

Nesrin G. Tift
ntift@bassberry.com
(615) 742-7861

October 14, 2022

By Email: idtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Dear Mr. Karberg,

Pursuant to Md. Code Ann. Com. Law § 14-3504, HH/Killeen Health System, LLC d/b/a Seton Medical Center Harker Heights (“SMCHH”) is sending you this letter to notify you of a potential unauthorized access or use of personal information affecting two (2) Maryland residents.

Nature of the Breach

SMCHH is an acute care hospital located in Harker Heights, Texas. SMCHH contracts with a vendor to provide hospital reimbursement consulting services. On August 19, 2022, SMCHH was informed by the vendor that, due to a phishing incident, an unauthorized agent gained access to the email accounts of two (2) vendor employees; as a result, this unauthorized agent may have accessed the protected health information of SMCHH patients. The unauthorized activity occurred on the vendor’s information system only. It did not occur on SMCHH’s information system or affect SMCHH’s electronic medical records. The unauthorized activity took place on or around November 5, 2021.

Information Potentially Compromised

The incident involved possible access to SMCHH patients’ first and last names, dates of birth, medical record numbers, and/or certain clinical information. The breach did **not** involve addresses, social security numbers, or any financial or credit card information.

Steps Taken Following Breach

The vendor responded to the incident by immediately changing the passwords of affected email accounts. Moreover, to restore the integrity of its information system, the vendor conducted thorough investigations—both internal and through a third-party digital forensics company—to determine the nature and scope of the incident. Ultimately, the vendor concluded that it had no reason to believe that any misuse of personal information occurred.

Number of Maryland Residents Potentially Affected

Based on the aforementioned investigations and pursuant to Md. Code Ann. Com. Law § 14-3504, it was determined that two (2) Maryland residents were affected.

Notice Provided to Affected Individuals

SMCHH is notifying affected Maryland patients by mail pursuant to Md. Code Ann. Com. Law § 14-3504.

Services Being Offered to Affected Individuals Without Charge

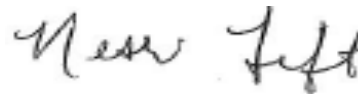
The notification letter encourages individuals to take precautions to protect the security of their personal information and also recommends that individuals remain vigilant to prevent identity theft and fraud by monitoring credit reports and financial institution and other account statements. The letter includes a Security Reference Guide that outlines other steps individuals should consider to lessen the risk of identity theft and a toll-free telephone number for individuals to call with any questions about the incident.

As an added precaution, SMCHH is offering a twelve (12) month membership to a credit monitoring service at no cost to affected patients. This product provides individuals with identity protection and resolution of identity theft. The notification letter provides information on how to enroll in the credit monitoring service.

Contact Information for SMCHH's Agent

For any questions or additional information regarding this incident, please contact Nesrin Tift at Bass, Berry & Sims PLC, by mail at 150 Third Avenue South, Suite 2800, Nashville, Tennessee 37201; by email at ntift@bassberry.com; or by telephone at (615) 742-6200.

Sincerely,

A handwritten signature in dark ink, appearing to read "Nesrin Tift", written in a cursive style.

Nesrin G. Tift

Enclosures: Attachment A (Sample Individual Notification Letter)



Seton Medical Center Harker Heights

A partner of the Seton Healthcare Family

Return Mail Processing
PO Box 999
Suwanee, GA 30024

October 14, 2022

60115048 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



Dear Sample A. Sample,

At Seton Medical Center Harker Heights (“SMCHH”), we take very seriously the privacy and security of your health information. I am writing to inform you of a recent incident experienced by one of our service providers. Please read this entire letter carefully.

SMCHH contracts with a vendor for hospital reimbursement services. On August 19, 2022, SMCHH was informed by this vendor that, as the result of a phishing incident, an unauthorized agent gained access to the email accounts of two (2) of its employees and may have accessed the protected health information of SMCHH patients. The unauthorized activity took place on or around November 5, 2021.

The vendor reported to SMCHH that it has taken the following steps in response to the incident:

- Changed passwords of the affected email accounts immediately upon becoming aware of the unauthorized access;
- Conducted an internal investigation into the incident and its scope;
- Engaged a digital forensics firm to review and determine the scope of unauthorized access; and
- Thoroughly reviewed the affected email accounts to determine what protected health information, if any, may have been exposed.

