T: 203-529-3271 • F:203-529-3273 • 521 BOSTON POST RD, ORANGE CT 06477

November 7, 2022

RE: Notice of Data Breach

Dear Valued Patient,

We are writing to notify you that DOCS Medical Group ("DOCS") was recently the victim of a cyber-attack that may have affected patient information stored on DOCS's network servers. Please note that this cyber-attack did not affect our electronic medical record or billing systems.

1. **Here is what happened**:

On September 7, 2022, DOCS began to identify limited unusual activity affecting a portion of its network. DOCS immediately began to investigate the matter and engaged Vancord, a well-known IT security firm to assist. Based upon its investigation, Vancord determined that DOCS was subject to a ransomware attack on September 7, 2022. Vancord completed its investigation and data review on October 18, 2022 which allowed DOCS to then begin to prepare a list of affected patients.

Vancord notified DOCS that the ransomware targeted a server containing various patient information. The information stored within the affected DOCS's environment include: demographic information (e.g. name and contact information), medical history, reasons for visiting DOCS Medical Group, Social Security numbers, insurance information and various financial information. The ransomware attack did not occur due to any act or omission of DOCS or its staff. Fortunately, the ransomware attack did not affect DOCS's electronic medical record or billing systems.

Please note that due to the limited nature of the ransomware attack, DOCS was fully operational at all times.

2. **Types of information involved:**

Based upon our review and investigation, we have determined that the affected information included: demographic information (e.g. name and contact information), medical history, reasons for visiting DOCS Medical Group, Social Security number, insurance information and various financial information.

Please note that this ransomware attack did not affect our electronic medical records or billing systems.

3. **Protection of your information:**

We are providing written notice to all individuals that we have identified as having information potentially affected by this incident. Included with this notice is a "Reference Guide" which provides useful information regarding how to protect your identity, including obtaining copies of your credit report and implementing credit freezes. We encourage you to review the Reference Guide closely.

We are also making available 24-months of credit monitoring at no cost to you. To learn more about the credit monitoring and to enroll, please go to https://app.idx.us/account-creation/protect or call 1-800-939-4170 and use the Enrollment Code GK2TXT7UL. IDX representatives are available Monday through Friday from 9 am – 9 pm Eastern Time. Please note the deadline to enroll is February 2, 2023.

4. Our Response

DOCS is notifying relevant state and federal authorities of this cyber-attack. While no health care provider is 100% secure in this day and age, we are working with outside advisors to evaluate ways in which we can reduce the likelihood of a future cyber-attack.

5. For more information:

DOCS takes its obligation to protect the privacy and confidentiality of our patients' personal information very seriously and we expect our vendors to do the same. We sincerely regret that this occurred. If you have any questions, you may contact us by calling the toll-free number 1 -844-240-5122 or emailing us at info@docsofct.com.

Sincerely,

DOCS Medical Inc.

Reference Guide

Review Your Account Statements. We encourage you to remain vigilant by reviewing your account statements. If you believe there is an unauthorized charge on your card, please contact your financial institution or card issuer immediately. The payment card brands' policies provide that cardholders have zero liability for unauthorized charges that are reported in a timely manner. Please contact your card brand or issuing bank for more information about the policy that applies to you.

Order A Free Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies 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 consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

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

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 2002 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

Equifax	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	1-800-349-9960	www.equifax.com/personal/credit-report-services/
Experian	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/freeze/center.html
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-888-909-8872	www.transunion.com/credit-freeze

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)
- Social Security Card, pay stub, or W2
- 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.