Gastroenterology
CONSULTANTS, P.A.

PO Box 4129
Everett WA 98204

ENDORSE

NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

BREAK

August 6, 2021

SEQ
CODE 2D
Ver 8P

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

Gastroenterology Consultants, P.A. ("Gastroenterology") is writing to inform you of a recent data security incident that may have resulted in an unauthorized access of your sensitive personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the event, steps we are taking in response, and resources available to help you protect against the misuse of your information.

What Happened? On January 10, 2021, Gastroenterology experienced a data security incident involving a ransomware virus which resulted in the potential exposure of our patients' personal information to an unauthorized individual. Upon discovery of the attack, Gastroenterology promptly engaged a specialized cybersecurity firm and breach counsel to conduct a forensic investigation to determine the nature and scope of the incident. The investigation indicated some files containing sensitive personal information may have been exfiltrated by the attacker. However, based on our negotiated resolution with the attacker, we received assurances that any potential exfiltrated data had been destroyed. Gastroenterology promptly performed data mining to identify the specific individuals and the type of information that may have been compromised. This step was necessary so that we could identify the affected population in order to send out notice of the incident to these individuals. However, after undertaking the extensive data mining process, Gastroenterology determined that it would take an unreasonably long period of time and effort to manually review thousands of documents. Therefore, although there is no evidence of any unauthorized use of patient data, Gastroenterology has determined it best to issue notifications to all patients. Notably our patient medical record system was not impacted by the incident. However, there were some sensitive personal information included in the files prepared by employees to facilitate patient processing.

What Information Was Involved? The types of information impacted varied by patients and not every patients was affected by this incident. However, the information present during the period of unauthorized access may have included your name, address, and personal health information. Your social security number and other sensitive financial information was not exposed.

What We Are Doing We are committed to doing everything we can to help protect the privacy and security of the personal information in our care. Since the discovery of the incident, we have taken and will continue to take steps to mitigate the risk of future issues. Notably, we launched an investigation to determine the full nature and scope of this incident. Additionally, we deployed endpoint monitoring and detection tools to continuously monitor for any malicious activity within our systems. We are also providing you with guidance on how to help protect against the possibility of information misuse.

Again, based on available evidence through monitoring, we are not aware of your information being used in an unauthorized manner, but out of an abundance of caution, we wanted to inform you of this incident.

What You Can Do We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information We recognize that you may have questions not addressed in this letter. If you have additional questions, please call (833) 909-3925 (toll free) during the hours of 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday, (excluding U.S. national holidays) or email us at potential_databreach_questions@gastroconsultants.com.

Gastroenterology sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Nita James R.N.

Nita James
Gastroenterology Consultants, P.A.

Steps You Can Take to Help Protect Your Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/cred

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped 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 or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

More information can also be obtained by contacting the Federal Trade Commission:
Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov.

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon*, and *West Virginia*: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a 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.

For residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

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