



By: U.S. Mail and Email (ldtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202



To whom it may concern,

We have recently learned that some personal information of SurgCenter of Western Maryland's patients may have been exposed in a security incident. Under an abundance of caution, SurgCenter of Western Maryland is giving you notice of that incident.

What Happened?

On January 31, 2025, Precision Orthopedics Management, one of SurgCenter of Western Maryland's former owners, advised us that Precision Orthopedics Management was subject to a data breach incident via a phishing attempt on one of their email accounts. They determined that the account included an secure email from SurgCenter of Western Maryland which contained operational information deemed necessary for the owners to review.

An attachment to that email included the names, dates of birth, a description of the services provided at SurgCenter of Western Maryland, the name of the treating provider, and other treatment or diagnostic information for as many as 354 individuals. The attachment did not include any financial information or social security numbers. It was determined that during the incident, the email and/or the attachment might have been accessed during the incident, although Precision advised that it was unable to confirm if the attachment itself was accessed. While the incident occurred in September of 2024, Precision Orthopedics Management did not become aware of the incident until after it was no longer an owner. Precision Orthopedics Management gave us notice of the incident at the conclusion of their investigation.

Our Investigation

Based on that information, SurgCenter of Western Maryland began its own investigation of the incident. After a thorough review of our physical, administrative, and technical security standards and consulting with independent IT professionals, we concluded that SurgCenter of Western Maryland did not experience a breach and that its information security was intact. With the understanding that Precision Orthopedics Management has already given notice to both you and 84 of the 354 individuals separately under their reporting obligations, we concluded that an additional 270 Maryland residents out of the 354 individuals may have had their personal information accessed in the Precision Orthopedics Management incident. These 270 residents were not given notice of the incident by Precision Orthopedics Management.

Following the delivery of this letter to you, we will provide each of these 270 residents with a copy of the attached letter and advise them of the resources available to assist them in maintaining the privacy of their information.



Corrective Actions

After this investigation, we reviewed our physical, administrative, and technical security measures for the purposes of better understanding and improving our information security. We implemented additional security measures to reduce the risk of future incidents, including adding additional administrative and technical safeguards. Lastly, we have undergone extensive personnel training on the importance of maintaining patient privacy.

Contact Information

Should you have any questions, please do not hesitate to contact me at SurgCenter of Western Maryland, c/o of the Privacy Officer, 12252 Williams RD SE, STE 103, Cumberland, MD 21502, Phone: 240-522-0185

Sincerely,

A handwritten signature in black ink, appearing to read 'Raghu Reddy', is written over a horizontal line.

RAGHU REDDY, CHIEF ADMINISTRATIVE OFFICER, PRIVACY OFFICER

(1) Attachment, Form Notice

[INSERT LETTERHEAD]

<Name>
<address>
<second address>
<City>, <State> <zip code>

Dear <Name>,

We have learned that your personal information may have been exposed in a recent security incident. The purpose of this letter is to notify you of the incident in accordance with applicable breach notification laws.

What Happened?

On January 31, 2025, we learned that a former owner of SurgCenter of Western Maryland was subject to a data breach incident via a phishing attempt on one of their email accounts. They determined that the account included an email from SurgCenter of Western Maryland which contained certain information deemed necessary for the owners to review.

A separate attachment to that email included the names, dates of birth, a description of the services provided at SurgCenter of Western Maryland, the name of the treating provider, and other treatment or diagnostic information. The attachment did not include any financial information or social security numbers. It was determined that during the incident, the email and/or the attachment might have been accessed during the incident, although it was not determined conclusively if the attachment itself was accessed. While the incident occurred in September of 2024, we did not receive notice of the incident at the conclusion of the former owner's investigation in January.

Based on that information, SurgCenter of Western Maryland began its own review of the incident. After consulting with independent IT experts and an extensive internal review, we have concluded that your information may have been involved in this incident.

What Next?

You may contact SurgCenter of Western Maryland, c/o of the Privacy Officer at <phone number>, <address> if you have any questions.

As a precautionary measure, you may wish to remain vigilant in monitoring your personal information. The following government agencies are available to provide you with information on steps that you may take to protect your privacy.

1. The Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington DC 20580, 1-877-IDTHEFT, www.consumer.ftc.gov, www.ftc.gov/idtheft.
2. The Maryland Office of the Attorney General, Attn: Security Breach Notification, 200 St. Paul Place, Baltimore, MD 21202, 410-576-6574, 1-888-743-0023 (Toll free), Idtheft@oag.state.md.us, or www.marylandattorneygeneral.gov/Pages/IdentityTheft/databreach.aspx.

You may also wish to contact any of the consumer reporting agencies if you have concerns about suspicious activity or if you wish to obtain additional information about what steps you may take to protect your identity:

1. Equifax, PO Box 105069, Atlanta, GA 30348-5069, 1-888-378-4329, www.equifax.com or www.equifax.com/personal/contact-us/.
2. Experian, PO Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com or <https://www.experian.com/help/identity-theft-victim-assistance.html>.
3. TransUnion; Consumer Disclosure Center, PO Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com or <https://www.transunion.com/get-credit-report/mail-or-phone>.

You may also obtain free credit reports by visiting <http://www.annualcreditreport.com>, by calling 877-322-8228, or by completing a free credit request report form available on their website to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

<We value our relationship with each and every one of our patients. Please know that SurgCenter of Western Maryland will continue to remain vigilant while protecting your privacy.>

Sincerely,
