Aesto, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Via US Mail

PNNUW000200021
Graham County Hospital
Attn: COMPLIANCE OFFICER
304 W. PROUT
HILL CITY, KS 67642-1435

June 26, 2026

PNNUW00020002100021010210 2A0400

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Dear Compliance Officer:

We are writing to let you know that Aesto, LLC ("Aesto") experienced a cyber incident that involved information your organization entrusted to us. We take this matter seriously and want to provide you with a clear account of what happened, what we've done in response, and what steps are available to you.

What Happened?
On or about December 18, 2025, Aesto experienced a network security incident that impacted a limited portion of our Amazon Web Services ("AWS") infrastructure. Our core data platform, where your live archive resides, was not compromised. Upon learning of the issue, we immediately launched a thorough investigation with experienced external cybersecurity professionals to determine whether sensitive information had been accessed and/or acquired. On May 26, 2026, we confirmed that between on or about December 2, 2025, and December 18, 2025, a limited amount of information stored in our network may have been accessed and/or acquired by an unauthorized actor through forensic analysis. However, your organization's information was not amongst the impacted data contained on the threat actor's list.

What Information Was Involved?
The affected information includes protected health information of certain individuals affiliated with your organization, consisting of full names, dates of birth, medical information, driver's license numbers, financial account numbers only, health insurance information, individual taxpayer identification numbers, other government ID numbers, and Social Security numbers. Not all individuals had Social Security numbers impacted. The list of affected individuals and specific data elements involved for each person will be provided to your organization upon request (*see Next Steps below*).

What We Are Doing.
As part of our investigation, we worked with cybersecurity professionals to secure our network. We have reset credentials, enhanced our security measures and monitoring tools, and are reviewing our existing policies and training protocols to help prevent similar incidents in the future. This was an isolated incident, and we are taking all necessary actions to address the situation and reduce risk going forward. **We are providing an attestation from our cybersecurity professionals detailing the root cause of the incident, the steps we took to remediate and harden our network, and confirmation that no further unauthorized activity has been observed.**

Next Steps and Services We are Offering:

1. Obtain Your Data File of Affected Individuals

Please send an email to **AestoDataReq@transunion.com** by **July 17, 2026**, and we will make arrangements to securely transfer a data file with the list of individuals related to your organization whose protected health information may have been affected by this incident. As the data owner, your organization can then review the files and determine which, if any, individuals should be notified of the incident.

2. Individual Notifications

Upon review of your data file, you may determine legal notification obligations are required. Unfortunately, Aesto is unable to issue individual notifications on your behalf. However, we are providing a notification package for you to assist with any notification obligations you identify. For individual notifications, the package will include Cover Letters with Aesto's letterhead that may be used for individual notifications. The package includes multiple Cover Letter versions to assist with various types of individuals who may need to be notified. The Cover Letters also include a call center for individuals who may have questions. The notification package includes a sample of the FAQs the call center will utilize. **Please note, other than the variable fields, these Cover Letters may not be altered in any way.**

Aesto does not represent that these Cover Letters will fulfill your legal notification obligations. You should seek counsel to determine your legal notification obligations and ensure the notifications you send fulfill all applicable laws. While Aesto has provided a Cover Letter, legal notification obligations typically include additional information such as:

- How to place a fraud alert or a security freeze.
- How to obtain a free credit report.
- Credit monitoring instructions.
- How to protect sensitive information.
- Additional helpful resources.
- Contact information for law enforcement and regulatory bodies.

You may download the notification package using this link:
https://ezshield.sharefile.com/d-s07fa1677a75b466f9ceb7fe5782b7ddf. Do not share this link outside of your response team.

3. Health and Human Services Office of Civil Rights (HHS OCR) Notification

We are offering to notify HHS OCR on your behalf if you choose to **OPT-IN by July 17, 2026.** If you would like to **OPT-IN** HHS OCR notification, you may do so by sending an email to **AestoOptIn@mcdonaldhopkins.com** with the following information by **July 17, 2026**:

a. **Name of your organization.**
b. **Organization's full address.**
c. **Point of contact for your organization (name, email, phone number).**
d. **Type of covered entity: health plan, healthcare clearing house, or healthcare provider.**
e. **Number of impacted individuals.**
f. **Estimated mailing date of your individual notice.**
g. **Whether you plan to use the cover letter as your notification letter. If not, you must provide a sample of your notice letter.**

To **OPT-IN**, you must provide all of the above information by **July 17, 2026** by sending an email to **AestoOptIn@mcdonaldhopkins.com**. Incomplete information *will not* be reported to HHS OCR.

