Jefferson Healthcare

January 11, 2021

Sent via email: SecurityBreach@atg.wa.gov

Office of the Washington State Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Re: Security Incident Notification

Dear Attorney General Ferguson:

This letter is to inform you of a recent data security incident involving information maintained by Jefferson Healthcare, a public hospital district in Port Townsend, Washington. This letter describes the incident, what Jefferson Healthcare's investigation has revealed so far about the information involved and potentially affected individuals, and the measures Jefferson Healthcare has taken in response to the incident.

On November 12, 2020, Jefferson Healthcare first discovered unauthorized access to an employee's email account by unidentified third parties who had obtained the employee's email login credentials through an email phishing attack. Upon learning of the incident, Jefferson Healthcare immediately took steps to halt the unauthorized access to the employee's email account and prevent further unauthorized access. These steps included temporarily suspending access to all systems for the affected employee, removing the affected computer from the network and engaging a forensics team to scrub the PC. Additional steps included requiring all employees to immediately change their email login passwords, requiring multi-factor authentication to log in when outside of the Jefferson Healthcare network, increasing cybersecurity training requirements for all employees, reminding employees to remain vigilant about phishing attacks, and increasing the number of sanctioned phishing attempts. Additional security enhancements are also underway, including a planned implementation of identity management and Single Sign-On as an added layer of authentication protection, as well as enhanced analytics to identify potential issues before they occur.

At the same time, Jefferson Healthcare also began an investigation to determine the nature and extent of the unauthorized access. This investigation determined that unauthorized access to the employee's email account began on November 9, 2020 and ended on November 12, 2020. Based on Jefferson Healthcare's investigation and security practices, we have no reason to believe that there was any unauthorized access to any other employee email accounts or to Jefferson Healthcare's electronic medical record system (which was protected by 2-factor-authentication at the time of the incident), billing systems, or other systems outside of the affected email account.

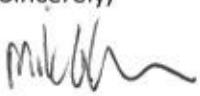
Based on the investigation, we reasonably believe that relatively few documents were likely actually viewed by the unauthorized parties during their access to the one affected email account. However, we could not definitively determine that the unauthorized parties did not access certain information and documents stored in the affected email account. We engaged outside forensic consultants to conduct a thorough review of information and documents in the email account. Following this detailed review and analysis, Jefferson Healthcare was able to determine that the email account contained the following types of information about patients of Jefferson Healthcare and other individuals: full names, dates of birth, phone numbers, home addresses, health insurance information, certain health information (such as dates of service, diagnosis and treatment information related to care received at Jefferson Healthcare), social security numbers, certain financial information, and certain online account information. The investigation determined that data stored in the affected email account included "personal information" as that term is defined by RCW 42.56.590.

Based on our investigation, we reasonably believe that approximately 2,543 individuals are potentially affected by the incident, of which approximately 2,496 individuals are Washington residents. In accordance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and implementing regulations, and in accordance with RCW 42.56.590, Jefferson Healthcare provided written notification of the data security incident to all affected individuals on January 11, 2020. This notification offered no-cost access to credit monitoring services for the limited number of individuals whose social security numbers were potentially exposed and provided contact information for a dedicated call center established for all affected individuals to contact with questions about the incident. Additionally, the notification provided guidance on how individuals can protect themselves against identity theft and fraud. Sample notification letters are enclosed with this letter. On January 11, 2020, Jefferson Healthcare also issued a press release about the incident to prominent print media outlets serving the geographic areas where affected individuals likely reside, posted a notice about the incident on its website, and provided notice to the U.S. Secretary of Health and Human Services.

Jefferson Healthcare has taken and will continue to take steps to prevent this type of incident from happening again, including implementing additional technology safeguards, requiring and providing additional training for staff members on preventing phishing attacks and securing login credentials, and other cybersecurity risk prevention measures. We have also reviewed our policies and procedures to ensure that they sufficiently protect against further incidents of this type.

We will update the information in this letter as necessary under RCW 42.56.590. For additional information, please contact Brandie Manuel, Chief Patient Safety & Quality Officer, at bmanuel@jeffersonhealthcare.org, or by calling (360) 385-2200 ext. 2002.

Sincerely,



Mike Glenn
Chief Executive Officer

Jefferson
Healthcare

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 11, 2021

G1123-L02-0000002 T00017 P003 *********ALL FOR AADC 123
SAMPLE A SAMPLE - L02 ADULT CM
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

RE: Important Security Notification. Please read this entire letter.

