

BakerHostetler

Baker&Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Eric A. Packel
direct dial: 215.564.3031
epackel@bakerlaw.com

May 28, 2021

VIA EMAIL (ATTORNEYGENERAL@DOJ.NH.GOV)

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Sturdy Memorial Hospital (“Sturdy”), a not-for-profit acute care community hospital located in Attleboro, Massachusetts. Sturdy is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).

On February 9, 2021, Sturdy identified a security incident that disrupted the operations of its IT systems. Sturdy immediately took steps to secure its systems, launched a thorough investigation with the assistance of a third-party forensic investigator, and notified law enforcement. Through the investigation, Sturdy determined that an unauthorized party gained access to some of its systems during the morning of February 9, 2021. The systems were secured later that same day. In exchange for a ransom payment, Sturdy obtained assurances that the information acquired would not be further distributed and that it had been destroyed.

On April 21, 2021, Sturdy’s review and analysis of the files involved in the incident determined they contained information belonging to 161 New Hampshire residents, including their names and Social Security numbers, Driver’s License numbers, and/or financial account numbers, routing numbers and/or bank names.

Sturdy mailed notification letters to the New Hampshire residents on May 28, 2021 in accordance with HIPAA and N.H. Rev. Stat. Ann. § 359-C:20.¹ Sturdy also offered the residents

¹ This report is not, and does not constitute, a waiver of Sturdy’s objection that New Hampshire lacks personal jurisdiction over Sturdy regarding any claims related to this data security incident.

Attorney General Gordon MacDonald

May 28, 2021

Page 2

whose Social Security numbers and/or Driver's License numbers may have been involved one year of complimentary credit and identity monitoring services through Experian. A copy of the notification letter is enclosed. To help prevent a similar incident from occurring in the future, Sturdy implemented additional safeguards and technical security measures to further protect and monitor its systems.

Please do not hesitate to contact me if you have any questions regarding this incident.

Sincerely,

A handwritten signature in cursive script, appearing to read "Eric A. Packel".

Eric A. Packel

Partner

Enclosure



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Sturdy Memorial Hospital is committed to protecting the confidentiality and security of our patient information. We are writing to inform you that we recently identified and addressed a data security incident that involved some of your information. This letter explains the incident, measures that have been taken in response, and additional steps you can take to further safeguard your information.

What Happened? On February 9, 2021, we identified a security incident that disrupted the operations of our IT systems. We immediately took steps to secure our systems, launched a thorough investigation with the assistance of a third-party forensic investigator, and notified law enforcement. Through our investigation, we determined that an unauthorized party gained access to some of our systems during the morning of February 9, 2021. Our systems were secured later that same day. In exchange for a ransom payment, we obtained assurances that the information acquired would not be further distributed and that it had been destroyed.

What Information Was Involved? On April 21, 2021, our review and analysis of the files involved in the incident determined that they may have contained some of your information, including your name, contact information- including address and phone number, date of birth, Social Security number, Medicare Health Insurance Claim number, Driver's License number or other government issued identification number, medical history information, diagnosis or treatment information, procedure or diagnosis codes, prescription information, provider name, medical record number, Medicare/Medicaid number, health insurance information, and/or treatment cost information. Note that our electronic health record system was **not** involved in the incident.

What You Can Do: Though we have no indication at this time that your information has been or will be misused, we are offering you a one-year membership to Experian's® IdentityWorksSM Credit 3B at no cost to you. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. Enrolling in this program will not hurt your credit score. We also recommend you review the statements you receive from your healthcare providers. If you see services you did not receive, please contact the provider that issued the statement immediately. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your membership, as well as some additional steps you can take, please see the pages that follow this letter.**

What We Are Doing: We want to assure you that we take this incident very seriously and sincerely regret any concern this may cause you. To help prevent future occurrences of this nature, we have implemented additional safeguards and technical security measures to further protect and monitor our systems.

For More Information: We have established a dedicated call center to help answer any questions you may have about the incident. You may reach the call center at 1-855-537-2087, Monday through Friday, between 9:00 AM and 6:30 PM, Eastern Time.

Sincerely,

Robin B. Morris
Senior Vice President, Clinical Operations
Corporate Integrity Officer
Sturdy Memorial Hospital

To help protect your identity, we are offering a **one-year membership** of Experian IdentityWorksSM Credit 3B at no cost to you. 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: <<b2b_text_2(EnrollmentDeadline)>> (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**: <<Member ID>>

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 **877-288-8057**. Be prepared to provide engagement number <<b2b_text_3(Engagement#)>> 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:

- A. Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- B. Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- C. Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- D. \$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 877-288-8057 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 **877-288-8057**.

* 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. 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

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov