ALSTON & BIRD

One Atlantic Center
1201 West Peachtree Street
Suite 4900
Atlanta, GA 30309-3424
404-881-7000 | Fax: 404-881-7777

Dawnmarie R. Matlock Direct Dial: 404-881-4253 Email: dawnmarie.matlock@alston.com

June 4, 2021

CONFIDENTIAL
VIA EMAIL

Office of the Washington Attorney General
SecurityBreach@atg.wa.gov

Re: Notice of Data Breach

To the Office of the Washington Attorney General:

We are writing on behalf of our client, Pediatrix Cardiology of Washington, P.C. d/b/a NorthWest Congenital Heart Care ("NWCHC"), a provider of comprehensive pediatric cardiac care in the Seattle-Tacoma metropolitan area, to notify you of a data security event. A copy of the notifications being sent to 1,136 Washington residents on June 4, 2021 by first class mail in accordance with notification requirements under state law and HIPAA is attached to this letter. NWCHC is also providing substitute notice at https://nwchcevent.com/ in accordance with HIPAA requirements.

During the early morning of May 7, 2021, an unauthorized third party entered the office of a single NWCHC physician and stole an external hard drive used for data backup purposes. NWCHC discovered this theft on the morning of May 7, 2021 and immediately contacted law enforcement and began a review to determine what information may have been included on the external hard drive. Based on this review, NWCHC determined that the external hard drive contained personal information for certain patients of this NWCHC physician, as well as for a small number of guardians or guarantors of the patients. Based upon its review of this matter, NWCHC is not aware of any actual or attempted misuse of such information as a result of this event.

The patient information may have included: (1) patient contact information (such as patient name, date of birth, and age); (2) medical and/or treatment information (dates of service, location, physician name, services requested or procedures performed, diagnosis codes, diagnosis or treatment descriptions, and Medical Record Numbers); and (3) for one individual, health insurance information. The external hard drive did not contain Social Security numbers or financial

account information for patients or guarantors. Please note that not all data fields may have been involved for all individuals.

NWCHC takes the security of personal information seriously. We have and continue to enhance our security controls to minimize the risk of any similar event in the future, including eliminating external hard drive data backups. Although no Social Security numbers and financial information were involved, and only one individual's health insurance information was involved, NWCHC is al so encouraging affected individuals to review statements sent from providers as well as from the ir insurance company to ensure that all account activity is valid and directing individuals to prom ptly report any questionable charges to the provider's billing office, or for insurance state ments, to the insurance company.

If you have any questions regarding this event or if you desire further information or assistance, please email me at Dawnmarie.Matlock@alston.com or call my direct line at (404) 881-4253.

Sincerely,

Dawnmarie R. Matlock

Enclosures

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data Security Event

Dear <<Name 1>>:

We are writing to inform you of a data security event that occurred at Pediatrix Cardiology of Washington, P.C. d/b/a NorthWest Congenital Heart Care ("NWCHC") and may have impacted your personal information.

What happened?

During the early morning of May 7, 2021, an unauthorized third party entered the office of a single NWCHC physician and stole an external hard drive used for data backup purposes. NWCHC discovered this theft on the morning of May 7, 2021 and immediately contacted law enforcement and began a review to determine what information may have been included on the external hard drive. Based on the review, we have determined that the external hard drive contained personal information for certain patients of this NWCHC physician, as well as for a small number of guardians or guarantors of the patients. Based upon our 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 on the stolen hard drive.

What information may have been involved?

The patient information may have included: (1) patient contact information (such as patient name, date of birth, and age); (2) diagnosis and/or treatment information (dates of service, location, physician name, services requested or procedures performed, diagnosis codes, diagnosis or treatment descriptions, and Medical Record Numbers); and (3) for one individual, health insurance information. The external hard drive *did not* contain Social Security numbers or financial account information for patients or guarantors. Please note that not all data fields may have been involved for all individuals.

What we are doing.

NWCHC takes the security of personal information seriously. We have and continue to enhance our security controls to minimize the risk of any similar event in the future, including eliminating external hard-drive data backups.

What you can do.

The enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. Although no Social Security numbers and financial information were involved, and only one individual's health insurance information was involved, we encourage you to carefully review 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 http://nwchcevent.com, or call toll-free (855) 535-1862. This call center is open from 9 am to 9 pm Eastern Time, Monday through Friday, excluding major U.S. holidays.

We regret that this event occurred and apologize for any inconvenience this event may cause you.

Sincerely,

Lee A. Wood
Assistant Secretary
Pediatrix Cardiology of Washington, P.C.

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.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
To the Parent or Legal Guardian of
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Notice of Data Security Event

To Parent or Legal Guardian of <<Name 1>>:

We are writing to inform you of a data security event that occurred at Pediatrix Cardiology of Washington, P.C. d/b/a NorthWest Congenital Heart Care ("NWCHC") and may have impacted your child's personal information.

What happened?

During the early morning of May 7, 2021, an unauthorized third party entered the office of a single NWCHC physician and stole an external hard drive used for data backup purposes. NWCHC discovered this theft on the morning of May 7, 2021 and immediately contacted law enforcement and began a review to determine what information may have been included on the external hard drive. Based on the review, we have determined that the external hard drive contained personal information for certain patients of this NWCHC physician, as well as for a small number of guardians or guarantors of the patients. Based upon our 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 child's personal information may have been on the stolen hard drive.

What information may have been involved?

The patient information may have included: (1) patient contact information (such as patient name, date of birth, and age); (2) medical and/or treatment information (dates of service, location, physician name, services requested or procedures performed, diagnosis codes, diagnosis or treatment descriptions, and Medical Record Numbers); and (3) for one individual, health insurance information. The external hard drive *did not* contain Social Security numbers or financial account information for patients or guarantors. Please note that not all data fields may have been involved for all individuals.

What we are doing.

NWCHC takes the security of personal information seriously. We have and continue to enhance our security controls to minimize the risk of any similar event in the future, including eliminating external hard-drive data backups.

What you can do.

The enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your child's personal information. Although no Social Security numbers and financial information were involved, and only one individual's health insurance information was involved, we encourage you to carefully review 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 http://nwchcevent.com, or call toll-free (855) 535-1862. This call center is open from 9 am to 9 pm Eastern Time, Monday through Friday, excluding major U.S. holidays.

We regret that this event occurred and apologize for any inconvenience this event may cause you.

Sincerely,

Lee A. Wood
Assistant Secretary
Pediatrix Cardiology of Washington, P.C.

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.