

Feb. 8, 2019

Subject: Notice of Data Security Incident

On October 5, 2018, we notified affected individuals about a data security incident that involved a limited number of our patients' personal information. At Equitas Health, we take the privacy and security of our patients' personal information very seriously.

What happened? On August 8, 2018, Equitas Health became aware of unusual activity within an employee's email account. Equitas Health conducted an internal investigation that revealed that an unauthorized individual had access to two employees' email accounts.

What information was involved? The following information may have been involved: names, dates of birth, patient account and medical record numbers, prescription information, medical procedure information, physician names, diagnoses, treatment and clinical information, and health insurance information. For a limited number of individuals, Social Security numbers and driver's license numbers may also have been affected.

What are we doing? Upon discovery of the incident, Equitas Health immediately launched an internal investigation and reported the matter to appropriate authorities. We also retained an independent third party forensics firm to investigate the incident, and sought the advice of legal counsel and cybersecurity experts. Equitas Health has also added additional security features and taken other steps to minimize the chance that an event like this can occur in the future.

On October 5, 2018, we provided notification to those affected patients. We may not have been able to reach all affected individuals, so we are providing this notice on our website.

We are providing affected patients free identity monitoring services for 12 months at no cost through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

What can you do? If you believe you may have been impacted by this incident, would like further information or have any questions about this incident, or need additional assistance, please contact the dedicated call center at 1-866-775-4209, Monday through Friday from 9:00 a.m. to 6:30 p.m. EST.

We deeply regret any inconvenience or concern this may cause. Please do not hesitate to reach out to our designated call center if you have any questions.

Sincerely,

Trent Stechschulte
Compliance Officer & Legal Counsel

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.com

Free Annual Report

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC at the address below, or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

**North Carolina Attorney
General**

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

**Rhode Island
Attorney General**

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.