

MEDIA NOTICE

Shields Health Care Group Notification of Data Privacy Event

Shields Health Care Group (“Shields”) recently became aware of suspicious activity on its network. Shields provides management and imaging services on behalf of the health care facilities (“Facility Partners”) listed below. With the assistance of third-party forensic specialists, Shields took immediate steps to contain the incident and to investigate the nature and scope of the incident. Shields is issuing this notice on behalf of itself and the Facility Partners to communicate what is known about the incident, the response, and steps impacted individuals can take, if deemed appropriate. Certain patients of these Facility Partners may be impacted.

What Happened? On March 28, 2022, Shields was alerted to suspicious activity that may have involved data compromise. Shields immediately launched an investigation into this issue and worked with subject matter specialists to determine the full nature and scope of the event.

This investigation determined that an unknown actor gained access to certain Shields systems from March 7, 2022 to March 21, 2022. Furthermore, the investigation revealed that certain data was acquired by the unknown actor within that time frame. Although Shields had identified and investigated a security alert on or around March 18, 2022, data theft was not confirmed at that time.

What Information Was Involved? To date, Shields has no evidence to indicate that any information from this incident was used to commit identity theft or fraud. However, the type of information that was or may have been impacted could include one or more of the following: Full name, Social Security number, date of birth, home address, provider information, diagnosis, billing information, insurance number and information, medical record number, patient ID, and other medical or treatment information. Shields review of the impacted data is ongoing.

What Are We Doing? Shields takes the confidentiality, privacy, and security of information in its care seriously. Upon discovery, Shields secured its system and launched an investigation with third party forensics specialists to determine the nature of the activity and the scope of potentially impacted data. Shields rebuilt certain systems and continues to review and further enhance its existing protections as part of an ongoing commitment to data security.

Shields notified federal law enforcement and will report this incident to relevant state and federal regulators. Once the review of impacted data is complete, Shields will directly notify impacted individuals where possible so that they may take further steps to help protect their information, should they feel it appropriate to do so.

What Can Affected Individuals Do? While Shields has no evidence to indicate identity theft or fraud occurred as a result of this incident, Shields encourages impacted individuals to review *Steps You Can Take to Help Protect Your Information*, which is included below.

For More Information. Individuals with questions about this event can call (855) 503-3386 from 9:00 a.m. to 6:30 p.m., Eastern Time, Monday through Friday, excluding major U.S. holidays. Individuals can also find information on our website, at <https://shields.com/>.

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. The number of impacted Rhode Island residents is unknown at this time. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

Shields MRI of Framingham, LLC
Shields PET/CT at CMMC, LLC
Shields PET_CT at Berkshire Medical Center, LLC
Shields PET-CT at Cooley Dickinson Hospital, LLC
Shields PET-CT at Emerson Hospital, LLC
Shields Radiology Associates, PC
Shields Signature Imaging, LLC
Shields Sturdy PET-CT, LLC
Shields-Tufts Medical Center Imaging Management, LLC (a business associate to Tufts Medical Center, Inc.)
South Shore Regional MRI Limited Partnership
Southeastern Massachusetts Regional MRI Limited Partnership
SportsMedicine Atlantic Orthopaedics P.A.
Tufts Medical Center, Inc.
UMass Memorial HealthAlliance MRI Center, LLC
UMass Memorial MRI - Marlborough, LLC
UMass Memorial MRI & Imaging Center, LLC
Winchester Hospital / Shields MRI, LLC
Radiation Therapy of Southeastern Massachusetts, LLC
Radiation Therapy of Winchester, LLC
South Suburban Oncology Center Limited Partnership
Shields Imaging of North Shore, LLC