MPS
Medical Practice Solutions

<<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>>,

We are writing to notify you of a security incident that Medical Practice Solutions, Inc. ("MPS"), a business associate to <<b2b_text_1 (COVERED ENTITY/practice name)>>, has reported that may have affected your personal information. MPS contracts with healthcare organizations to provide billing and collection services.

MPS is not aware of any actual or attempted misuse of personal information as a result of this event, however, we take patient privacy very seriously. We want to make sure you are aware of the facts surrounding this event so you can take the precautions you feel are needed to protect your personal information.

What Happened?

On August 18, 2021, MPS discovered that an unauthorized party had gained access to an email account. Based on a third party forensics firm's investigation, the account was compromised from August 17, 2021 at 1:18 a.m. (CST) until August 18, 2021 at 9:34 p.m. (CST). Our forensics firm was unable to identify the source of the compromise and whether the unauthorized party actually viewed or accessed the contents of the email messages and their attachments. Unfortunately, your personal information was stored within one or more of these email messages.

What Information Was Involved?

Personal information may have included:

(1) Patient contact information (such as patient name, guarantor name, address, email address, and date of birth);

(2) Health insurance information (payer name; payer contract dates; policy information, including type and deductible amount; and subscriber/Medicare/Medicaid number)

(3) Medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers)

(4) Billing, payment, and claims information (invoices, payment details, submitted claims and appeals, and patient account identifiers used by your provider).

Please note that the unauthorized party may not have had access to all this information on every person affected by this event. Your Social Security number and/or financial information were **not** included.

What We Are Doing

After discovering the security incident, MPS terminated the unauthorized party's access to the affected email account. This included, for example, resetting the password for the email account where the unauthorized activity was detected. MPS has added two-factor authentication to restrict remote access to its employees' e-mail accounts. MPS also will be increasing security training requirements for all its employees to identify and defend against cyberattacks and social engineering techniques.

What You Can Do

As a precaution, we recommend you review statements you receive from your healthcare providers and health insurer. If you see charges for services you did not receive, you should contact the provider or insurer immediately.

For More Information

If you have any questions or would like additional information, please call our dedicated, toll-free call center at 1-855-541-3572, Monday through Friday between 8:00a.m. and 5:30p.m. Central Time, excluding some U.S. holidays.

Keeping your information private and secure is a high priority for us, and we apologize for any inconvenience as a result of this incident.

Sincerely,

Christopher L. Morgan

Chris Morgan
CEO, Medical Practice Solutions, Inc.

IDENTITY PROTECTION REFERENCE GUIDE

1. Review your Credit Reports. We recommend that you remain vigilant by monitoring your credit reports for any activity you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form. Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
1-888-378-4329	1-888-397-3742	1-800-916-8800
P.O. Box 105281	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5281	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

If you see anything in your credit report that you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

If you believe you are a 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 can also contact your local law enforcement authorities and file a police report. Keep a copy of the police report in case you are asked to provide copies to creditors to correct your credit record.

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

2. Place Fraud Alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and 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. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites.

It is only necessary to contact 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 should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Place Security Freezes. By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security 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.

To place a security freeze, you must contact each of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your Social Security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government-issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze.

4. Monitor Your Account Statements. We encourage you to carefully monitor your financial account statements, medical provider statements, and insurance statements for fraudulent activity and report anything suspicious to the respective institution or provider.

5. You can obtain additional information about the steps you can take to avoid identity theft and more information about fraud alerts and security freezes from the Federal Trade Commission (FTC). You may contact the FTC, Consumer Response Center at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.

***

You can obtain additional information about identity theft prevention and protection from the Attorney General at Mississippi Attorney General's Office, Consumer Protection Division, Post Office Box 22947, Jackson, MS 39225 or https://msda17.com/preventing-crime/identity-theft/ You may also contact the Consumer Protection Division of the Attorney General's Office at 1-800-281-4418.