POLSINELLI

150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

February 6, 2025

Bruce Radke
312-463-6212
bradke@polsinelli.com

VIA E-MAIL (SECURITYBREACH@ATG.WA.GOV)
WA State Office of the Attorney General
800 Fifth Avenue
Suite 2000
Seattle, WA 98104

Re: ***Notification of Data Security Incident***

Dear Madam/Sir:

We represent Hospital Sisters Health System ("HSHS"), 4936 LaVerna Road, Springfield, Illinois 62579, in connection with an incident that involved the personal information of six hundred and sixty-two (662) Washington residents. HSHS does not waive any rights or defenses relating to the incident, this notice, or the applicability of Washington law on personal jurisdiction.

NATURE OF THE INCIDENT

On August 27, 2023, Hospital Sisters Health System (HSHS) discovered an unauthorized third party gained temporary access to HSHS's network. Upon learning of the situation, HSHS immediately took steps to contain and remediate the incident and launched an internal investigation. HSHS also reported the incident to law enforcement and engaged a leading forensic security firm to assist in the investigation and confirm the security of the HSHS computer systems and network. The forensic investigation determined that the unauthorized third party accessed certain files on the HSHS network between August 16 and August 27, 2023. HSHS has since been reviewing those files and notifying individuals whose information was found in the files on a rolling basis as the review has continued. HSHS recently concluded the comprehensive review of the involved files and is notifying the additional individuals whose personal information was identified in the remaining files. HSHS is providing notice of the incident to the Washington Attorney General since the number of Washington residents has now surpassed the numerical threshold for such notification.

NOTICE TO WASHINGTON RESIDENTS

HSHS has notified six hundred and sixty-two (662) residents of Washington whose personal information was contained in the files involved in the incident. These notifications have been made via letters mailed by USPS First Class Mail starting on August 30, 2024 and completed on February 7, 2025. The notification letters describe the incident and provide information on ways the individuals can protect themselves against potential fraud and identity theft and include an offer of complimentary credit monitoring and identity theft protection services for those individuals whose Social Security number was included. HSHS has also arranged for a toll-free, dedicated call line to assist the notified individuals with any questions they may have regarding the incident. Enclosed is a sample of the letter.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, HSHS began an internal investigation. As mentioned, HSHS is notifying employees and patients whose information was contained in the files and is offering complimentary credit monitoring and identity theft protection services.

CONTACT INFORMATION

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Bruce Radke

Enclosure

Hospital Sisters HEALTH SYSTEM

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Dear <<Name1>>:

Hospital Sisters Health System (HSHS) cares deeply about our patients, and that is why we are writing to advise you of an incident that may have involved some of your personal information. This letter tells you what happened, what information was potentially accessed, what HSHS is doing in response to the incident, and provides guidance on what you can do to protect yourself, should you feel it is important to do so.

What Happened? On August 27, 2023, HSHS discovered an unauthorized third party gained temporary access to HSHS's network. Upon learning of the situation, we immediately took steps to contain and remediate the incident and launched an internal investigation. We also reported the incident to law enforcement and engaged a leading forensic security firm to assist in our investigation and confirm the security of our computer systems and network. The forensic investigation determined that the unauthorized third party accessed certain files on our network between August 16 and August 27, 2023. We have since been reviewing those files and notifying individuals whose information was found in the files on a rolling basis as our review has continued.

What Information Was Involved? The type of information varied for each individual, but may have included your name, address, date of birth, medical record number, limited treatment information, health insurance information and Social Security number and/or driver's license number. At this time, we have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft.

What We Are Doing. In addition to the actions described above, we have taken steps to reduce the risk of this type of incident from occurring in the future, including enhancing our technical security measures. Although we are not aware of any instances of fraud or identity theft resulting from this incident, out of an abundance of caution, we are offering a free one-year membership of **Equifax Credit Watch™ Gold.** This service helps detect possible misuse of your personal information and provides you with identity protection services including immediate identification and resolution of identity theft. **Equifax Credit Watch™ Gold** is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and Equifax Credit Watch™ Gold, including instructions on how to activate your complimentary, one-year membership, please see the additional information attached to this letter.**

What You Can Do. Again, while we have no evidence that your personal information has been misused, we encourage you to take advantage of the complimentary credit monitoring offer included in this letter. You can learn about more steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* page.

For More Information. We value the trust you place in us to protect the privacy and security of your information and deeply regret any inconvenience or concern this incident might cause. For further information and assistance, please call [redacted] from 8:00 am - 8:00 pm Central, Monday through Friday, except major U.S. holidays.

Sincerely,

HSHS Privacy Department

Enter your Activation Code: **<<Activation Code>>**
Enrollment Deadline: **<<Enrollment Deadline>>**

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to **www.equifax.com/activate**
Enter your unique Activation Code of **<<Activation Code>>** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and 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 get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Iowa Residents: Iowa residents can contact the Office of the Attorney General to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's Office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/. HSHS' main address and telephone number are 4936 Laverna Road Springfield, Illinois and 217-523-4747.

New Mexico: Individuals have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Oregon Residents: Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 503-378-4400; https://www.doj.state.or.us/.

Rhode Island Residents: We believe that this incident affected 17 Rhode Island residents. Rhode Island residents can contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).