4. State Regulatory Notifications

Aesto is unable notify regulators on your behalf. However, to aid in any regulatory notification obligations you may determine are necessary, the notification package includes a **regulatory letter** detailing the incident including contacts for more information that may be attached to any state regulatory reports.

5. Website and Media Notification

Aesto has posted website notice and provided nation-wide media notices. An example of the media notification is included in the notification package. The media notification includes call center information and a live link to a list of Covered Entities who choose to be named to satisfy their substitute notice obligations. **If you want to add your organization's name to a live link on Aesto's website, please send an email to AestoOptIn@mcdonaldhopkins.com indicating the full name of your organization and your consent to be added to the list.**

Please note, you should seek your own counsel to ensure that Aesto's website and media notice satisfy your substitute notice legal obligations. Aesto does not guarantee that these notices fulfill your legal obligations.

We sincerely regret that this incident occurred. We are committed to maintaining the privacy of information in our possession and continually evaluate and strengthen our practices and internal controls. Since this incident, we have reset passwords and worked with an external cybersecurity firm to further harden our network security. If you have questions, please contact our dedicated and confidential toll-free response line at **833-918-8060.** The response line is staffed with professionals familiar with this incident and is available Monday through Friday, 8 am - 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide **your engagement number B167548.** Thank you for your cooperation and your continued trust.

Sincerely,

Aesto, LLC
1800 International Park Drive, Suite 110
Birmingham, AL 35243

PNNUW00020002100021020202Q0000

McDonald Hopkins
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,

Spencer Pollock

Attestation of Security Investigation

January 23, 2026

On December 18, 2025, McDonald Hopkins as Legal Counsel (“Counsel”) on behalf of Aesto Health (“Aesto”) engaged GuidePoint Security, LLC (“GuidePoint”) to perform Incident Response services. GuidePoint utilized Aesto’s existing security tools and data sources and deployed supplemental tools to establish broad environmental visibility as outlined below. GuidePoint leveraged industry standard Incident Response techniques and tools to the best extent possible to identify the intrusion vector, signs of data theft, and other threat actor related activity. GuidePoint has made every effort to perform a thorough and comprehensive analysis and to provide appropriate recommendations. GuidePoint is bound by defined scope, allocated time, therefore this investigation is the result of a point-in-time assessment based on the state of the Aesto’s environment at the conclusion of the investigation.

REMEDIATION SUMMARY

Based on the available data, GuidePoint was able to determine that Aesto was the victim of a cyber incident with an earliest known date of December 2, 2025.

GuidePoint has been able to identify how the threat actor breached the network, the accounts that the threat actor managed to compromise, the changes the threat actor made to existing AWS Lambda functions, and other threat actor actions taken during the dwell time on the network. Based on these findings and other best practices, Aesto has taken numerous security steps to remediate this incident and to harden their defense posture moving forward. Some of these steps include:

1. Closed the security gaps exploited by the threat actor to gain access to the network.
2. Deleted the impacted Lambda functions.
3. Rotated all impacted AWS secrets.
4. Deleted unauthorized files uploaded by the threat actor.

Based on these steps and the continuing monitoring of the network, GuidePoint has not observed any threat actor activity on the network since December 18, 2025.

(877) 889-0132 dfir.team@guidepointsecurity.com

Aesto, LLC
c/o HaystackID Return mail processing
PO Box 173071 | Milwaukee, WI 53217

Via First-Class Mail

<<First Name>> <<Last Name >
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA <<HEADER>>

Dear <<First Name>>:

Aesto, LLC ("Aesto") provides healthcare data migration and archiving services for Graham County 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 Graham County 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 Graham County Hospital, which was stored in 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. 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 833-918-8060. 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. Time. The response line is available Monday through Friday, 8 am – 8 pm Central Time, excluding U.S. national holidays. Be prepared to provide **your engagement number B167683.**

Sincerely,

Aesto LLC, *on behalf of*
Graham County Hospital

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity. You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed 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 for a fee by contacting one or more of the three national credit reporting agencies. You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative, you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html

Equifax	P.O. Box 740241 Atlanta, GA 30374 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com/personal/credit-report-services
TransUnion	P.O. Box 1000 Chester, PA 19016 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

For Iowa and Oregon residents, you are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

For Massachusetts residents, you are advised of their right to obtain a police report in connection with this incident.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at www.ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/.

For Rhode Island residents, this data event involves zero individuals in Rhode Island. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.