Hubbard Plastic Surgery & Skin Enhancement Notice Regarding Data Privacy Incident

Hubbard Plastic Surgery & Skin Enhancement ("Hubbard") is committed to our patients, their treatment, and their families – as well as protecting the privacy and security of their personal information. On August 10, 2022, we received information that some patient protected health information was impermissibly accessed by a former Hubbard employee. Prior to the former employee's last day on June 17, 2022, they used their Hubbard user credentials to access certain patient protected health and contact information on our systems. We later learned the former employee obtained employment at a new medical practice, and contacted several Hubbard patients to request they obtain services from her new employer. Upon learning of the issue, we commenced an immediate and thorough investigation, and alerted law enforcement.

Our investigation determined the former employee accessed an unusual number of patient files between May 31, 2022 and June 16, 2022. We are taking additional steps to mitigate this incident, which include reassessing our internal policies and engaging legal counsel to assist in our response to this incident. Pursuant to state and federal laws, we are also notifying all potentially affected patients about this incident.

The information accessed may have contained the following protected health information: full patient names, email and mailing addresses, Social Security numbers, phone numbers, dates of birth, sex, and marital status. At this time, we have no evidence other sensitive personal information, such as financial information, was involved in this incident. This incident does not affect all Hubbard patients.

We remind our patients to remain vigilant in reviewing their credit file for any fraudulent activity. We also recommend that our patients review the explanation of benefits statements that they receive from their health insurance providers, and follow up on any items not recognized. Please see the "Other Important Information" section below with additional information to help further safeguard your personal data.

As a team of dedicated and caring medical professionals, we understand that healthcare is about people taking care of people. We remain fully committed to maintaining the privacy of personal information in our possession, and upon learning of the event we took immediate action to try and remedy this situation. We continually evaluate and modify our practices to enhance the security and privacy of personal and protected health information, and are taking measures to augment our existing security.

If you are receiving or have received communication, including emails and texts, from the former employee or her new employer, Cosmetic Surgery Center for Women, you may forward such communications to us so that we may attempt to stop such communication. Please forward any unsolicited material to kgebler@hubbardplastic.com.

For further questions or additional information regarding this incident, please contact our office at (757) 687-1900 or kgebler@hubbardplastic.com. A Hubbard representative will respond to your inquiry within a timely manner. We appreciate your understanding as we respond to this unfortunate incident.

###

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Protecting Your Health Information.

As a general matter the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your "explanation of benefits" statement which you receive from your health insurance company. Follow up with your insurance company or the care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the dates of the potential disclosure to current date.

- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or care provider for any items you do not recognize.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.