December 26th, 2024

Attorney General Bob Ferguson

1125 Washington St SE

PO Box 40100

Olympia, WA 98504

(360) 753-6200

Re: Data Event Involving Northwest Asthma & Allery Center

Dear Attorney General Ferguson,

Northwest Asthma & Allergy Center is a HIPAA covered entity with several locations throughout Washington state. This notice is in regard to a recent data event that was first discovered on November 13th, 2024. Please know that Northwest Asthma & Allergy Center (NAAC) takes the security and privacy of the information in our systems very seriously.

This letter is intended to provide information regarding the nature of the event, what information may have been compromised, the number of Washington residents being notified, and the steps NAAC has taken in response to the event.

1. **Nature of the Event**

The breach occurred overnight on November 12th,2024 and was terminated immediately after we became aware of it on the morning of November 13th,2024. Our third-party IT support and security partner, Praece did a comprehensive investigation to determine the nature and scope of the date event. Per that investigation, Praece determined that an unauthorized user was able to gain access to an email account of one of our employees that contained PHI until they were locked out on the morning of November 13th.
The analysis was completed on November 14th. Praece confirmed what data was accessed by the malicious actors. Although NAAC and our security partner are unaware of any fraudulent misuse of information, the data that may have been exposed because of the unauthorized activity include: patient names, birthdates, social security numbers, insurance carriers, treatment dates, test results, treatment plans, and contact information

2. **Number of Washinton Resident that may be Affected**

NAAC identified and notified 39,342 individuals potentially affected by this Event. Of those, 33,074 were sent email notifications, and 6268 were sent traditional mail notifications. Notification letters to these individuals started being emailed on December 11th,2024 and physically mailed on **(This Date)** by standard first-class mail. A sample copy of the notification letter is included with this letter following the cover letter.

3. **Steps taken in Response to the Date Event**

NAAC is committed to ensuring the security and privacy of all personal information on all our systems. Upon discovery of the event, Praece (NAAC's security partner) moved quickly to investigate and respond to the event. Praece conducted a forensic investigation to determine the nature and scope of the event. After determining the scope of the event Praece sifted through the affected staff's email to determine what data may have been compromised. Additionally, Praece and NAAC have ensured that all staff are being compliant with MFA and have added additional Security Trainings to provide guidance on how to better protect against the newest types of identity theft and fraud. In our letter to affected patients we have included information on how to place a fraud alert and a security freeze on one's credit file, and contact details for the 3 major national consumer reporting agencies, information on how to obtain a credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports.

4. **Contact Information**

Northwest Asthma & Allergy Center remains dedicated to protecting all PHI in our systems. If you have any questions or need additional information, please contact me at rnagi@nwasthma.com or 206.527.1200 ext1155

Sincerely,

Ravindra Nagi

[Date]

[Patient Name]
[Patient Address]
[City, State, Zip Code]

Dear [Patient]:

We take the privacy of our patients very seriously and are writing to notify you that your protected health information ("PHI") may have been compromised as a result of a security breach at our practice.

The breach occurred overnight on 12 November 2024 and was terminated immediately after we became aware of it on the morning of 13 November 2024. To the best of our knowledge and belief, information containing patient names, birthdates, social security numbers, insurance carriers, treatment dates, test results, treatment plans, and contact information were potentially accessible to an unauthorized intruder when the email inbox of one of our employees was compromised by a malicious actor. A thorough review of the correspondence, attached files, and digitalized faxes in the employee's email inbox contained patient referrals, patient registration forms, test results, authorization and consent forms, and prior treatment records which contained PHI. Please note that our electronic medical record and other network systems were not impacted by this security breach.

Although you are not required to take any action, we suggest that you immediately take the following steps:

- Call the toll-free numbers of any one of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.
    - Equifax: 1- 866-349-5191; www.equifax.com; P.O. Box 105069, Atlanta, GA 30348-5069.
    - Experian: 1-888-397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013.
    - TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19016
- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.
- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.

We deeply regret that this incident occurred and are taking steps to address it and to guard against future breaches. To that end, we have engaged outside experts to conduct a thorough review of our security measures and introduced additional training for all staff.

Please do not hesitate to contact us with any questions about this incident, or if you need additional information on what you should do as a result of the breach.

Sincerely,

Name
Title