EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, WAGI does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about March 10, 2025, WAGI discovered that certain data was accessed and exposed by an unknown third party. WAGI quickly took steps to confirm that its systems were secure and launched an investigation into the nature and scope of the activity. Upon identifying the at-risk data, WAGI initiated a diligent review of the data to determine what information was included and to whom this information belongs. On May 1, 2025, we identified a specific impact to a group of individuals. On May 9, 2025, we provided preliminary notice of this event to the Department of Health and Human services, as well as a notice on our website. WAGI continues its detailed review of the relevant data in an effort to notify all individuals whose information may have been impacted.

The information that could have been subject to unauthorized access includes name, date of birth, Social Security number, and financial account information.

Notice to Washington Residents

On or about May 23, 2025, WAGI began providing written notice of this incident to one thousand two hundred and sixty-one (1,261) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, WAGI moved quickly to investigate and respond to the incident, assess the security of WAGI systems, and identify potentially affected individuals. WAGI is also working to implement additional safeguards. WAGI is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, WAGI is providing impacted individuals with guidance on how to better protect against identity theft and fraud. WAGI is providing individuals with information on how to place a fraud alert and security freeze on one's credit file and the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

WAGI is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. WAGI notified the U.S. Department of Health and Human Services, attached here as ***Exhibit B***, and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

EXHIBIT A

P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<XXXXXXXX>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

May 23, 2025

NOTICE OF <<VARIABLE DATA 1>>

Dear <<First Name>> <<Last Name>>:

Washington Gastroenterology ("WAGI") is writing to notify you about a recent matter that may affect certain information related to you. This letter provides you with details about this matter, our response, and the resources available to assist you with safeguarding your information, should you feel it appropriate to do so.

What Happened? On or about March 10, 2025, WAGI discovered that certain data was accessed and exposed by an unknown third party. WAGI quickly took steps to confirm that its systems were secure and launched an investigation into the nature and scope of the activity. Upon identifying the at-risk data, WAGI initiated a diligent review of the data to determine what information was included and to whom this information belongs. We are notifying all individuals whose information may have been impacted.

What Information Was Involved? The investigation determined that the information impacted may include your name, and <<Variable Data 3>>.

What We Are Doing. We take this incident and the obligation to safeguard the information in our care very seriously. After discovering the incident, we promptly took steps to confirm our system security and engaged a third-party forensic firm to assist in conducting a comprehensive investigation. This incident involved a legacy WAGI system, and no current networks or affiliate systems were impacted by this incident. As an added precaution, we are offering <<Membership Offering Length>> of credit monitoring and identity restoration services through IDX. If you wish to activate these complimentary services, you may follow the instructions included in the attached *Steps You Can Take to Help Protect Personal Information*. If you elect to activate these services, you must enroll in these services directly as we are unable to act on your behalf to do so.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity to detect errors over the next 12 to 24 months.

For More Information. If you have additional questions or concerns, please feel free to call us at 1-800-939-4170. We are available Monday through Friday from 6 am - 6 pm Pacific Time, excluding major U.S. holidays.

Sincerely,
Washington Gastroenterology

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that

they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

EXHIBIT B

From: Portal <OCR_Portal@nih.gov>
Sent: Friday, May 9, 2025 3:50 PM
To: Amanda Harvey <aharvey@mullen.law>
Subject: 32586408 for breach submitted to Office for Civil Rights

32586408 (Breach Tracking Number:)

Thank you for filing a breach notification via the website of the Office for Civil Rights (OCR) at the Department of Health and Human Services. This is an automated response to acknowledge receipt of your breach notification.

Please do not fax, email, or mail a copy of this breach notification to us as that may delay the processing of your breach notification.

If you have questions or would like to provide feedback about the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification process, or OCR's investigative process, please send us an email at OCRbreachreportingfeedback@hhs.gov

Notice to the Secretary of HHS

Breach of Unsecured Protected Health Information

This site is available as we continuously work to make improvements to better serve the public. Should you need assistance with this site or have any questions, please email ocrprivacy@hhs.gov or call us toll-free: (800) 368-1019, TDD toll-free: (800) 537-7697.

General:

***Report Type: What type of breach report are you filing?**

☒ Initial Breach Report

☐ Addendum to Previous Report

*If Addendum, Do you have a valid breach tracking number?

☐ Yes ☐ No

*If yes, please supply your breach tracking number:

Contact:

***Please select one of the following:**

☒ **Are you a Covered Entity who experienced a breach, and are you filing on behalf of your organization?**

***Name of Covered Entity (Name of Entity, no abbreviations, no acronyms):** Washington Gastroenterology

***Type of Covered Entity:** ☐ Health Plan ☐ Healthcare Clearing House ☒ Healthcare Provider

***Street Address 1**: 3209 S. 23rd Street

Street Address 2:

***City**: Tacoma

***State**: Washington

***ZIP**: 98405

Covered Entity Point of Contact Information:

***First Name**: Amanda

***Last Name**: Harvey

***Email**: aharvey@mullen.law

***Phone Number**: (267) 930-1697

☐ Home / Cell

☒ Work

☐ **Are you a Business Associate who experienced a breach, and are you filing on behalf of a Covered Entity?**

***Name of Business Associate (Name of Entity Only, no abbreviations, no acronyms):**

Business Associate Street Address 1:

Street Address 2:

***City:**

***State:**

***ZIP:**

Business Associate Point of Contact Information:

***First Name:**

***Last Name:**

***Email:**

***Phone Number:** (XXX) XXX-XXXX

☐ Home / Cell

☐ Work

Enter the contact information for all Covered Entities on whose behalf you are filing. Can add multiple Covered Entities.

***Name of Covered Entity 1 (Name of Entity Only, no abbreviations, no acronyms):**
***Covered Entity 1 Street Address:**
Street Address 2:
***City:**
***State:**
***ZIP:**
Covered Entity Address:
***Street Address 1:**
Street Address 2:
***City:**
***State:**
***ZIP:**
Covered Entity Point of Contact Information:
***First Name:**
***Last Name:**
***Email:**
***Phone Number:** (XXX) XXX-XXXX

☐ Home / Cell

☐ Work

***Type of Covered Entity:** ☐ Health Plan ☐ Healthcare Clearing House ☐ Healthcare Provider

☐ **Are you a Covered Entity filing because your Business Associate experienced a breach?**

***Name of Covered Entity (Name of Entity Only, no abbreviations, no acronyms):**
***Type of Covered Entity:** ☐ Health Plan ☐ Healthcare Clearing House ☐ Healthcare Provider
Covered Entity Address:
***Street Address 1:**
Street Address 2:
***City:**
***State:**
***ZIP:**
Covered Entity Point of Contact Information:
***First Name:**
***Last Name:**
***Email:**
***Phone Number:** (XXX) XXX-XXXX

☐ Home / Cell

☐ Work

***Name of Business Associate (Name of Entity Only, no abbreviations, no acronyms):**
Business Associate Street Address 1:

Street Address 2:
***City:**
***State:**
***ZIP:**
Business Associate Point of Contact Information:
***First Name:**
***Last Name:**
***Email:**
***Phone Number:** (XXX) XXX-XXXX
☐ Home / Cell
☐ Work

Breach:
***Breach Affecting: How many individuals are affected by the breach?**
☒ 500 or More Individuals
☐ Fewer Than 500 Individuals

Breach Dates: Please provide the state and end date (if applicable) for the dates the breach occurred in.
***Breach Start Date**: 10/23/2024
***Breach End Date**: 10/23/2024

Discovery Dates: Please provide the start and end date (if applicable) for the dates the breach was discovered.
***Discovery Start Date**: 03/10/2025
***Discovery End Date**: 03/10/2025

***Approximate Number of Individuals Affect by the Breach:** 501

***Type of Breach:**
☒ Hacking / IT Incident
☐ Improper Disposal
☐ Loss
☐ Theft
☐ Unauthorized Access / Disclosure

***Location of Breach:**
☐ Desktop Computer
☐ Electronic Medical Record
☐ Email
☐ Laptop
☒ Network Server
☐ Other Portable Electronic Device
☐ Paper / Films
☐ Other:
*Location of Breach (if Other):

***Type of Protected Health Information Involved in Breach:**
☐ Clinical
☒ Diagnosis / Conditions
☐ Lab Results
☐ Medications
☐ Other Treatment Information

☐ Demographic
- ☒ Address / ZIP
- ☒ Date of Birth
- ☐ Driver's License
- ☒ Name
- ☐ Social Security number
- ☐ Other Identifier

☐ Financial
- ☐ Claims Information
- ☐ Credit Card / Bank Account Number
- ☐ Other Financial Information

☐ Other

*Type of Protected Health Information Involved in Breach (if Other):

***Brief Description of the Breach (max 4,000 characters):**

On or about March 10, 2025, Washington Gastroenterology ("WAGI") discovered that certain data was potentially accessed and exposed by an unknown third party. WAGI quickly took steps to confirm that its systems were secure and launched an investigation into the nature and scope of the activity. Upon identifying the at-risk data, we have initiated a diligent review of the data to determine what information was included and to whom this information belongs. This process is currently underway.

***Safeguards in Place Prior to Breach:**

- ☐ None
- ☒ Privacy Rule Safeguards (Training, Policies and Procedures, etc.)
- ☒ Security Rule Administrative Safeguards (Risk Analysis, Risk Management, etc.)
- ☒ Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.)
- ☒ Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)

Notice of Breach and Actions Taken:

***Individual Notice Start Date:** 05/09/2025

Individual Notice Provided Projected/Expected End Date: MM/DD/YYYY

Was Substitute Notice Required? ☒ Yes ☐ No

Was Media Notice Required? ☒ Yes ☐ No

***Actions Taken In Response to Breach:**

- ☐ Adopted encryption technologies
- ☐ Changed password/strengthened password requirements
- ☐ Created a new/updated Security Rule Risk Management Plan
- ☒ Implemented new technical safeguards
- ☐ Implemented periodic technical and nontechnical evaluations

☐ Improved physical security
☐ Performed a new/updated Security Rule Risk Analysis
☐ Provided business associate with additional training on HIPAA requirements
☐ Provided individuals with free credit monitoring
☐ Revised business associate contracts
☐ Revised policies and procedures
☐ Sanctioned workforce members involved (including termination)
☒ Took steps to mitigate harm
☐ Trained or retrained workforce members
☒ Other

Please provide explanation of other. No specific action was taken with the impacted legacy system as it was not in use at the time of the event and has since been decommissioned.

Attestation:

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

Name: