Vision Upright MRI, LLC

828 SOUTH BASCOM AVE, SUITE 110 SAN JOSE CALIFORNIA 95128-2652
408-292-7970 | FAX: 408-292-7966 www.VisionMRI.com

Date of Notification: May 27, 2025

NOTICE OF DATA BREACH AFFECTING YOUR PROTECTED HEALTH INFORMATION (PHI)

To Our Clients,

The Health Insurance Portability and Accountability Act (HIPAA) requires Vision Upright MRI (Vision) to notify potentially affected clients of data breaches. Please be advised that on December 10, 2019, Vision learned of a security breach that may have affected some Vision clients in mid-2018 until corrective measures were implemented in December 2020. Please note that while this date is provided based on initial information, we are unable to confirm a specific date at this time. Vision is individually notifying patients in our database, however, some patients' addresses are unavailable to us. This message constitutes substitute service for those clients we are unable to reach due to insufficient contact information.

Brief Description of Breach: We regret to inform some patients that confidential health information regarding you was accessed through an unauthorized user. A hacktivist organization known as "Greenbone" discovered and informed Vision of an unintended deficiency in our firewall configuration, which had been present since mid-2018, allowing a backdoor entry for an unauthorized entity to view and access our web-based imaging system server. This server houses our study list which contains certain identifiable information of our Vision patients. The Greenbone hacker had brought this to our attention in an email detailing their entry into our servers and ability to access client's PHI.

PHI Involved: As a result of this breach, the hacker was able to see that an MRI was performed and imported X-rays were stored for patients at our clinics, coupled with the patient's full name and date of birth. No financial information was compromised. No other information was accessed.

Vision's Response: Vision immediately launched an internal investigation to determine the scope and cause of the breach. As part of this investigation, our technical security officer identified and corrected a misconfigured firewall on December 4, 2020, which had been allowing unintended access. In addition, we conducted a thorough review of our security infrastructure—including detailed analysis of system logs and protocols—to ascertain any further vulnerabilities. To mitigate potential risks, we tightened our overall security protections by deactivating our web-based imaging system server and implementing enhanced procedures to increase the frequency of data log monitoring and audits. These comprehensive measures have contained the breach and eliminated unauthorized access. We strive to protect our patient's data and sensitive information from unauthorized persons or entities.

What You Can Do: While no financial information was taken, it's always a good idea to stay proactive about protecting your personal information. Below are some steps you can take, along with links to helpful resources:

Monitor Your Financial Accounts

- Regularly review your bank statements and credit card activity. If you notice any unusual transactions, contact your financial institution immediately. You can also learn more about keeping your accounts secure at the Federal Trade Commission (FTC).

Review Your Credit Reports

- Obtain a free credit report annually from the major credit reporting agencies:
  Equifax
  Experian
  TransUnion

For further guidance on safeguarding your identity, visit your state's official identity theft protection page or check out the resources at IdentityTheft.gov.

Stay Alert for Suspicious Activity

- Set up alerts with your bank or credit bureaus to stay informed of any changes. If you observe any irregularities or suspect unauthorized activity, promptly contact your financial institution and consider placing a fraud alert on your credit file.

Our commitment is to protect your privacy and support you in safeguarding your personal information. If you have any questions or need further assistance, please contact us at 408-292-7970.

Contact Information: We sincerely apologize for this situation and understand that it may cause you concern. Please know that we take the privacy of our patients very seriously, and made every effort to correct this issue and protect the sensitive information about you. Confidentiality is key in our practice in keeping your information safe. If you have any further questions or would like further information regarding this breach, please contact us via the email or toll-free number below.

Sincerely,

Kassidi Freel

Kassidi Freel, Privacy & Security Officer
Phone: (408) 292-7970
Toll-Free Number: (279) 205-2738
Email: Kassidi@visionupright.com