Billings Clinic

Notice of Data Security Incident

Billings Clinic is informing its patients of a data security incident that involved the personal information of a limited number of patients. We believe that this incident presents a minimal risk to those patients whose information was involved in this incident. However, because Billings Clinic takes the privacy and security of its patients very seriously, out of an abundance of caution, we are notifying and informing our patients about steps that can be taken to protect their personal information.

What happened? On February 26, 2018, Billings Clinic became aware of unusual activity within our email system. Billings Clinic immediately launched an investigation to determine what happened, disabled access to the accounts, and took action to further secure our email system. Billings Clinic 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 viewed a small number of emails whose text or attachments included limited personal information of some Billings Clinic patients.

What information was involved? The following information was involved: individuals' names, dates of birth, phone numbers and patient pharmacy balance. For a small number of patients, information that was potentially viewed included medical record numbers, internal billing numbers, medication names, and/or limited diagnosis and treatment information.

This incident did **not** include information such as Social Security numbers, credit card numbers, banking information or insurance information. There is no indication of any unauthorized access to medical records or financial systems.

What are we doing? Billings Clinic took the steps referenced above in response to the data security incident. We have also reported this incident to the authorities, including the FBI. We are also providing you the additional information below about steps you can take to protect your personal information.

What you can do: Even though there was no financial information involved in this incident, please see below for some suggestions on steps you can take to protect your information.

For more information: Further information about how to protect your personal information appears on the following page. 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 take the privacy and security of your information very seriously. We will continue to take steps to limit the impact of this incident and prevent similar incidents in the future. Please don't hesitate to reach out if you have any questions. We are sorry for any inconvenience or concern this may cause.

Sincerely,

Jeremy Lougee
Compliance Officer
Billings Clinic

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:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.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 three 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 or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

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 the right 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, and your

rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.