MEDNAX®
HEALTH SOLUTIONS PARTNER

December 23, 2020

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Security Event

To <<first_name>> <<middle_name>> <<last_name>>:

We are writing to inform you of a data security event that occurred at MEDNAX Services, Inc. ("MEDNAX") and may have impacted your personal information. MEDNAX provides revenue cycle management and other administrative services to its affiliated physician practice groups, including <<b2b_text_1 (covered entity name,/one)>> from which you may have received services.

What happened?

On <<b2b_text_2 (Date of Discovery)>>, 2020, MEDNAX discovered that an unauthorized third party gained access to a Microsoft Office 365-hosted MEDNAX business email account through phishing. "Phishing" occurs when an email is sent that looks like it is from a trustworthy source, but it is not. The phishing email prompts the recipient to share or give access to certain information. Upon discovery of this event, MEDNAX immediately took action to prevent any further unauthorized activity, began an investigation, and engaged a national forensic firm.

Based on the investigation, the unauthorized party was able to access a business email account <<b2b_text_5 (Incident Timeline)>><<b2b_text_6 (Incident Timeline Continued)>>. The email account is separate from internal network and systems, which were not involved in the event. Even though a thorough investigation was conducted, it was not possible to conclusively determine whether personal information was actually accessed by the unauthorized party. Based on the data analysis that was performed and ultimately completed in December 2020, we were able to determine which individuals may have had personal information in the impacted business email account. Based upon our thorough review of this matter, we are not aware of any actual or attempted misuse of personal information as a result of this event. However, we are notifying you because your personal information may have been in the impacted business email account.

What information may have been involved?

The patient information may have included: (1) patient contact information (such as patient name, guarantor name, address, email address, date of birth, and/or electronic signature); (2) Social Security number, driver's license number, non-resident and alien registration number, and/or financial account information; (3) health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber or Medicare number); (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, physician names, and Medical Record Numbers); and (5) billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider). Please note that not all data fields may have been involved for all individuals.

What we are doing.

MEDNAX takes the security of personal information seriously. As soon as we discovered the phishing event, we immediately took action to prevent any further unauthorized activity, including resetting the user password for the business email account where unauthorized activity was detected. We have and continue to enhance our security controls as appropriate to minimize the risk of any similar event in the future.

In addition, we have arranged to offer you identity monitoring services for a period of one year, at no cost to you. You have until March 23, 2021 to activate these services, and instructions on how to activate these services are included in the enclosed Reference Guide.

What you can do.

In addition to activating the complimentary identity monitoring, the enclosed Reference Guide includes additional information on general steps you can take to monitor and help protect your personal information. We encourage you to carefully review credit reports and statements sent from providers as well as your insurance company to ensure that all account activity is valid; any questionable charges should be promptly reported to the provider’s billing office, or for insurance statements, to your insurance company.

For more information

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, visit www.emailevent.kroll.com, or call toll-free 1-833-971-3267. This call center is open from 8:00 a.m. to 5:30 p.m. Central Time, Monday through Friday, excluding major U.S. holidays.

We regret that this event occurred and are very sorry for any inconvenience this event may cause you.

Sincerely,

Mary Ann E. Moore

Mary Ann E. Moore
Chief Compliance Officer

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

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.

Upon receiving 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 credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. 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. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

How to Activate Identity Monitoring

To help relieve concerns and restore confidence following this event, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **March 23, 2021** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

Place 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 against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor 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 fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

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

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, 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 security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security 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 security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	888-298-0045	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

MEDNAX
HEALTH SOLUTIONS PARTNER

December 23, 2020

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Security Event

To <<first_name>> <<middle_name>> <<last_name>>:

We are writing to inform you of a data security event that occurred at MEDNAX Services, Inc. ("MEDNAX") and may have impacted your personal information. MEDNAX provides revenue cycle management and other administrative services to its affiliated physician practice groups, including <<b2b_text_1 (covered entity name,/one)>> from which you may have received services.

What happened?

On <<b2b_text_2 (Date of Discovery)>>, 2020, MEDNAX discovered that an unauthorized third party gained access to a Microsoft Office 365-hosted MEDNAX business email account through phishing. "Phishing" occurs when an email is sent that looks like it is from a trustworthy source, but it is not. The phishing email prompts the recipient to share or give access to certain information. Upon discovery of this event, MEDNAX immediately took action to prevent any further unauthorized activity, began an investigation, and engaged a national forensic firm.

Based on the investigation, the unauthorized party was able to access a business email account <<b2b_text_5 (Incident Timeline)>><<b2b_text_6 (Incident Timeline Continued)>>. The email account is separate from internal network and systems, which were not involved in the event. Even though a thorough investigation was conducted, it was not possible to conclusively determine whether personal information was actually accessed by the unauthorized party. Based on the data analysis that was performed and ultimately completed in December 2020, we were able to determine which individuals may have had personal information in the impacted business email account. Based upon our thorough review of this matter, we are not aware of any actual or attempted misuse of personal information as a result of this event. However, we are notifying you because your personal information may have been in the impacted business email account.

What information may have been involved?

The patient information may have included: (1) patient contact information (such as patient name, guarantor name, address, email address, date of birth, and/or electronic signature); (2) health insurance information (payor name, payor 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, physician names, and Medical Record Numbers); and (4) billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider). Please note that not all data fields may have been involved for all individuals.

What we are doing.

MEDNAX takes the security of personal information seriously. As soon as we discovered the phishing event, we immediately took action to prevent any further unauthorized activity, including resetting the user password for the business email account where unauthorized activity was detected. We have and continue to enhance our security controls as appropriate to minimize the risk of any similar event in the future.

What you can do.

The enclosed Reference Guide includes additional information on general steps you can take to monitor and help protect your personal information. We encourage you to carefully review credit reports and statements sent from providers as well as your insurance company to ensure that all account activity is valid; any questionable charges should be promptly reported to the provider's billing office, or for insurance statements, to your insurance company.

For more information

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, visit www.emailevent.kroll.com, or call toll-free 1-833-971-3267. This call center is open from 8:00 a.m. to 5:30 p.m. Central Time, Monday through Friday, excluding major U.S. holidays.

We regret that this event occurred and are very sorry for any inconvenience this event may cause you.

Sincerely,

Mary Ann E. Moore

Mary Ann E. Moore
Chief Compliance Officer

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

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.

Upon receiving 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 credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. 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. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

Place 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 against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor 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 fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

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

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, 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 security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security 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 security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	888-298-0045	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.