Dear Sample A Sample:

This letter is to inform you of a recent data security incident that may have involved your personal information maintained by Jefferson Healthcare. This letter describes the incident, outlines measures we have taken in response, and provides information regarding additional steps you can take to help protect your information.

What Happened?

On November 12, 2020, Jefferson Healthcare first discovered that an email phishing attack resulted in unauthorized access to an employee's email account by unidentified third parties, who were able to obtain the employee's email login credentials. Upon learning of the incident, Jefferson Healthcare immediately took steps to halt the unauthorized access to the employee's email account and prevent further unauthorized access, in addition to other mitigation and security measures. At the same time, Jefferson Healthcare began an investigation to determine the nature and extent of the unauthorized access.

What Information Was Involved?

Our investigation determined that unauthorized access to the employee's email account began on November 9, 2020, and we reasonably believe that relatively few documents were likely actually viewed by the unauthorized parties during their brief access to the email account. However, our investigation could not definitively conclude that the unauthorized parties did not access certain information and documents stored in the affected email account which may have included some of the following information: your full name, date of birth, phone number, home address, health insurance information, certain health information such as dates of service, diagnosis and treatment information, social security number, and certain financial information. Based on our investigation and security practices, we have no reason to believe that there has been any improper access to Jefferson Healthcare's electronic medical record system, billing systems, or other systems outside of the employee's email account.

What We Are Doing?

Jefferson Healthcare has taken and will continue to take steps to prevent this type of incident from happening again, including implementing additional technology safeguards, conducting additional training for staff members on preventing phishing attacks, securing login credentials, and other cybersecurity risk prevention measures. We have also reviewed our policies and procedures to ensure that they sufficiently protect against further incidents of this type.

What You Can Do.

Due to the nature of your information which may have been accessed by the third parties, Jefferson Healthcare has arranged for you to enroll in a credit monitoring service through Experian at no cost to you. Please see the Experian enrollment instructions attached to this letter. This service monitors the creation of a credit file in your name and includes identity theft insurance.

In addition, please review the enclosed *Information about Identity Theft Protection* section included with this letter. This section describes steps you can take to help protect your identity, including recommendations by the Federal Trade Commission regarding identify theft protection and details on how to place a fraud alert or a security freeze on your credit file if you wish to do so.

For More Information.

We sincerely regret any inconvenience or concern caused by this incident. We take our responsibility to protect the personal information of patients and other individuals very seriously, and we are committed to full transparency. If you have further questions or concerns, please call (877) 584-0360. Be prepared to provide engagement [redacted] for assistance.

Sincerely,

Mike Glenn

Mike Glenn, CEO
Jefferson Healthcare

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (877) 584-0360. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit

or call (877) 584-0360 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at (877) 584-0360.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions

Information about Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/
credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/
freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/
credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Jefferson
Healthcare

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 11, 2021

G1123-L06-0000006 T00017 P003 *********ALL FOR AADC 123
SAMPLE A SAMPLE - L06 ADULT, PII ONLY + CM
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

RE: Important Security Notification. Please read this entire letter.

Dear Sample A Sample:

This letter is to inform you of a recent data security incident that may have involved your personal information maintained by Jefferson Healthcare. This letter describes the incident, outlines measures we have taken in response, and provides information regarding additional steps you can take to help protect your information.

What Happened?

On November 12, 2020, Jefferson Healthcare first discovered that an email phishing attack resulted in unauthorized access to an employee's email account by unidentified third parties, who were able to obtain the employee's email login credentials. Upon learning of the incident, Jefferson Healthcare immediately took steps to halt the unauthorized access to the employee's email account and prevent further unauthorized access, in addition to other mitigation and security measures. At the same time, Jefferson Healthcare began an investigation to determine the nature and extent of the unauthorized access.

What Information Was Involved?

Our investigation determined that unauthorized access to the employee's email account began on November 9, 2020, and we reasonably believe that relatively few documents were likely actually viewed by the unauthorized parties during their brief access to the email account. However, our investigation could not definitively conclude that the unauthorized parties did not access certain information and documents stored in the affected email account which may have included some of the following information: your full name, date of birth, phone number, home address, driver's license number, account credentials, social security number, and certain financial information. Based on our investigation and security practices, we have no reason to believe that there has been any improper access to Jefferson Healthcare's electronic medical record system, billing systems, or other systems outside of the employee's email account.

What We Are Doing?

Jefferson Healthcare has taken and will continue to take steps to prevent this type of incident from happening again, including implementing additional technology safeguards, conducting additional training for staff members on preventing phishing attacks, securing login credentials, and other cybersecurity risk prevention measures. We have also reviewed our policies and procedures to ensure that they sufficiently protect against further incidents of this type.

What You Can Do.

Due to the nature of your information which may have been accessed by the third parties, Jefferson Healthcare has arranged for you to enroll in a credit monitoring service through Experian at no cost to you. Please see the Experian enrollment instructions attached to this letter. This service monitors the creation of a credit file in your name and includes identity theft insurance.

In addition, please review the enclosed *Information about Identity Theft Protection* section included with this letter. This section describes steps you can take to help protect your identity, including recommendations by the Federal Trade Commission regarding identify theft protection and details on how to place a fraud alert or a security freeze on your credit file if you wish to do so.

For More Information.

We sincerely regret any inconvenience or concern caused by this incident. We take our responsibility to protect the personal information of patients and other individuals very seriously, and we are committed to full transparency. If you have further questions or concerns, please call (877) 584-0360. Be prepared to provide engagement [redacted] for assistance.

Sincerely,

Mike Glenn

Mike Glenn, CEO
Jefferson Healthcare

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (877) 584-0360. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit

or call (877) 584-0360 to register with the activation code above

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at (877) 584-0360.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Information about Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/
credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/
freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/
credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Jefferson
Healthcare

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 11, 2021

G1123-L08-0000008 T00017 P003 *********ALL FOR AADC 123
SAMPLE A SAMPLE - L08 MINOR PII ONLY
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

RE: Important Security Notification. Please read this entire letter.

Dear Parent/Guardian of Sample A Sample:

This letter is to inform you of a recent data security incident that may have involved your child's personal information maintained by Jefferson Healthcare. This letter describes the incident, outlines measures we have taken in response, and provides information regarding additional steps you can take to help protect your child's information.

What Happened?

On November 12, 2020, Jefferson Healthcare first discovered that an email phishing attack resulted in unauthorized access to an employee's email account by unidentified third parties, who were able to obtain the employee's email login credentials. Upon learning of the incident, Jefferson Healthcare immediately took steps to halt the unauthorized access to the employee's email account and prevent further unauthorized access, in addition to other mitigation and security measures. At the same time, Jefferson Healthcare began an investigation to determine the nature and extent of the unauthorized access.

What Information Was Involved?

Our investigation determined that unauthorized access to the employee's email account began on November 9, 2020, and we reasonably believe that relatively few documents were likely actually viewed by the unauthorized parties during their brief access to the email account. However, our investigation could not definitively conclude that the unauthorized parties did not access certain information and documents stored in the affected email account which may have included some of the following information: your child's full name, date of birth, phone number, home address, driver's license number, and account credentials. Please be assured that your child's social security number and financial information were not stored in the email account and therefore were not involved in this incident. Further, based on our investigation and security practices, we have no reason to believe that there has been any improper access to Jefferson Healthcare's electronic medical record system, billing systems, or other systems outside of the employee's email account.

What We Are Doing?

Jefferson Healthcare has taken and will continue to take steps to prevent this type of incident from happening again, including implementing additional technology safeguards, conducting additional training for staff members on preventing phishing attacks, securing login credentials, and other cybersecurity risk prevention measures. We have also reviewed our policies and procedures to ensure that they sufficiently protect against further incidents of this type.

What You Can Do.

Please review the enclosed *Information about Identity Theft Protection* section included with this letter. This section describes steps you can take to help protect your child's identity, including recommendations by the Federal Trade Commission regarding identify theft protection and details on how to place a fraud alert or a security freeze on your child's credit file if you wish to do so.

For More Information.

We sincerely regret any inconvenience or concern caused by this incident. We take our responsibility to protect the personal information of patients and other individuals very seriously, and we are committed to full transparency. If you have further questions or concerns, please call (877) 584-0360. Be prepared to provide engagement [redacted] for assistance.

Sincerely,

Mike Glenn

Mike Glenn, CEO
Jefferson Healthcare

Information about Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/
credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/
freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/
credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Jefferson
Healthcare

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 11, 2021

G1123-L07-0000007 T00017 P003 *********ALL FOR AADC 123
SAMPLE A SAMPLE - L07 DECEASED ADULT PII ONLY
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

RE: Important Security Notification. Please read this entire letter.

Dear Family of Sample A Sample:

This letter is to inform you of a recent data security incident that may have involved your family member's personal information maintained by Jefferson Healthcare. This letter describes the incident, outlines measures we have taken in response, and provides information regarding additional steps you can take to help protect your family member's information.

What Happened?

On November 12, 2020, Jefferson Healthcare first discovered that an email phishing attack resulted in unauthorized access to an employee's email account by unidentified third parties, who were able to obtain the employee's email login credentials. Upon learning of the incident, Jefferson Healthcare immediately took steps to halt the unauthorized access to the employee's email account and prevent further unauthorized access, in addition to other mitigation and security measures. At the same time, Jefferson Healthcare began an investigation to determine the nature and extent of the unauthorized access.

What Information Was Involved?

Our investigation determined that unauthorized access to the employee's email account began on November 9, 2020, and we reasonably believe that relatively few documents were likely actually viewed by the unauthorized parties during their brief access to the email account. However, our investigation could not definitively conclude that the unauthorized parties did not access certain information and documents stored in the affected email account which may have included some of the following information: your family member's full name, date of birth, phone number, home address, driver's license number, and account credentials. Please be assured that your family member's social security number and financial information were not stored in the email account and therefore were not involved in this incident. Further, based on our investigation and security practices, we have no reason to believe that there has been any improper access to Jefferson Healthcare's electronic medical record system, billing systems, or other systems outside of the employee's email account.

What We Are Doing?

Jefferson Healthcare has taken and will continue to take steps to prevent this type of incident from happening again, including implementing additional technology safeguards, conducting additional training for staff members on preventing phishing attacks, securing login credentials, and other cybersecurity risk prevention measures. We have also reviewed our policies and procedures to ensure that they sufficiently protect against further incidents of this type.

What You Can Do.

Please review the enclosed *Information about Identity Theft Protection* section included with this letter. This section describes steps you can take to help protect your family member's identity, including recommendations by the Federal Trade Commission regarding identify theft protection and details on how to place a fraud alert or a security freeze on your family member's credit file if you wish to do so.

For More Information.

We sincerely regret any inconvenience or concern caused by this incident. We take our responsibility to protect the personal information of patients and other individuals very seriously, and we are committed to full transparency. If you have further questions or concerns, please call (877) 584-0360. Be prepared to provide engagement [redacted] for assistance.

Sincerely,

Mike Glenn

Mike Glenn, CEO
Jefferson Healthcare

Information about Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/
credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/
freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/
credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Jefferson
Healthcare

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 11, 2021

G1123-L01-0000001 T00017 P003 *********ALL FOR AADC 123
SAMPLE A SAMPLE - L01 ADULT FINAL
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

RE: Important Security Notification. Please read this entire letter.

Dear Sample A Sample:

This letter is to inform you of a recent data security incident that may have involved your personal information maintained by Jefferson Healthcare. This letter describes the incident, outlines measures we have taken in response, and provides information regarding additional steps you can take to help protect your information.

What Happened?

On November 12, 2020, Jefferson Healthcare first discovered that an email phishing attack resulted in unauthorized access to an employee's email account by unidentified third parties, who were able to obtain the employee's email login credentials. Upon learning of the incident, Jefferson Healthcare immediately took steps to halt the unauthorized access to the employee's email account and prevent further unauthorized access, in addition to other mitigation and security measures. At the same time, Jefferson Healthcare began an investigation to determine the nature and extent of the unauthorized access.

What Information Was Involved?

Our investigation determined that unauthorized access to the employee's email account began on November 9, 2020, and we reasonably believe that relatively few documents were likely actually viewed by the unauthorized parties during their brief access to the email account. However, our investigation could not definitively conclude that the unauthorized parties did not access certain information and documents stored in the affected email account which may have included some of the following information: your full name, date of birth, phone number, home address, health insurance information, and certain health information such as dates of service, diagnosis and treatment information related to care received at Jefferson Healthcare. Please be assured that your social security number and financial information were not stored in the email account and therefore were not involved in this incident. Further, based on our investigation and security practices, we have no reason to believe that there has been any improper access to Jefferson Healthcare's electronic medical record system, billing systems, or other systems outside of the employee's email account.

What We Are Doing?

Jefferson Healthcare has taken and will continue to take steps to prevent this type of incident from happening again, including implementing additional technology safeguards, conducting additional training for staff members on preventing phishing attacks, securing login credentials, and other cybersecurity risk prevention measures. We have also reviewed our policies and procedures to ensure that they sufficiently protect against further incidents of this type.

What You Can Do.

Please review the enclosed *Information about Identity Theft Protection* section included with this letter. This section describes steps you can take to help protect your identity, including recommendations by the Federal Trade Commission regarding identify theft protection and details on how to place a fraud alert or a security freeze on your credit file if you wish to do so.

For More Information.

We sincerely regret any inconvenience or concern caused by this incident. We take our responsibility to protect the personal information of patients and other individuals very seriously, and we are committed to full transparency. If you have further questions or concerns, please call (877) 584-0360. Be prepared to provide engagement [redacted] for assistance.

Sincerely,

Mike Glenn

Mike Glenn, CEO
Jefferson Healthcare

Information about Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/
credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/
freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/
credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Jefferson
Healthcare
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 11, 2021

G1123-L04-0000004 T00017 P003 *********ALL FOR AADC 123
SAMPLE A SAMPLE - L04 DECEASED ADULT
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

RE: Important Security Notification. Please read this entire letter.

Dear Family of Sample A Sample:

This letter is to inform you of a recent data security incident that may have involved your family member's personal information maintained by Jefferson Healthcare. This letter describes the incident, outlines measures we have taken in response, and provides information regarding additional steps you can take to help protect your family member's information.

What Happened?

On November 12, 2020, Jefferson Healthcare first discovered that an email phishing attack resulted in unauthorized access to an employee's email account by unidentified third parties, who were able to obtain the employee's email login credentials. Upon learning of the incident, Jefferson Healthcare immediately took steps to halt the unauthorized access to the employee's email account and prevent further unauthorized access, in addition to other mitigation and security measures. At the same time, Jefferson Healthcare began an investigation to determine the nature and extent of the unauthorized access.

What Information Was Involved?

Our investigation determined that unauthorized access to the employee's email account began on November 9, 2020, and we reasonably believe that relatively few documents were likely actually viewed by the unauthorized parties during their brief access to the email account. However, our investigation could not definitively conclude that the unauthorized parties did not access certain information and documents stored in the affected email account which may have included some of the following information: your family member's full name, date of birth, phone number, home address, health insurance information, and certain health information such as dates of service, diagnosis and treatment information related to care received at Jefferson Healthcare. Please be assured that your family member's social security number and financial information were not stored in the email account and therefore were not involved in this incident. Further, based on our investigation and security practices, we have no reason to believe that there has been any improper access to Jefferson Healthcare's electronic medical record system, billing systems, or other systems outside of the employee's email account.

What We Are Doing?

Jefferson Healthcare has taken and will continue to take steps to prevent this type of incident from happening again, including implementing additional technology safeguards, conducting additional training for staff members on preventing phishing attacks, securing login credentials, and other cybersecurity risk prevention measures. We have also reviewed our policies and procedures to ensure that they sufficiently protect against further incidents of this type.

What You Can Do.

Please review the enclosed *Information about Identity Theft Protection* section included with this letter. This section describes steps you can take to help protect your family member's identity, including recommendations by the Federal Trade Commission regarding identify theft protection and details on how to place a fraud alert or a security freeze on your family member's credit file if you wish to do so.

For More Information.

We sincerely regret any inconvenience or concern caused by this incident. We take our responsibility to protect the personal information of patients and other individuals very seriously, and we are committed to full transparency. If you have further questions or concerns, please call (877) 584-0360. Be prepared to provide engagement [redacted] for assistance.

Sincerely,

Mike Glenn

Mike Glenn, CEO
Jefferson Healthcare

Information about Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/
credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/
freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/
credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Jefferson
Healthcare

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 11, 2021

G1123-L03-0000003 T00017 P003 *********ALL FOR AADC 123
SAMPLE A SAMPLE - L03 MINOR
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

RE: Important Security Notification. Please read this entire letter.

Dear Parent/Guardian of Sample A Sample:

This letter is to inform you of a recent data security incident that may have involved your child's personal information maintained by Jefferson Healthcare. This letter describes the incident, outlines measures we have taken in response, and provides information regarding additional steps you can take to help protect your child's information.

What Happened?

On November 12, 2020, Jefferson Healthcare first discovered that an email phishing attack resulted in unauthorized access to an employee's email account by unidentified third parties, who were able to obtain the employee's email login credentials. Upon learning of the incident, Jefferson Healthcare immediately took steps to halt the unauthorized access to the employee's email account and prevent further unauthorized access, in addition to other mitigation and security measures. At the same time, Jefferson Healthcare began an investigation to determine the nature and extent of the unauthorized access.

What Information Was Involved?

