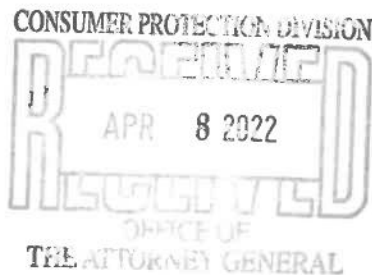




Jason M. Schwent
T (312) 985-5939
Email:jschwent@ClarkHill.com



Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

March 31, 2022

Sent via USPS

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

We represent South Shore Hospital Corporation (“SSH”) with respect to a data security incident involving potential exposure of certain personally identifiable information (“PII”) and Protected Health Information (“PHI”) described in more detail below. SSH is a not-for-profit community hospital in Chicago, Illinois. SSH is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On December 10th, 2021, SSH detected a security incident impacting access to its systems. SSH immediately disconnected all system from external access, implemented its incident response protocols, and notified law enforcement. SSH also engaged external cybersecurity experts to conduct a forensic investigation to determine how the incident occurred and what information may have been impacted.

The investigation is now complete and SSH has determined that past and current employee information and patient information may have been compromised as part of this incident. The investigation determined that the files impacted may have contained first and last names, addresses, dates of birth, Social Security numbers, financial information, health insurance information, medical information, diagnoses, driver’s license information, health insurance policy numbers, and Medicare/Medicaid information for some employees and some patients.

2. Number of residents affected.

Ten (10) of Maryland residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on March 31, 2022 (a copy of the form notification letter is enclosed as Exhibit A).

March 31, 2022

Page 2

3. Steps taken in response to the incident.

SSH took steps to address this incident and to prevent similar incidents in the future, including implementing additional security controls to protect its network. These steps include enforcing stronger password requirements, enabling multifactor authentication, and additional data privacy and security awareness trainings for SSH's workforce. SSH has also deployed supplementary anti-malware and email phishing tools and will continue to evaluate its security protocols for opportunities to further bolster its network security.

On February 7th, 2022, SSH provided substitute notice on its website and media notice to two major Chicago news outlets. As part of this initial notice, affected individuals were offered 12 months of credit monitoring and identity protection services through IDX. Subsequently, once SSH identified specific individuals that were impacted as part of this incident, SSH followed up with individual notices to the affected individuals on March 31, 2022. Notice was also provided to the Department of Health and Human Services Office of Civil Rights on February 7th, 2022.

4. Contact information.

SSH takes the security of the information in its control seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com.

Sincerely,

CLARK HILL



Jason Schwent
Senior Counsel

cc: Daisy Dai ddai@clarkhill.com



P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-783-1445

Or Visit:

<https://response.idx.us/SouthShoreHospital>

Enrollment Code: <<Enrollment>>

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

March 31, 2022

NOTICE OF DATA SECURITY INCIDENT

Dear <<First Name>> <<Last Name>>,

South Shore Hospital ("SSH") is writing to let you know about a data security incident that may have impacted your Protected Health Information ("PHI"). We take the privacy and security of your information seriously and sincerely apologize for any concerns or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What happened:

On Friday, December 10, 2021, SSH became aware of unauthorized activity on its network. Upon discovery, we immediately implemented our incident response protocols, disconnected its network from external access, and external cybersecurity experts were hired to conduct a forensic investigation to determine what happened and what information may have been impacted. The investigation found that PHI for patients, including name, address, Social Security number, date of birth, driver's license number, and information related to diagnoses, may have been impacted. The privacy and security of our patients' information is important to us, and we wanted to let you know about the incident out of an abundance of caution.

What information was involved:

Impacted information may include your name, address, Social Security number, date of birth, driver's license number, and information related to diagnoses.

What we are doing:

To help reduce the risk of something like this happening again, we have implemented additional security controls and will continue to enhance our security controls to protect our network. These steps include enforcing stronger password requirements, enabling multifactor authentication, and additional data privacy and security awareness training for SSH's workforce. We have also deployed supplementary anti-malware and email phishing tools and will continue to evaluate our security protocols for opportunities to further bolster our network security.

As a safeguard, we are also offering identity theft protection services through IDX, a data breach and recovery services expert, at no charge to SSH patients affected. These services include <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

What you can do:

It is always a good idea to remain vigilant for incidents of identity theft or fraud, and credit reports and financial statements for suspicious activity.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-783-1445 or going to <https://response.idx.us/SouthShoreHospital> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is June 30, 2022. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information:

If you have any questions or concerns, please call 1-833-783-1445 Monday through Friday from 8 am to 8 pm Central Time. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,



Timothy A. Caveney, CEO
South Shore Hospital

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

- 1. Website and Enrollment.** Go to <https://response.idx.us/SouthShoreHospital> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-833-783-1445 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351
www.equifax.com/personal/credit-report-services

Experian Fraud Reporting and
Credit Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft