NOTIFICATION OF POTENTIAL DATA BREACH

Hospital Español Auxilio Mutuo de Puerto Rico, Inc. is publishing this notice to inform you that our organization experienced a security incident.

Hospital Español Auxilio Mutuo de Puerto Rico, Inc. is publishing this notice to inform you that our organization experienced a data security incident in which your information may have been included, as described below. We take privacy and security seriously, so we are providing you with a notice about the incident, steps you can take to help protect your information, and the opportunity to enroll in free credit monitoring services.

What Happened: On September 23, 2023, the Department of Homeland Security informed Hospital Español Auxilio Mutuo de Puerto Rico, Inc. that our systems could be the target of a cyberattack. Immediately after receiving this notice, we initiated our incident response plan, retained legal counsel, and engaged outside information technology experts (through legal counsel) specializing in cyber incident response. On November 21, 2023, our initial investigation identified evidence consistent with unauthorized access to certain systems but was unable to determine the extent, if any, of any misuse or data exfiltration.

In an attempt to further determine the scope of the incident, we launched a second investigation, and on May 15, 2024, our preliminary findings identified unauthorized activity on our systems. Although ultimately inconclusive, a comprehensive review of the available evidence was conducted by internal and external IT experts on September 24, 2024, narrowing the potentially affected patients to those who visited our facilities between August 2022 and September 2023.

While we reiterate that there is no evidence at this time to affirmatively conclude that your personal and medical information was exfiltrated in this incident, out of an abundance of caution, we are providing you with this notice and the steps you can take to protect your personal information.

What information was affected: Potentially affected information includes your first and last name, combined with the following data elements:

- Health insurance information (such as primary, secondary, or other health plans/policies, insurance companies, member/group identification numbers, and government-Medicaid-Medicare payer identification numbers).
- Medical information (such as medical record numbers, providers, diagnoses, medications, test results, images, care and treatment).
- Billing, claims, and payment information (such as claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due). AND/OR
- Other personal information, such as Social Security numbers, driver's license or state ID numbers, or passport numbers.

What we're doing: Upon learning of the incident, we took immediate steps to secure our systems. We also engaged legal counsel and hired external forensic specialists to help determine the nature and scope of the incident. We have taken steps to strengthen our network systems to reduce the risk of a similar incident occurring in the future.

We also offer you the opportunity to enroll in Medical Shield Pro and **Equifax WebDefend** services at no cost to you. These services provide alerts for 12 months from the date of enrollment. These services will be provided by CyEx and Equifax, respectively; both companies specialize in fraud assistance and remediation services. Instructions on how to enroll in these services, along with additional resources available to you, are included in the attached document, " *Steps You Can Take to Protect Your Information* ."

What you can do: To date, we are not aware of any reports of identity fraud or misuse of your personal or medical information as a direct result of this incident. We also have no indication that your personal or medical information has been or is at risk of being misused. However, we encourage you to remain vigilant by reviewing your account statements and credit reports to detect suspicious activity and errors. If you discover any suspicious or unusual activity on your accounts, contact the financial institution or company immediately. Below we provide additional information about steps you can take to protect yourself against fraud and identity theft, as well as instructions for enrolling in credit monitoring.

For more information: If you have questions or concerns, please contact our dedicated helpline at 1-877-721-5315 between 9:00 a.m. and 9:00 p.m. EST, Monday through Friday. Please note that information security is of utmost importance to us. We remain committed to maintaining your trust and thank you for your support during this time.

Sincerely,
Jorge J. Vélez Gutiérrez
General Counsel
Hospital Español Auxilio Mutuo de Puerto Rico, Inc

Steps you can take to protect your information

Registration instructions

Medical Shield Pro
If you need help with the enrollment process or have questions about Medical Shield, please call Medical Shield directly at 866.622.9303.

Equifax WebDefend

Key Features

- Equifax WebDetect Internet scanning alerts you if your information is found on websites used by scammers.
- Equifax Social Scan searches social media sites and reports fraud risks from information you may be sharing.

If you currently have or have had any Equifax services in the past, you will not be able to register online.

Please contact Equifax Customer Care Monday to Friday, 9:00 am to 5:00 pm (GMT), at +44 (0)800 587 1584 or +442037885496 if you are calling from outside the UK.

Monitor your accounts and credit reports

We encourage you to be vigilant for identity theft and fraud by reviewing your account statements and credit reports, as well as your explanation of benefits forms, for suspicious activity and errors. Under U.S. law, you are entitled to one free annual credit report from each of the three major credit reporting bureaus: TransUnion, Experian, and Equifax. To request your free credit report, visit www.annualcreditreport.com or call toll-free 1-877-322-8228. After reviewing your credit report, check for discrepancies and try to identify accounts you didn't open or inquiries from lenders you didn't authorize. If you have questions or notice inaccurate information, contact the credit reporting bureau.