Based on its review, the vendor determined that an unauthorized agent could have accessed or viewed the following: your first and last name, date of birth, medical record number, and/or certain clinical information. The information **did not contain your address, social security number or any financial or credit card information.**

The vendor has no indication that any protected health information has been misused. Regardless, we encourage you to take precautions to protect the security of your information. We recommend that you remain vigilant to prevent identity theft and fraud by monitoring your credit reports and financial institution and other account statements. We also advise that you promptly report any suspicious activity or suspected identity theft to law enforcement or your state’s attorney general. In addition, under the federal Fair Credit Reporting Act, you have the right as a consumer to place fraud alerts on credit reports and to alert potential creditors or lenders of potential fraudulent activity related to the use of your personal information. You may do so by contacting credit reporting agencies. The enclosed Security Reference Guide provides contact information for the three major credit reporting agencies and the toll-free number, website and address for the Federal Trade Commission (“FTC”).

As an additional precaution, to reduce the risk of fraud or identity theft, SMCHH is offering you a [twelve (12)/twenty-four (24)] month membership in Experian’s® IdentityWorksSM at no cost to you. This product provides you with superior identity protection and resolution of identity theft. We have provided you with the enrollment instructions in the attached Security Reference Guide.

This breach only affected the vendor's separately-maintained information system. It did not occur on an SMCHH-maintained information system and **did not** affect SMCHH's electronic medical records. However, we deeply regret this situation and any inconvenience this may cause you. If you have questions about this incident or the IdentityWorks 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 (888) 401-0572.

Sincerely,

A handwritten signature in black ink, appearing to read "Patrick Swindle". The signature is fluid and cursive, with the first name "Patrick" and last name "Swindle" clearly distinguishable.

Patrick Swindle
Chief Executive Officer

Security Reference Guide

How to Enroll in the Experian IdentityWorksSM Product

As stated in the attached letter, we are offering you a [twelve (12)/twenty-four (24)] month membership in Experian IdentityWorksSM at no cost to you.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary [twelve (12)/twenty-four (24)] month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by January 31, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website: <https://www.experianidworks.com/credit>
- Provide your **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 **(888) 401-0572** before **January 31, 2023**. Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [12/24]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

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

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** 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.

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

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Steps You Can Take to Protect the Security of Your Information:

- Place a “fraud alert” on your credit file. An initial 90 day alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax

1-800-525-6285
PO Box 105069
Atlanta, GA 30348
www.equifax.com

Experian

1-888-397-3742
PO Box 9701
Allen, TX 75013
www.experian.com

TransUnion

1-800-680-7289 (fraud alert)
1-800-888-4213 (credit report)
PO Box 2000
Chester, PA 19022
www.transunion.com

- Place a “credit freeze” on your credit file. A credit freeze prevents your credit from being shared with potential creditors or insurance companies. To place a credit freeze on your credit file, contact each of the three major credit reporting agencies - Equifax, Experian and TransUnion. Each credit reporting agency may charge a small fee to place a credit freeze.
- Review and monitor your credit report for any new developments. You can order a copy of your credit report on the internet at www.annualcreditreport.com or by calling the Annual Credit Report Request Service toll-free at 1-877-322-8228.
- Review your credit card, bank and other account statements promptly and regularly for any unauthorized activity.
- If you find suspicious activity on your credit reports or account statements, or have reason to believe that your personal information is being misused, contact your local law enforcement authorities immediately and file a police report. You have the right to request a copy of the police report and should retain it for further use, as many creditors want the information it contains to absolve you of potential fraudulent debts.
- If you become aware of possible identity theft, report it to your state Attorney General and the Federal Trade Commission (“FTC”). You can contact the FTC to learn more about how to protect yourself from identity theft, how to place a fraud alert on your credit report and how to place a security freeze on your credit report:
 - Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/
- If you are a North Carolina resident, you can obtain information from the North Carolina Attorney General’s Office about preventing identity theft. You can contact the North Carolina Attorney General at:
 - North Carolina Attorney General’s Office
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (toll-free in North Carolina)
919-716-6400
www.ncdoj.gov

- If you are a Maryland resident, you can obtain information from the Maryland Attorney General's Office about steps you can take to prevent identity theft. You can contact the Attorney General at:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023 (toll-free)
410-576-6300
www.marylandattorneygeneral.gov

