	Date	Reviewer
Written by:	3-31-2021	Tribal Attorney & Quality Assurance
Protocol Approved by:		
Last Updated	4-14-2021	Quality Assurance

NUMBER: **HIPAA VIOLATION COMPLAINT – INVESTIGATION PROTOCOL**
SUBJECT: **HEALTH CLINIC INTERNAL OPERATION PROCEDURE**
AUTHORIZING BODY: Nooksack Health Clinic Management
RESPONSIBLE OFFICE: Health

I. PURPOSE

The purpose of this protocol is to ensure consistent investigative procedures are being followed by the HIPAA Compliance Officer, so our clients, and the community at large, maintain trust in our clinic.

II. PROTOCOL / PROCEDURES

A. Every Complaint will receive a timely response.

1. The Nooksack HIPAA Compliance Officer shall treat all patient complaints of privacy seriously by taking prompt action.
2. Upon receipt of a complaint, the Compliance Officer shall acknowledge receipt in writing to the complainant, and he or she shall open a file in every case in which all the required information is provided regarding the complaint.
3. Absent extraordinary circumstances, the Compliance Officer shall resolve all investigations within 30 days of receipt of the complaint, and if necessary, correct any breach within an additional 30 days.
   a) If the Compliance Officer determines that the Nooksack Tribal Health Clinic is required to report a breach, he or she shall do so within 60 days from discovery of the breach.
   b) Under these procedures, the Compliance Officer shall consider time is of the essence when handling complaints.
      i. The complainant shall be requested to produce his or her complaint in writing, within 30-days of the notification of any issue, by filling out a complaint form approved by the Compliance Officer.
      ii. Once the patient or personal representative (as defined in the HIPAA Privacy and Security Rule) submits a completed complaint form, the HIPAA Compliance Officer must assume exclusive responsibility over the investigation and shall determine if a HIPAA breach has occurred.
      iii. The Compliance Officer shall accept complaints only from prospective, current, or former patients, or their personal representatives, as defined in the HIPAA Privacy and Security Rule; complaints by any other person shall be dismissed without investigation.
      iv. No person, or office, other than the Compliance Officer has authority under these procedures to investigate HIPAA complaints.
      v. All HIPAA investigations shall be strictly confidential to the extent required by law.

B. All Formal Complaints shall receive a thorough investigation.

1. The HIPAA Compliance Officer shall fully investigate the complaint by engaging in fact finding to understand the incident and to determine if there is a breach of the HIPAA Privacy and Security Rule. The Compliance Officer has full discretion to determine the scope and extent of a thorough investigation; however, in most cases, the Compliance Officer shall review internal policies and procedures to determine if there was a violation; shall identify any persons who accessed, used or received any protected health information (PHI), including interviewing and obtaining statements from the complainant and staff that may have been involved in the incident; and shall review the nature and extent of the PHI involved.
   a) If the investigation does not substantiate a HIPAA violation then the Compliance Officer shall proceed to section **F.** below; otherwise, he or she shall continue to section **C.** The Compliance Officer's decision on whether there has been a breach and what remedy, if any, is appropriate shall be final.

C. Steps will be taken to correct and mitigate any harmful effects.

1. If the investigation establishes, by clear and convincing evidence, that a breach has occurred, the HIPAA Compliance Officer shall attempt to mitigate the harmful effects of the breach.
2. The Compliance Officer shall start by correcting the breach if possible by ordering the halt of any further disclosure or uses of unauthorized PHI.
3. If the breach has already occurred, the Compliance Officer shall take immediate measures to mitigate the breach.
   a) The Compliance officer shall complete an investigation to:
      i. Understand the causes of the breach.
      ii. Determine ways to prevent similar breaches in the future.
   b) Mitigation efforts may include:
      i. Updating policies and procedures.
      ii. Providing refresher compliance training for staff.
      iii. Implementing new safeguards to prevent noncompliance.
   c) The type and number of mitigation efforts are in the best professional judgment of the Compliance Officer and shall be final.

D. The Compliance officer shall determine if there is a reportable breach.

1. If the Compliance Officer determines that a breach has occurred, but involves the use, or disclosure of secured PHI, then the breach does not have to be reported to the United States Department of Health and Human Services.
2. If the disclosure, or use involves unsecured PHI that is not properly rendered unusable, unreadable, or indecipherable, then a breach is presumed under the Breach Notification Rule. In such cases, the Compliance Officer shall undertake further analysis as necessary to determine if an exception applies or if there is a low probability that the PHI has been compromised.
   a) First, the Compliance Officer shall determine if the breach fits within one of the three exceptions of the Breach Notification Rule:
      i. The unintentional access, use, or acquisition of PHI by a workforce member, or person acting under the authority of the Nooksack Tribal Health Clinic, if done in good faith and within the scope of authority and does not result in further use or disclosure that violates HIPAA.
      ii. An inadvertent disclosure of PHI by an authorized person to another authorized person as long as the PHI is not further used or disclosed.
      iii. Provider has a good faith belief that the unauthorized person would not likely retain the PHI that was disclosed.

b) If an exception does not apply, the Compliance Officer shall then conduct a risk assessment that considers the following four factors:
    i. The nature and extent of the PHI involved, including the types of identifiers, and the likelihood of re-identification;
    ii. The unauthorized person who used the PHI or to whom the disclosure was made;
    iii. Whether the PHI was actually acquired or viewed; and
    iv. The extent to which the risk to the PHI has been mitigated.
c) If the assessment indicates more than a low probability of PHI compromise, then the breach must be reported.
    i. Breaches affecting less than 500 individuals require notices to affected individuals within 60 days following the discovery of a breach and notice to the United States Department of Health and Human Services (HHS) within 60 days of the end of the calendar year.
    ii. For larger breaches, affecting 500 or more individuals, notices to affected individuals, HHS and major media outlets must be sent within 60 days following the discovery of the breach.
    iii. In addition to HIPAA, Washington state breach notifications laws must also be followed.
d) The Compliance Officer shall contact the Office of Tribal Attorney for legal advice before making a final determination on the issue of a reportable breach and of appropriate mitigation measures.

E. HR must be involved to determine disciplinary measures.

1. HIPAA requires the Nooksack Tribal Health Clinic apply appropriate sanctions against employees who violate HIPAA. The Compliance Officer must refer any breach involving Nooksack Tribal Health Clinic employees to the Nooksack Human Resources Department and the Nooksack Health Department Director, both of whom will then consult with the Compliance Officer to identify appropriate disciplinary measures.
2. The Compliance Officer is not authorized to take disciplinary actions against any Nooksack Tribal employees and only has the authority to order employees to take such measures, as are necessary, to halt current breaches or to prevent future breaches.

F. All investigations must be documented.

1. The Compliance Officer shall document all investigative efforts including:
    a) The patient complaint.
    b) The internal investigation and determination.
    c) All documents reviewed and witness statements obtained.
    d) All actions taken to mitigate the breach.
    e) Copies of breach notices or rationale for not reporting.
    f) Any and all referrals to the Human Resources Department.

G. The HIPAA Compliance Officer must follow up with the patient or personal representative.

1. The Compliance Officer shall promptly notify the patient, or personal representative, of the findings and resolution of the complaint in writing.
2. The patient, or personal representative, must be informed of additional rights under the HIPAA Privacy and Security Rule.

Appendix A

Office of the Nooksack HIPAA Compliance Officer
Health Information Privacy and Security Complaint Form

FIRST NAME	**LAST NAME**	
HOME PHONE (Please include area code)	**WORK PHONE** (Please include area code)	
STREET ADDRESS	**CITY**	
STATE	**ZIP**	**E-MAIL ADDRESS** (If available)

Are you filing this complaint for someone else? ☒ Yes ☐ No

If yes, what is your relationship to the other person? _____

If Yes, whose health information privacy/security rights do you believe were violated?

FIRST NAME	**LAST NAME**

What person(s) or entities representing or conducting services on behalf of the Nooksack Tribal Health Clinic do you believe violated the HIPAA Privacy and Security Rule?

PERSON / AGENCY / ORGANIZATION

NAME	**AGENCY / ORGANIZATION**	
STREET ADDRESS	**CITY**	
STATE	**ZIP**	**PHONE** (Please include area code)

When do you believe the violation(s) occurred?
LIST DATE(S)

Briefly describe/state the violation (what happened). How and why do you believe the HIPAA Privacy/Security/Breach Notification rules were violated? Please be as specific as possible. (**Attach additional pages as needed**)

Please sign and date this complaint. You do not need to sign if submitting this form by email because submission by email constitutes your signature.

_____ _____
Signature Date

Filing a complaint is voluntary. However, without the information requested above, we may not be able to proceed with your complaint. We will use the information to evaluate your complaint and determine how we will process your complaint. Information submitted on this form is treated confidential. Names or other identifying information about individuals are disclosed when it is necessary for investigation of possible health information privacy violations, internal systems operations, or routine uses. This can include disclosure of information outside the Nooksack Tribal Health Clinic for purposes associated with health information privacy compliance and as required or permitted by law. It is illegal for the Nooksack Tribal Health Clinic to intimidate, threaten, coerce, discriminate, or retaliate against you for filing this complaint. You are not required to use this form; you may also write a letter or submit a complaint electronically to us, which includes all the information requested on the form.

Submit your complaint to:
Nooksack Tribal Health Clinic
HIPAA Compliance Officer
2510 Sulwhanon Dr.
Everson, WA 98247