# Notice of Data Security Incident

June 7, 2022

*Su información personal puede haber estado involucrada en un incidente de datos. Si desea recibir una version de esta carta en español, por favor llame 1-855-503-3418.*

Atrium Health at Home ("Atrium Health") discovered on April 8, 2022, that an unauthorized third party gained access to a home health employee's business email and messaging account through "phishing." Phishing occurs when an email is sent that looks like it is from a trustworthy source, but it is not. The phishing email misleads the recipient, resulting in them unknowingly sharing or providing access to certain information.

As soon as we discovered what happened, Atrium Health immediately took action to prevent any further unauthorized activity by securing the affected account and confirming the unauthorized third party had no further access. We also immediately began an investigation, notified law enforcement and engaged a leading security firm. Based on the investigation, it appears the unauthorized party had access to the affected account for a short time between April 7, 2022 and April 8, 2022. The behavior of the unauthorized party indicates they were likely focused on sending other phishing emails and not targeting medical or health information. Unfortunately, despite a thorough investigation, we could not conclusively determine whether personal information was actually accessed by the unauthorized party.

Depending upon the individual, personal information in the affected account may have included: full name, home address, date of birth, health insurance information and medical information (such as medical record number, dates of service, provider and facility and/or diagnosis and treatment information). For a limited subset of individuals, Social Security numbers, driver's license/state ID numbers and/or financial account information also may have been involved. Not all data fields may have been involved for all individuals. Our electronic medical record systems are separate from email accounts and <u>were not affected</u> by this incident.

Atrium Health takes privacy and security very seriously. As soon as we discovered the incident, we immediately took action to prevent any further unauthorized activity, including resetting the user password, confirming no further activity could occur, and notifying law enforcement. We have enhanced our security controls as appropriate and continue to evaluate measures to minimize the risk of any similar incident in the future. We also continue to provide regular, ongoing phishing training to our employees.

Atrium Health is providing additional information on general steps individuals can take to monitor and help protect their personal information in the below Reference Guide. Although we are unaware of any actual or attempted misuse of patient information as a result of this incident, individuals should carefully review credit reports and statements sent from providers, as well as their insurance company, to ensure that all account activity is valid. Any questionable charges should be promptly reported to the company which maintains the account.

Individuals potentially affected by this incident are being mailed notices. Since contact information may be insufficient for some individuals, this substitute notice is being posted and will remain active for at least 90 days. For those whose Social Security number, driver's license/state ID number and/or financial account information may have been involved, free credit monitoring and identity restoration services will be offered.

Atrium Health has established a dedicated assistance line for people who have questions or are seeking additional information regarding this matter. It is available toll-free at 1-855-503-3418 from 9:00 a.m. – 6:30 p.m. Eastern Time, Monday through Friday, except major US holidays.

Atrium Health is committed to protecting the privacy and security of personal information and deeply regrets any inconvenience and concern this incident may cause.

## REFERENCE GUIDE

### Review Your Account Statements

Carefully review statements sent to you from your healthcare providers, insurance company and financial institutions to ensure all of your account activity is valid. Report any questionable charges promptly to the company with which you maintain the account.

### 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 provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from which you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. 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 incidents 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, consider placing a fraud alert on your credit file. 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 identity of the applicant. You can place a fraud alert on your credit report by calling any one 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 105069<br>Atlanta, Georgia 30348 | 888-766-0008 | www.equifax.com |
| Experian | P.O. Box 9554<br>Allen, Texas 75013 | 888-397-3742 | www.experian.com |
| TransUnion | P.O. Box 2000<br>Chester, PA 19016 | 800-680-7289 | www.transunion.com |

## Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, 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. To place a security freeze on your credit report, you must contact the credit reporting agency by phone, mail or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her/them as well): (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 | P.O. Box 105788<br>Atlanta, GA 30348 | 800-685-1111 | www.equifax.com |
| Experian Security Freeze | P.O. Box 9554<br>Allen, TX 75013 | 888-397-3742 | www.experian.com |
| TransUnion | P.O. Box 160<br>Woodlyn, PA 19094 | 888-909-8872 | www.transunion.com |

Once you have submitted your request, the credit reporting agency must place the security freeze no later than one business day after receiving a request by phone or secure electronic means, and no later than three 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.

**For Residents of North Carolina**

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
1-919-716-6000
www.ncdoj.gov.