Our investigation determined that unauthorized access to the employee's email account began on November 9, 2020, and we reasonably believe that relatively few documents were likely actually viewed by the unauthorized parties during their brief access to the email account. However, our investigation could not definitively conclude that the unauthorized parties did not access certain information and documents stored in the affected email account which may have included some of the following information: your child's full name, date of birth, phone number, home address, health insurance information, and certain health information such as dates of service, diagnosis and treatment information related to care received at Jefferson Healthcare. Please be assured that your child's social security number and financial information were not stored in the email account and therefore were not involved in this incident. Further, based on our investigation and security practices, we have no reason to believe that there has been any improper access to Jefferson Healthcare's electronic medical record system, billing systems, or other systems outside of the employee's email account.

What We Are Doing?

Jefferson Healthcare has taken and will continue to take steps to prevent this type of incident from happening again, including implementing additional technology safeguards, conducting additional training for staff members on preventing phishing attacks, securing login credentials, and other cybersecurity risk prevention measures. We have also reviewed our policies and procedures to ensure that they sufficiently protect against further incidents of this type.

What You Can Do.

Please review the enclosed *Information about Identity Theft Protection* section included with this letter. This section describes steps you can take to help protect your child's identity, including recommendations by the Federal Trade Commission regarding identify theft protection and details on how to place a fraud alert or a security freeze on your child's credit file if you wish to do so.

For More Information.

We sincerely regret any inconvenience or concern caused by this incident. We take our responsibility to protect the personal information of patients and other individuals very seriously, and we are committed to full transparency. If you have further questions or concerns, please call (877) 584-0360. Be prepared to provide engagement [redacted] for assistance.

Sincerely,

Mike Glenn

Mike Glenn, CEO
Jefferson Healthcare

Information about Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/
credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/
freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/
credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Jefferson
Healthcare
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 11, 2021

G1123-L05-0000005 T00017 P003 *********ALL FOR AADC 123
SAMPLE A SAMPLE - L05 ADULT PII ONLY
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

RE: Important Security Notification. Please read this entire letter.

Dear Sample A Sample:

This letter is to inform you of a recent data security incident that may have involved your personal information maintained by Jefferson Healthcare. This letter describes the incident, outlines measures we have taken in response, and provides information regarding additional steps you can take to help protect your information.

What Happened?

On November 12, 2020, Jefferson Healthcare first discovered that an email phishing attack resulted in unauthorized access to an employee's email account by unidentified third parties, who were able to obtain the employee's email login credentials. Upon learning of the incident, Jefferson Healthcare immediately took steps to halt the unauthorized access to the employee's email account and prevent further unauthorized access, in addition to other mitigation and security measures. At the same time, Jefferson Healthcare began an investigation to determine the nature and extent of the unauthorized access.

What Information Was Involved?

Our investigation determined that unauthorized access to the employee's email account began on November 9, 2020, and we reasonably believe that relatively few documents were likely actually viewed by the unauthorized parties during their brief access to the email account. However, our investigation could not definitively conclude that the unauthorized parties did not access certain information and documents stored in the affected email account which may have included some of the following information: your full name, date of birth, phone number, home address, driver's license number, and account credentials. Please be assured that your social security number and financial information were not stored in the email account and therefore were not involved in this incident. Further, based on our investigation and security practices, we have no reason to believe that there has been any improper access to Jefferson Healthcare's electronic medical record system, billing systems, or other systems outside of the employee's email account.

What We Are Doing?

Jefferson Healthcare has taken and will continue to take steps to prevent this type of incident from happening again, including implementing additional technology safeguards, conducting additional training for staff members on preventing phishing attacks, securing login credentials, and other cybersecurity risk prevention measures. We have also reviewed our policies and procedures to ensure that they sufficiently protect against further incidents of this type.

What You Can Do.

Please review the enclosed *Information about Identity Theft Protection* section included with this letter. This section describes steps you can take to help protect your identity, including recommendations by the Federal Trade Commission regarding identify theft protection and details on how to place a fraud alert or a security freeze on your credit file if you wish to do so.

For More Information.

We sincerely regret any inconvenience or concern caused by this incident. We take our responsibility to protect the personal information of patients and other individuals very seriously, and we are committed to full transparency. If you have further questions or concerns, please call (877) 584-0360. Be prepared to provide engagement [redacted] for assistance.

Sincerely,

Mike Glenn

Mike Glenn, CEO
Jefferson Healthcare

Information about Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/
credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/
freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/
credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft