15340

Norwood Hospital
A STEWARD FAMILY HOSPITAL

Steward

July 3, 2019

[redacted]

Dear Mr. [redacted]

We are sending you this letter as part of Norwood's Holy Family Hospital's commitment to patient privacy. We take our patients' privacy very seriously, and it is important that you are made aware of a recent incident involving your personal and protected health information

What Happened To My Information?

The Masshealth application completed on your behalf by Norwood Hospital intended for you was inadvertently emailed to an incorrect recipient. The application contains personal information including your Social Security Number.

Steps that have been taken in follow up to this incident?

Norwood Hospital has the utmost concern for your privacy and takes measures to provide a safe and secure system to protect your confidential information in a responsible manner. We take any breach of patient privacy very seriously and continue to educate our workforce and business associates on proper procedures to safeguard patients' information and belongings. The Hospital has an established compliance program, including policies on protecting patient privacy, and staff training which occurs at time of hire and at least annually. In response to this incident, the hospital contacted the recipient and obtained assurances that the information has been deleted.

Steps You Can Take to Protect Your Information

Norwood Hospital has no reason to believe that any person has misused, or will misuse, your data in way that might harm you. That said, there are steps you can take if you are concerned that your data might be misused—including requesting a security freeze or fraud alert on any bank and/or payment card accounts that you may maintain, and monitoring your credit. Additionally, Under Massachusetts

law, 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. Additional Information regarding security freezes and fraud alerts is enclosed with this letter as is required by the State of Massachusetts data breach notification laws.

Norwood Hospital would like to offer you 2 year of credit monitoring from Experian at no cost to you. If you would like to put such monitoring in place, you can activate credit monitoring product by taking the following steps no later than 9/26/19.

1. VISIT the Web Site https://www.experianidworks.com/credit or call 877.890.9332
2. PROVIDE Your Activation Code: QSM5CC9XT and Engagement Number: DB13452

In Closing

We sincerely apologize for any concern and inconvenience this incident has caused you. We take the confidentiality of your information very seriously. If you have any additional questions about this incident, please contact Jennifer Leighton, Patient Advocate at 781-278-6301.

Sincerely,

Kelly Breslin
Compliance & Privacy Officer
Norwood Hospital

ADDITIONAL INFORMATION ON IDENTIFY THEFT PREVENTION

The following proactive steps can help to detect and prevent financial fraud, medical identity theft or other misuse of your personal information:

Review your Credit Reports and Account Statements

It is recommended that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report once every 12 months by either visiting http://www.annualcreditreport.com, calling toll-free at 877-322-8228, or by completing an Annual Credit Report Request Form (found at http://www.ftc.gov/bcp/menus/consumer/credit/rights.shtm) and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You can also purchase a copy of your credit report by contacting one of the three national credit reporting companies:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374-0241	Allen, TX 75013	Fullerton, CA 92834-6790

When you receive your credit reports, review them carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

It is recommended you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to proper law enforcement authorities, including local law enforcement. You may contact your local state Attorney General's Office or the national credit reporting agencies listed above, to learn about preventing identity theft and to obtain additional information about avoiding identity theft. All U.S. residents may also contact the Federal Trade Commission ("FTC") for additional information at the following address:

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

Fraud Alerts

One may also consider placing a fraud alert to put creditors and potential creditors on notice that one may be a victim of fraud. There are also two types of fraud alerts that 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 at least 90 days. 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. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Credit or "Security" Freezes

You have the right to a free 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 a freeze. A credit freeze 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. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report

available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.