

Notice of Breach / Cybersecurity Incident

August 17, 2026 - G.I. Medicine Associates, P.C. ("GIMA"), is posting this Notice to inform you about a cyber 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 (and other healthcare providers) 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 July 15, 2026 GIMA received the list of patients whose medical records were affected by Aesto's data breach. Upon further review of the information, GIMA discovered its patients' information, which varied per individual, included full names and one or more of the following elements: dates of birth, medical information, driver's license numbers, financial account numbers only, health insurance information, individual taxpayer identification numbers, other government identification numbers, and Social Security numbers.

Aesto has advised GIMA that there is no evidence of any identity theft or financial fraud related to this incident. However, out of an abundance of caution, GIMA will be notifying all affected individuals for whom we have an address and whose sensitive personal information was involved in the incident. Out of an abundance of caution, GIMA will be offering individuals whose sensitive information may have been involved in this incident complimentary credit monitoring services for 12 months (or as state mandated) at no charge. Letters with directions on how to enroll in this free credit monitoring service will be mailed shortly.

If you have any further questions regarding this incident, please call Aesto's dedicated and confidential toll-free response line that it has set up to respond to questions at **833-918-8060**. This response line is staffed with professionals familiar with this incident. The response line is available Monday through Friday, 8 am – 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide the following engagement number: **B167683**.

WHAT CAN YOU DO NOW?

Fraud Alerts: It is both recommended and required by certain state laws to advise you of your right to place Fraud Alerts with one of the three major credit bureaus by phone and via TransUnion's, Experian's or Equifax's website **at no cost to you**. A Fraud Alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a Fraud Alert can protect you, but also may delay you when you seek to obtain credit. Initial Fraud Alerts last for one year. Victims of identity theft can also get an extended Fraud Alert for seven (7) years. Contact information for all three credit bureaus to place a Fraud Alert is listed in this Notice.

Monitoring: You should always remain vigilant and monitor your accounts (i.e., account statements and Explanations of Benefits ("EOB")) for suspicious or unusual activity. You should also periodically obtain and review a copy of your Credit Report, **at no charge**, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting anyone (1) or more of the national consumer reporting agencies listed in this Notice.

You may also 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.

Security Freeze: You also have the right to place a security freeze on your credit report **at no cost to you**. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. Unlike a Fraud Alert, to place a Security Freeze on your credit file, you need to make the request at each consumer reporting agency individually. You may make that request by mail or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique

PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<https://www.experian.com/freeze/center.html>

TransUnion (FVAD)

P.O. Box 2000

Chester, PA 19016

<https://freeze.transunion.com>

For more information on security freezes, you may contact the three nationwide consumer reporting agencies listed ABOVE or the FTC as described below:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (1-877-438-4338), and TTY: 1-866-653-4261, and www.ftc.gov/idtheft.

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 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.

GIMA takes the protection of your personal information seriously. We have been advised that Aesto has taken many precautions to safeguard the information entrusted to it and continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

We sincerely apologize to you and all our patients for concern caused by this incident.

Sincerely,

GI Medicine Associates, PC.