You have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert is a one-year alert placed on a consumer's credit file. Upon receiving a fraud alert, the business is required to take steps to verify the consumer's identity before granting new credit. If you are a victim of identity theft, you have the right to an extended fraud alert that lasts seven years. If you would like to place a fraud alert, please contact any of the three credit reporting bureaus listed below:

As an alternative to a fraud alert, you have the right to place a "credit freeze" on your credit report, which will prohibit a credit bureau from disclosing information in your credit report without your express authorization. A credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prevent the timely approval of a subsequent application or request you make regarding a new loan, credit, mortgage, or any other account related to the extension of credit. Under federal law, you cannot be charged for placing or removing a credit freeze on your credit report. To request a credit freeze, you must provide the following information:

1. Full name (including your middle initial, as well as Jr., Sr., III, etc.).
2. Social Security Number.
3. Birthdate.
4. Address for the previous two to five years.

5. Proof of current address, such as a current utility or telephone bill.
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.).
7. A copy of the police report, investigation report, or report to a law enforcement agency for identity theft, if you are a victim of such a crime.

If you want to place a fraud alert or credit freeze, contact the three credit reporting bureaus listed below:

T ransUnion
1-800-680-7289
www.transunion.com

T ransUnion Fraud Alert
P.O. Box 2000
Chester, PA 19016-2000

T ransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094

Experian
1-888-397-3742
www.experian.com

Experian Fraud Alert
P.O. Box 9554
Allen, TX 75013

Experian Credit Freeze
P.O. Box 9554
Allen, TX 75013

Equifax
1-888-298-0045
www.equifax.com

Equifax Fraud Alert
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788

Additional information

Para obtener más información acerca del robo de identidad, las alertas de fraude, el congelamiento de crédito y las medidas que puede tomar para proteger su información personal, comuníquese con las oficinas de informes crediticios, la Comisión Federal de Comercio (Federal Trade Commission, FTC) o con el fiscal general de su estado. La FTC también recomienda a aquellas personas que descubren que su información ha sido utilizada indebidamente que presenten un reclamo ante dicho organismo. Puede contactar a la FTC en 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338) y TTY: 1-866-653-4261. Tiene derecho a presentar una denuncia a la policía si alguna vez es víctima de fraude o robo de identidad. Recuerde que, para presentar una denuncia a la policía por robo de identidad, probablemente deberá proporcionar algún tipo de prueba que demuestre que ha sido víctima de tal delito. Las instancias de sospecha o certeza de robo de identidad también deben denunciarse a la policía, ante el fiscal general de su estado y a la FTC. Esta notificación no fue retrasada por la policía.

Para los residentes del Distrito de Columbia, pueden comunicarse con el Fiscal General del Distrito de Columbia en 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400 y https://oag.dc.gov/consumer-protection.

Para los residentes de Maryland, pueden comunicarse con el Fiscal General de Maryland en Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; o www.marylandattorneygeneral.gov.

Para residentes de Nuevo México, usted tiene ciertos derechos de acuerdo con la Ley de Información Crediticia Justa, como por ejemplo el derecho de obtener información si su expediente crediticio ha sido utilizado en su contra, el derecho de saber lo que contiene su expediente crediticio, el derecho de solicitar su calificación crediticia y el derecho de impugnar información incompleta o incorrecta. Además, en virtud de la Ley de Información Crediticia Justa: (i) las agencias de informes del consumidor deben corregir o eliminar toda información incorrecta, incompleta o no verificable; (ii) las agencias de informes del consumidor no pueden reportar información negativa desactualizada; (iii) el acceso a su expediente es limitado; (iv) usted debe otorgar consentimiento para proporcionar informes crediticios a sus empleadores; (v) usted puede limitar las ofertas de crédito y seguro "preautorizadas" que usted recibe con base en información en su informe crediticio; y (vi) usted puede reclamar daños y perjuicios de quienes violen sus derechos. Es posible que también tenga otros derechos en virtud de la Ley de Información Crediticia Justa, que no son mencionados en el presente documento. Las víctimas de robo de identidad y el personal militar en servicio activo cuentan con otros derechos específicos en virtud de la Ley de Información Crediticia Justa. Le recomendamos revisar sus derechos en virtud de la Ley de Información Crediticia Justa ingresando en https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, o por correo postal dirigido a Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.
For North Carolina residents , you can contact the North Carolina Attorney General at 9001 Mail Service Center, Raleigh, NC 27699-9001; by calling 1-877-566-7226 or 1-919-716-6000; and at www.ncdoj.gov .

For Oregon residents, you can contact the Oregon Attorney General at the Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096; 1-877-877-9392; and https://doj.state.or.us/consumer-protection/ .

For Rhode Island residents , you may contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903; by phone at 1-401-274-4400; and at www.riag.ri.gov . Under Rhode Island law, you have the right to obtain the police report filed regarding this incident.