Christopher DiIenno
Office: 267-930-4775
Fax: 267-930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

July 15, 2019

VIA EMAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
Email: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Northwood, Inc. ("Northwood"), 25790 Commerce Drive, Madison Heights, Michigan 48071, and are writing to notify you of a recent incident that may affect the security of the personal information of approximately one thousand one hundred and eighty-five (1,185) Washington residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Northwood does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data incident notification statute, or personal jurisdiction.

Nature of the Data Event

On May 6, 2019, Northwood became aware of suspicious activity relating to an employee email account. Northwood immediately launched an investigation to determine what may have happened and what information may have been affected. Working together with a leading computer forensics expert, their investigation determined that an unauthorized individual accessed the employee email account between May 3 and May 6, 2019. No other email accounts or Northwood systems were impacted by this incident.

Because the investigation was unable to determine which email messages in the account may have been opened or taken by the unauthorized individual, an intensive review of the impacted email

account contents was performed to identify all individuals for whom personally identifiable information ("PII") may have been impacted. The large volume and variety of documents in need of review required a combination of automated forensic tools and manual document review to check this data for the presence of PII. The individuals impacted by this incident were identified on June 19, 2019.

Once the affected individuals were identified, Northwood worked to verify the information at issue and identify the best possible contact information for the impacted individuals. Northwood then began preparing an accurate written notice of this incident.

The types of PII relating to Washington residents determined to be stored within the impacted email account were not identical for every potentially affected individual. The email account contained information pertaining to certain healthcare providers in connection with their exclusion status with the Centers for Medicare & Medicaid Services. The types of PII relating to Washington residents determined to be stored within the impacted email account included the following: name and Social Security number.

Notice to Washington Residents

On July 15, 2019, Northwood began mailing written notice of this incident to potentially impacted individuals, including approximately one thousand one hundred and eighty-five (1,185) Washington residents. Such notice is being provided in substantially the same form as the letter attached here as ***Exhibit A.***

Other Steps Taken

Northwood is offering the affected individuals complimentary access to two years of free credit monitoring and identity restoration services through Kroll. Additionally, Northwood is providing potentially affected individuals with information on how to protect against identity theft and fraud, including information on how to contact the Federal Trade Commission and law enforcement to report any attempted or actual identity theft and fraud. In addition to providing notice of this incident to you, Northwood will be providing notice to other state regulators and the United States Department of Health and Human Services.

Northwood has taken several immediate steps to protect against similar incidents in the future. Upon learning of this incident, Northwood quickly took the impacted email account offline and changed the account password. Northwood then implemented mandatory password resets for all employee email accounts and notified employees to be on the lookout for suspicious emails. They are continuing to monitor their systems to ensure they are secure. Northwood will be taking steps to enhance data security protections to protect against similar incidents in the future, including implementing multi-factor authentication, additional technical safeguards, and providing additional training and education to its employees.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security incident, please contact me at (267) 930-4775.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD:CRM
Enclosure

cc:

Office of the Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188
Email: securitybreach@atg.wa.gov

Exhibit A

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Breach

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Northwood, Inc. ("Northwood") is a manager and supplier of durable medical equipment for insurance plans and other entities. Northwood is writing to notify you of an incident that occurred at Northwood which may affect the security of some of your personal information. We take this incident very seriously. This letter provides details of the incident and the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On May 6, 2019, Northwood became aware of suspicious activity relating to an employee email account, as a result of a phishing email that captured the employee's login credentials. We immediately launched an investigation to determine what may have happened and what information may have been affected. Working together with a leading computer forensics expert, our investigation determined that an unauthorized individual accessed the email account between May 3 and May 6, 2019. Because we were unable to determine which email messages in the account may have been accessed or viewed by the unauthorized individual, we reviewed the entire contents of the email account to identify what personal and protected information was stored within it. On June 19, 2019, we identified the individuals potentially impacted by this incident after a thorough review of the email account. No other email accounts or Northwood systems were impacted by this incident.

What Information Was Affected? Although we cannot confirm whether your personal information was actually accessed, viewed, or acquired without authorization, we are providing you this notification out of an abundance of caution, because such activity cannot be ruled out. The email account contained information pertaining to certain healthcare providers in connection with their exclusion status with the Centers for Medicare & Medicaid Services, which included your <<ClientDef1(Breach Details Variable Text)>>.

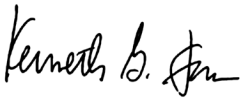
What Are We Doing? Information privacy and security are among our highest priorities. Northwood has strict security measures to protect the information in our possession. Upon learning of this incident, we immediately took the impacted email account offline and changed the account password. We then implemented mandatory password resets for all employee email accounts and notified our employees to be on the lookout for suspicious emails. Following this incident, we implemented additional technical safeguards on our email system, including multi-factor authentication, advanced threat protection, and email archiving, and provided further training and education for employees to prevent similar future incidents.

What Can You Do? Although we are not aware of any actual or attempted misuse of your information, we arranged to have Kroll monitor your identity for 2 years at no cost to you as an added precaution. Please review the instructions contained in the attached "Steps You Can Take to Protect Your Information" to enroll in and receive these services. Northwood will cover the cost of this service; however, you will need to enroll yourself in the credit monitoring service.

For More Information: We recognize that you may have questions not addressed in this letter. If you have additional questions, please call Northwood's dedicated assistance line at 1-800-494-0297 (toll free), Monday through Friday, 8:00 a.m. to 5:30 p.m., CT.

We sincerely regret any inconvenience this incident may cause you. Northwood, Inc. remains committed to safeguarding the information in our care and we will continue to take steps to ensure the security of our systems.

Sincerely,



Kenneth G. Fasse
President, Northwood, Inc.

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring

As an added precaution, we have arranged to have Kroll monitor your identity for 24 months at no cost to you. The following identity monitoring services start on the date of this notice.

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **October 10, 2019** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-800-494-0297. Additional information describing your services is included with this letter.

Monitor Your Accounts.

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity.

Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Security Freeze. You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	TransUnion	Equifax
PO Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 2000 Chester, PA 19016 1-888-909-8872 www.transunion.com/credit-freeze	PO Box 105788 Atlanta, GA 30348 1-800-685-1111 www.equifax.com/personal/credit-report-services

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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

Additional Information. You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. ***For Maryland residents,*** the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov. ***For New Mexico residents,*** you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. ***For North Carolina Residents:*** The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at www.ncdoj.gov. ***For Rhode Island Residents:*** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately XXX Rhode Island residents impacted by this incident. This notice has not been delayed by a law enforcement investigation.