EAST BRUNSWICK OPEN UPRIGHT MRI

NOTICE OF SECURITY INCIDENT

April 27, 2021

As you may know, the ownership of East Brunswick Open Upright MRI (EBMRI) changed hands in December 2020. After the change of ownership, EBMRI discovered a security incident involving a radiology PACS server of the prior owner that contained some EBMRI patient information. EBMRI is unaware of any misuse of your personal or health information as a result of this incident.

What Happened? During the period from March 1, 2021 to March 26, 2021, EBMRI learned that the PACS server had been breached by an unauthorized party beginning on or about August 26, 2019. Upon learning of this incident, EBMRI undertook an investigation to determine causal factors as well as actions to ensure EBMRI's systems are secure. The investigation revealed that an insecure port allowed access by unauthorized persons to certain information stored in the PACS server. We also confirmed that all unauthorized access was terminated on or about February 23, 2021.

What Personal Information Was Involved? Based on our investigation, the information accessible to unauthorized persons included <u>only</u> some or all of the following: radiology exam/study description and date and hour of exam, patient name, patient date of birth, patient ID (internally assigned by EBMRI and unrelated to any other patient information), radiology exam ID (assigned by radiology machine), ordering physician, and modality type. Based on our investigation, the following information was **<u>not</u>** involved in this incident and remained secure: email or postal address; radiographic images, reports or medical records; Social Security number; any financial information such as credit card or bank information; and medical insurance card information.

What We Are Doing. We take the privacy and security of personal and health information seriously. As part of the transition of ownership of EBMRI and in response to this incident, we have been implementing updated technology and enhanced systems security, as well as a comprehensive HIPAA privacy and security program and training. We will take further action as necessary to ensure the security of our systems.

What You Can Do. EBMRI is unaware of any misuse of your personal information as a result of this incident. There are actions you can take to protect your personal information. Please review the *Identity Theft Prevention Information* in the attached *Security Incident Q&A* document.

For More Information. EBMRI realizes you may have questions that are not addressed in this notice. As such, we have prepared the attached *Security Incident Q&A* document to provide further information about this incident. We sincerely apologize for any concern or inconvenience this issue has caused you.

*****

EAST BRUNSWICK OPEN UPRIGHT MRI

SECURITY INCIDENT Q&A

East Brunswick Open Upright MRI (**EBMRI**) provides the following "questions and answers" in order to assist patients who received written notification of a security breach incident involving a PACS server containing certain patient information. This notice will be posted for a period of 90 days, beginning April 27, 2021.

	QUESTION	RESPONSE
1.	What happened?	EBMRI underwent a change of ownership and management in December 2020. Between March 1, 2021 and March 26, 2021, the new owners of EBMRI learned of a security incident relating to a PACS server that belonged to the prior owner. The new owners undertook a detailed investigation to get to the root cause of the incident, the types and amount of patient information affected, and how the issue could be mitigated and resolved. The investigation revealed that an insecure port (or communication endpoint) allowed access to unauthorized persons to a portion of the information in the PACS system. Based on the investigation, access was possible between August 26, 2019 and February 23, 2021.
2.	What is a PACS server?	Radiology imaging centers typically use a specialized software for electronic storage of patient information, radiographic images and radiographic reports. This system is called a Picture Archiving and Communication System, or PACS. The PACS software is typically contained on a computer or "server" that houses the software and the patient information within the software.
3.	How is medical information accessed in the PACS system?	Generally speaking, a PACS system may be accessed through a computer desktop application or remotely through the internet or through a virtual private network, or VPN. This would permit, for example, your ordering physician to remotely retrieve your radiographic images and report from the PACS in order to coordinate your medical care.
4.	How did unauthorized persons access patient information?	EBMRI's investigation revealed that an insecure port (or communication endpoint) used for internet access to the PACS server was used by unauthorized individuals to gain access to certain patient information. The root cause of the issue was a security protection weakness that has been resolved and the port is now secure. The virtual private network, or VPN, was not affected in the incident, and remained secure.

