

April 11, 2024

Anjali Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Online Portal

Attorney General Anthony Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Regulatory Notice Re: Data Security Incident Involving Hapy Bear Surgery Center

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Hapy Bear Surgery Center, LLC (“HBSC”), a pediatric ambulatory dental surgery center located at 1979 Hillman Street, Tulare, CA 93274, with respect to a recent cybersecurity incident that was first discovered by HBSC on December 27, 2023 (hereinafter, the “Incident”). HBSC takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the Incident

On December 27, 2023, HBSC experienced a network disruption that impacted the functionality and access of certain systems. Upon discovery of this incident, MSC immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. Based on the investigation, HBSC found evidence to suggest some HBSC files were accessed by an unauthorized actor. HBSC then began reviewing the affected systems to identify the specific individuals and the types of information that may have been compromised. Prior to the completion of the forensic investigation, and in compliance with HIPAA, on February 23, 2024, HBSC posted substitute notice on their website. Additionally, on February 27, 2024, HBSC provided notice to a local media outlet, Visalia Times-Delta.

The forensic investigation was completed on March 8, 2024. The investigation determined that there were indicators that sensitive data may have been subject to unauthorized access and potential exfiltration. As a result of this determination, Hapy Bear Surgery Center (“HBSC”) conducted a

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Los Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

thorough review of the impacted systems to determine the extent that personal identifying information and patient health information was impacted. Out of an abundance of caution, HBSC decided to treat all protected information in their digital environment as at risk and to extend notice to all individuals whose information they maintained.

On March 19th, 2024, HBSC completed their investigation and identified all individuals who may have been impacted by this incident. Upon completion of its review, HBSC engaged a thirty-party mailing vendor to assist with mailing notice letters to the affected individuals, providing a ninety (90) day call center for individuals to contact should they have additional questions regarding the Incident, and provide complimentary credit monitoring and identity theft protection services to the affected individuals.

2. What Information Was Involved?

HBSC has determined that the following types of personally identifiable information may have been impacted: names, addresses, Social Security number, medical information, and health insurance information.

Please note that to date there has been no evidence to indicate that any individuals' personal information has been misused as a result of the Incident.

3. Number of Maryland residents affected.

Upon completion of its review, HBSC determined that information pertaining to five (5) Maryland residents were impacted as a result of the Incident. Notification letters to these individuals were mailed on April 11, 2024, by first class mail. A sample copy of the notification letter is attached hereto as **Exhibit A**.

4. Steps taken in response to the Incident.

HBSC is committed to ensuring the security and privacy of all personal information within its control and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, HBSC moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, HBSC engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, HBSC continues to enhance its network security to prevent a similar incident from occurring in the future, including replacing their firewall and engaged a managed cybersecurity services provider to oversee their digital environment. Lastly, HBSC informed their law firm and began identifying the potentially affected individuals in preparation for notice.

Although HBSC is not aware of any actual or attempted misuse of the affected personal information, HBSC offered twelve (12) months of complimentary credit monitoring and identity theft restoration services through Identity Force, a TransUnion company, to the impacted individuals residing in State of Maryland to help protect their identity. Additionally, HBSC provided guidance on how to better protect against identity theft and fraud, provide information on how to place a fraud alert and security freeze on one's credit file, the contact details for the

national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

5. Contact information

HBSC remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@wilsonelser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali Das

EXHIBIT A

EXHIBIT A

Hapy Bear Surgery Center, LLC
c/o Cyberscout

HAPY BEAR SURGERY CENTER LLC



April 11, 2024

Notice of Data Breach

Dear [REDACTED],

Hapy Bear Surgery Center, LLC (“HBSC”) is writing to inform you of a recent data incident (the “Incident”) that may have involved some of your health information. This letter contains details about the Incident, steps we have taken to remediate the Incident, and steps you can take to protect your health information.

What Happened?

On December 27, 2023, HBSC experienced a network disruption that impacted the functionality and access of certain systems. Upon discovery of this incident, HBSC immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident.

The forensic investigation, which concluded on March 8, 2024, determined that certain systems may have been compromised by an unauthorized actor. Based on these findings, HBSC found evidence to suggest some HBSC files were accessed by an unauthorized actor. HBSC then began reviewing the affected systems to identify the specific individuals and the types of information that may have been compromised. This review was completed on March 19th, 2024, and identified that some of your personal information may have been impacted by this incident.

What Information Was Involved?

Based on the investigation, the following information related to you may have been subject to unauthorized access: full name; address; medical information; health insurance information; Social number; and Driver’s License number.

We take our data responsibilities and protection of your data very seriously and we are sorry for any worry and inconvenience this news will cause. As of this writing, we have not received any reports of related identity theft since the date of the incident (December 27, 2023, to present). We would like to reassure you that we have taken all efforts possible to mitigate any further exposure of your personal information and we are committed to supporting you.

What We Are Doing

Data privacy and security is among HBSC’s highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon discovery of the Incident, HBSC moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, HBSC engaged a specialized cybersecurity firm and IT Personnel to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, HBSC replaced their firewall systems and engaged a managed cybersecurity services provider to oversee our digital environment.

000010102G0400

P

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Additional Important Information*, to learn more about how to protect against the possibility of information misuse.

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/hbhc> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information

HBSC recognizes that you may have questions not addressed in this letter. Should you have any additional questions representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident. Please do not hesitate to call 1-833-659-2763 (toll free) during the hours of 5:00 am to 5:00 pm Pacific, Monday through Friday (excluding U.S. national holidays).

We sincerely regret any inconvenience or concern that this matter may cause, and we remain dedicated to ensuring the privacy and security of all information within our control.

Sincerely,

Hapy Bear Surgery Center, LLC



Kenneth D. Pierson
CEO

Additional Important Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285

www.experian.com/fraud/center.html

www.transunion.com/fraud-alerts

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045

www.experian.com/freeze/center.html

www.transunion.com/credit-freeze

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

File Police Report: You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.



FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade

Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261.

The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a 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.

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at 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.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

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

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov