-442-9828.

Protecting Your Personal Health Information.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the consumer reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.