Notification of Privacy Incident

Galen Medical Group is committed to our patients' privacy. In pursuant to 45 CFR 164.404(d)(2) Galen is posting the below Substitute Notice. As an initial matter, please be aware that this incident should not disrupt or interfere with the care you received or will receive at Galen. We sincerely regret any concern or inconvenience this notice may cause you. If you have additional questions or concerns after reading the below notice letter, please feel free to call Galen's Privacy Officer at (423) 385-2024, option 2 or by emailing privacy@galenmedical.com.

Substitute Notice Issued on Behalf of Specialty Networks, LLC

Chattanooga, Tennessee –September 19, 2024 – Galen Medical Group, PC learned of a data security incident, experienced by its vendor, Specialty Networks, LLC ("Specialty Networks", Prime Imaging) that may have impacted personal and/or protected health information belonging to certain current and former patients. Specialty Networks provides radiology information systems, digital transcription services, and Enterprise Practice Management solutions for medical facilities.

On December 18, 2023, Specialty Networks became aware of unusual activity in its network. Upon discovering this activity, Specialty Networks immediately took steps to secure the network and engaged a digital forensics and incident response firm to conduct an investigation to determine what happened and whether any data within its environment may have been impacted. The investigation revealed that on or around December 11, 2023, an unauthorized actor acquired certain data stored within its systems. Specialty Networks then undertook a comprehensive review of the potentially impacted data and, on May 31, 2024, determined that certain personal and/or protected health information may have been involved. On June 12, 2024, Specialty Networks notified Galen Medical Group, PC regarding this incident. On June 24, 2024, Galen Medical Group, PC directed Specialty Networks to provide formal notice to affected individuals. Specialty Networks then worked to verify the affected information and mailing addresses for impacted individuals to effectuate formal notification, with address verification efforts completed on August 12, 2024.

The personal and protected health information that may have been involved in the incident included: name, date of birth, driver's license number, Social Security number, medical record number, treatment and condition information, diagnoses, medications, and health insurance information.

As soon as it discovered the incident, Specialty Networks took the steps referenced above. Specialty Networks also notified the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the responsible parties accountable, if possible. Specialty Networks takes the security and privacy of personal information in its possession very seriously and has taken additional steps to prevent a similar event from occurring in the future.

On August 15, 2024, Specialty Networks mailed notice of this incident to potentially impacted individuals for which Specialty Networks had identifiable address information. In this notification letter, Specialty Networks provided information about the incident and steps that potentially affected individuals can take to protect their information. Specialty Networks also offered individuals access to complimentary identity protection services through IDX.

Specialty Networks has established a toll-free call center to answer questions about the incident and to address related concerns. Call center representatives are available Monday through Friday between 8:00 am to 8:00 pm Central Time and can be reached at 1-888-678-3575. All affected individuals may qualify for complimentary identity protection services through IDX. Individuals who have not received a notification letter must obtain verification of eligibility through the call center to enroll in services.

Specialty Networks takes the privacy and security of all information within its possession very seriously. Thank you for your understanding about this incident.

While we are not aware of the misuse of any affected individual's information, we are providing the following information to help those who want to know more about steps they can take to protect themselves and their personal information:

What steps can I take to protect my personal information?

- Please notify your financial institution immediately if you detect any suspicious activity on any of your accounts, including unauthorized transactions or new accounts opened in your name that you do not recognize. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.
- You can request a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To do so, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is listed at the bottom of this page.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.
- Additional information on what you can do to better protect yourself is included in your notification letter.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348 . Use the following contact information for the three nationwide credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

How do I put a fraud alert on my account?

You may consider placing a fraud alert on your credit report. This fraud alert statement informs creditors to possible fraudulent activity within your report and requests that your creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is included in the letter and is also listed at the bottom of this page.

How do I put a security freeze on my credit reports?

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, or regular stamped mail, or online by following the instructions found at the websites listed below. You will need to provide the following information when requesting a security freeze (note that if you are making a request 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) address. You may also be asked to provide other personal information such as your email address, 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. There is no charge to place, lift, or remove a freeze. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	Experian Security Freeze	TransUnion (FVAD)
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-909-8872
www.equifax.com	www.experian.com	www.transunion.com

What should I do if my family member was involved in the incident and is deceased?

You may choose to notify the three major credit bureaus, Equifax, Experian and Trans Union, and request they flag the deceased credit file. This will prevent the credit file information from being used to open credit. To make this request, mail a copy of your family member's death certificate to each company at the addresses below.

Equifax	Experian	TransUnion
Equifax Information Services	Experian Information Services	Transunion Information Services
P.O. Box 740256	P.O. Box 9701	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

What should I do if my minor child or protected person's information was involved in the incident?

You can request that each of the three national credit reporting agencies perform a manual search for a minor's or protected person's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report ay fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft. Contact information for the three credit reporting agencies may be found above.