November 27, 2018
Membership Number: <<Member ID>>

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Su información personal puede haber estado involucrada en un posible incidente cibernético.
Si desea recibir una versión de esta carta en español, por favor llame 1-833-228-5726.

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to notify you of a cyber incident involving AccuDoc Solutions, Inc. ("AccuDoc"), a vendor that provides billing services for healthcare providers, including Atrium Health. This incident may have involved personal information provided in connection with payment for health services at an Atrium Health location (formerly Carolinas HealthCare System) and at locations managed by Atrium Health, including Blue Ridge HealthCare System, Columbus Regional Health Network, NHRMC Physician Group, Scotland Physicians Network, and St. Luke's Physician Network (collectively, our "Managed Locations").

What happened?

On October 1, 2018, AccuDoc informed Atrium Health that AccuDoc had been the victim of a cyber incident and that certain databases containing billing information belonging to Atrium Health and its Managed Locations may have been involved. Following an extensive review of AccuDoc's systems by multiple forensic experts, it appears that an unauthorized third party gained access to AccuDoc's databases between September 22, 2018 and September 29, 2018.

Please note that your information does not appear to have been taken from AccuDoc's systems and, to date, we are not aware of any misuse. We wanted, however, to let you know about the incident and provide you with additional information.

What information was involved?

Based on the review, the information involved may have included certain personal information about patients and guarantors (a person who is responsible for paying a patient's bill), including your first and last name, home address, date of birth, insurance policy information, medical record number, invoice number, account balance, and dates of service.

What information was NOT involved?

This incident did not involve access to your Social Security number, financial account numbers, or credit or debit card numbers. Additionally, your clinical information and medical records were not accessed, and Atrium Health's own systems and those of our Managed Locations were not affected by this incident at AccuDoc.

What did we do and what are we doing in response?

As soon as AccuDoc discovered the incident, it immediately terminated the unauthorized access, engaged a forensic investigator, and took steps to secure its affected databases and enhance its security controls. AccuDoc continues to monitor its systems for any additional related activity. Atrium Health takes this matter very seriously and engaged its own nationally-recognized forensic investigator to conduct an independent review of the incident. Atrium Health also reviewed its security safeguards and remains vigilant for similar types of incidents. Both AccuDoc and Atrium Health have been in contact with the Federal Bureau of Investigation (FBI).

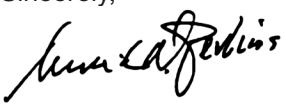
For more information

The enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. We encourage you to remain vigilant in monitoring your account statements, bills, notices, and insurance transactions for incidents of unauthorized activity, and to promptly report such incidents.

Questions

We sincerely regret this incident occurred regarding AccuDoc's databases, and we apologize for any inconvenience. If you have questions or would like additional information, please call toll-free 1-833-228-5726, Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time. You can also visit www.krollfraudsolutions.com/accudocincident for a list of frequently asked questions. Thank you.

Sincerely,



Kenneth Perkins, General Counsel
AccuDoc Solutions, Inc.

Alicia Bowers, Chief Privacy Officer
Atrium Health

REFERENCE GUIDE

Review Your Account Statements

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus (Equifax, Experian and TransUnion) provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Errors may be a warning sign of possible identity theft. If you see anything you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidence of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC. You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft/

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, you have the right to place a fraud alert on your credit file for one year at no cost. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the applicant's identity. You can place a fraud alert on your credit report by calling any of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax
P.O. Box 740241
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
800-680-7289
www.transunion.com

Security Freezes

You have the right to put a security freeze, also known as a credit freeze, on your credit file free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau by contacting the credit reporting agency by phone, mail, or secure electronic means and providing proper identification to verify your identity. 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.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
800-685-1111	888-397-3742	888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

Residents of North Carolina: As required by law, you may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.