Billings Clinic

Notice of May, 2018 Data Security Incident

Billings Clinic is notifying patients affected by a data security incident. This incident did not include patient Social Security numbers, credit card numbers, banking information, insurance information or access to the Billings Clinic electronic medical record system. However, because Billings Clinic takes the privacy and security of our patients' information very seriously, we are notifying our patients about the incident and informing patients about steps that can be taken to protect their personal information.

What happened? On May 14, 2018, Billings Clinic became aware of unusual activity within one of our employee's email accounts. We immediately disabled access to the account, launched an investigation to determine what happened, and took action to further secure our email system. We also engaged a digital forensics firm to determine the nature and extent of the incident. As a result of the forensics investigation, we learned that an unauthorized individual had access to emails and attachments within that one account, some of which included patient information.

What information was involved? There was no unauthorized access to Billings Clinic's electronic medical record or financial systems, and there is no indication that any patient information has been misused. However, we are notifying patients that the following types of information were included in the email account: first initial or first name, last name, date of birth, contact information, medical record number, internal financial control number, diagnosis, and limited information about medical services received. Each patient had different types of information included in the emails, and no one email contained all of these types of information.

What are we doing? We are taking steps to limit the impact of this incident and to prevent similar incidents in the future. In addition to the steps referenced above, we have also reported this incident to the appropriate authorities, including the FBI. We are also providing affected patients with free identity monitoring services for 12 months through Experian.

What you can do: Suggestions on steps you can take to protect your information appear on the following page.

For more information: If you have questions or need assistance, please contact our offices at 406-657-4229, 8:00 a.m. to 5:00 p.m. (Mountain Time), Monday through Friday.

We are sorry for any inconvenience or concern this may cause. Please do not hesitate to reach out to us if you have any questions.

Sincerely,

Jeremy Lougee Compliance Officer

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	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	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: In some U.S. states, you have the right to put a security freeze on your credit file. 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. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. 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	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

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.