5.	What patient information was affected by the incident?	Fortunately, the types and amount of patient information affected by the incident were relatively small. The information accessible to unauthorized persons included **only** some or all of the following: radiology exam/study description and date and hour of exam, patient name, patient date of birth, patient ID (internally assigned by EBMRI and unrelated to any other patient information), radiology exam ID (assigned by radiology machine), ordering physician, and modality type. Based on EBMRI's investigation, the following information was **not** involved in this incident and remained secure: email or postal address; radiographic images, reports or medical records; Social Security number; any financial information such as credit card or bank information; and medical insurance card information.
6.	Was my medical record accessed by unauthorized individuals?	No. The amount and types of information accessible to unauthorized persons in this incident were small. EBMRI's investigation revealed that unauthorized individuals could **not** access radiographic images, radiographic reports or patient medical records, as such images, reports and records were within a secure system only accessible with authorized usernames and passwords.
7.	Were identifying or financial information accessed by unauthorized individuals?	EBMRI's investigation revealed that the only "identifying" information accessible to unauthorized individuals was patient name and date of birth. No Social Security numbers were involved in the incident. Although patient ID and radiology exam ID numbers were accessible, these are internally assigned numbers that would have no meaning to those outside EBMRI and are not connected to a person's identity. EBMRI's investigation also revealed that financial information, such as credit card numbers or financial account numbers, and medical insurance identification information, was **not** accessible by unauthorized persons.
8.	How long was this information potentially accessible to unauthorized individuals?	EBMRI's investigation revealed that the information was accessible to unauthorized individuals during the period between August 26, 2019 and February 23, 2021.

9.	Why did it take so long to discover the security incident?	Ownership of EBMRI changed hands in December 2020. After the change of ownership, EBMRI underwent a period of transition of management, personnel and processes. During this period, EBMRI learned that the federal Department of Health and Human Services had sent an inquiry to the prior owner of the imaging center whose PACS server was used by EBMRI regarding a potential security incident involving PACS servers and seeking information about whether the PACS server containing EBMRI patient information was at risk of or had been breached. Immediately upon EBMRI's discovery of a potential security breach, EBMRI undertook an investigation and mitigating actions.
10.	What is EBMRI doing to protect my electronic health information?	EBMRI takes seriously its responsibility to protect the privacy and security of patient information. As part of the transition of EBMRI's ownership and management, EBMRI reviewed the radiology center's electronic technology systems and security features. EBMRI replaced many systems and security features, and enhanced security protections at the center. In addition, EBMRI purchased a new PACS software and server to ensure the security of patient information stored and accessed through the PACS.
11.	Was any of my information misused?	EBMRI is unaware of any misuse of patient information as a result of this incident.
12.	Has any identity theft or fraud been reported as a result of this incident?	EBMRI is unaware of any reports of identity theft or fraud as a result of this incident.
13.	What can I do to better protect myself against identity theft and fraud?	Please see the "Identity Theft Protection Information" contained at the end of this Q&A document.
14.	Why am I not being offered credit monitoring services?	The types of information involved in this incident are not generally the types of information that can be easily used to steal someone's credit or identity. EBMRI's investigation revealed that none of the following information was accessible to unauthorized individuals: email or postal address; radiographic images, reports or medical records; Social Security number; any financial information such as credit card or bank information; and medical insurance card information.

15.	Have you notified law enforcement or other government officials?	EBMRI has not notified law enforcement of this security incident because the types of information involved in this incident are not generally the types of information that can be easily used to steal someone's credit or identity. EBMRI has notified the federal Department of Health and Human Services of this incident, as required by applicable law, and is working with department officials to comply with all of EBMRI's legal obligations.
16.	My spouse or dependent received a letter, but I did not. Am I impacted by this incident?	EBMRI mailed notification letters to all patients EBMRI was able to identify as potentially impacted by this incident.
17.	How do I obtain more information about this incident?	If you need further information about this incident, please send written correspondence to: East Brunswick Open Upright MRI 620 Cranbury Road Suite 10 East Brunswick, NJ 08816 Attention: Legal Department Or call toll-free: 1-833-804-6243

Identity Theft Protection Information

Nationwide Credit Reporting Agencies.

Equifax	**Experian**	**TransUnion**
Phone: 800-685-1111 P.O. Box 740256 Atlanta, GA 30348 www.equifax.com	Phone: 888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com	Phone: 888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. Be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You also may order an annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's (FTC) website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze: (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.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you immediately should contact the FTC and/or the Attorney General's office in your home state. You also may contact these agencies for information on how to prevent or avoid identity theft. You may contact the FTC, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/ 1-877-IDTHEFT (438-4338) (TTY: 866-653-4261). Information regarding state Attorneys General offices may be found through the National Association of Attorneys General, at: https://www.naag.org/find-my-ag/ or by telephone at 202-326-6000.

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

*****