Procedure Number: HR.1306.7	**Policy Section:** Human Resources
Correlating Policy: Employee Corrective Action - HR.1306	
Effective Date: 01/2024	**Reviewed By:** Quality Improvement Committee
Review Date(s): 01/2024	
Procedure Name: HIPAA Sanction Procedure	
Purpose: To establish clear criteria for determining educational, corrective or disciplinary action when violations of NOAH's privacy and security policies or other related regulatory requirements have occurred	

Procedure:

Sanction Process for NOAH Workforce HIPAA Violations

1. It is the policy of NOAH that all workforce members must protect the confidentiality, integrity and availability of sensitive information at all times. NOAH will impose sanctions, as described below, on any individual who accesses, uses or discloses sensitive information without proper authorization. NOAH will take appropriate disciplinary action against workforce members, contractors or any individuals who violate NOAH information security and privacy policies or state or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

2. All privacy or security infractions will be communicated to the Quality & Compliance Services where the matter will be tracked, investigated, and reported to government authorities or the affected patient(s), as applicable. Quality & Compliance Services may involve other appropriate departments in the investigation including, but not limited to, Human Resources, Information Technology (IT) Security and department management in which the matter occurred.

3. This policy/procedure applies to all individuals who have access to Protected Health Information (PHI) in electronic, paper or any other format including employees, volunteers, physicians, contractors, vendors, etc. Such individuals are referred to as "users" in this policy/procedure.

4. The Compliance Officer, Privacy Officer and/or IT Security Officer in consultation with the Human Resources and department leadership, will review all privacy/security policy violations and make recommendations for corrective and disciplinary action.

5. Any questions about this policy should be directed to the Compliance Officer or Human Resources.

Levels of Infractions

The following three (3) levels of activity will be used as a guide in determining appropriate corrective or disciplinary action for violations of NOAH's privacy and security policies and applicable law:

1. Level I Infractions: Unintentional/Erroneous Access, Use, Transmission or Disclosure of PHI

    A. This Level refers to unintentional or careless access, use, transmission or disclosure of protected health information (PHI) for reasons not related to treatment, payment or healthcare operations. Examples include, but are not limited to:

        a. Discussions of PHI in public areas where others can overhear where reasonable efforts weren't made to protect the information being disclosed

        b. Faxing PHI to the wrong fax number due to User error by mis-keying or data entry

        c. Leaving PHI accessible in public areas (e.g. PHI left in cafeteria, surgery schedules not covered in waiting areas, etc.)

        d. Accidental transmission of PHI outside of the NOAH network

        e. Emailing PHI outside of NOAH network without properly encrypting document/email

        f. Transmitting/emailing/messaging unnecessary PHI inside or outside of NOAH network

        g. Computer left logged on and unattended (without another person accessing PHI)

        h. Disclosing information without verifying the identity of the requester

        i. Independently accessing one's own medical record in the electronic medical record (EMR)

        j. Handing or mailing wrong information to patients

2. Level II Infractions: Intentional Access, Use, Transmission or Disclosure of PHI

    A. This Level refers to intentional access, use, transmission or disclosure of PHI for reasons other than treatment, payment or healthcare operations. This Level also includes situations where a User exhibits a degree of negligence where they had otherwise received adequate training on appropriate controls to avoid a loss or exposure of PHI. Examples include, but are not limited to:

        a. Access of PHI for patients who the User does not have a legitimate job duty to access including, but not limited to, family members, friends, co-workers,

volunteers, board members, physicians, persons listed as VIPs, celebrities, sports figures, politicians, etc.

b. Accessing PHI out of concern or curiosity, regardless of intent

c. Verbally disclosing PHI to individuals at work who do not have a specific need to know to perform their job duties

d. Verbally disclosing PHI with individuals outside of the work setting

e. Changing/Modifying the patient record without authorization

f. Displaying (failing to safeguard) a User's password in or around the User's work space

g. Taking a picture of a patient with a personal cell phone

h. Sharing a User's login/password with another person

i. Computer left logged on and unattended and another person uses the logged in computer to access PHI

j. Intentional transmission of PHI outside of the NOAH network (via texting, email, or other electronic means)

k. Loss of computer equipment containing PHI due to employee negligence

l. Intentionally using another person's logged in computer and/or username and password to access patient information

m. Posting PHI on any social media or Internet site

3. Level III Infractions: Access, Use, Transmission or Disclosure of PHI for Personal Gain, Malicious Intent or that Results in Harm to a Patient

A. This Level refers to access, use, transmission or disclosure of PHI for personal gain, with malicious intent or that could result in harm to a patient. Examples include, but are not limited to:

a. Accessing PHI to sell for personal profit, gain, or benefit or which causes harm or loss to the patient

b. Accessing, using, displaying or disclosing PHI that causes embarrassment, damage to an individual's reputation, or to undermine a person's integrity or character

c. Accessing, using or transmitting PHI that creates financial risk to a patient including use of Social Security Number

d. Physical break-in or theft of computer equipment containing PHI; or intentional manipulation, downloading or re-coding of software programs, applications or settings that results in unauthorized disclosure of PHI

e. Disclosing PHI, in any form, with any third party with the intent to cause harm to an individual

Levels of Corrective/Disciplinary Action

Each Level of Infraction corresponds to a level of corrective action as follows:

1. Corrective/Disciplinary Action for Level I Infractions:

a. The User will be provided education and awareness of the infraction and informed of appropriate procedures and protocols to protect PHI.

b. Education and awareness training will be documented in the User's record by the employee's direct supervisor, if an employee, or documented by the individual who owns the User's relationship with NOAH

c. The user will be informed of the impact of repeated infractions of this policy.

d. A documented verbal coaching or counseling will be applied in these cases.

2. Corrective/Disciplinary Action for Level II Infractions:

a. For purposes of corrective action, a second offense of any Level I infraction (does not have to be the same infraction) will follow the action taken of a Level II Infraction.

b. Will result in a Final Written Warning. If the User has already received a Final Written Warning, for any reason, the employee will be terminated as per the Employee Corrective Action policy.

c. The User will receive education and training on the appropriate policies that govern the subject matter where the infraction was committed. All education and training will be documented in the User's record, if an employee, or documented by the individual who owns the User's relationship with NOAH.

d. Depending on the nature of the situation and compounding facts, an employee could be terminated for a Level II infraction.

e. A User who is not an employee will have their access removed from applicable systems. Exceptions to this access removal must be approved by the HR Director, Security and/or Privacy Officer and Compliance Officer.

f. Will be considered reportable to professional governing board, if applicable.

g. The User will be informed of the impact of repeated infractions of this policy.

3. Corrective/Disciplinary Action for Level III Infractions:

a. For purposes of corrective action, a third offense of any Level I infraction (does not have to be the same infraction) will follow the action taken of a Level III Infraction and a second offense of any Level II infraction (does not have to be the same infraction).

b. Immediate termination of employment, affiliation or association with NOAH

c. Reporting to the User's professional governing board will be made, where applicable.

d. Notification will be made to law enforcement, where applicable.

e. For contracted User's, legal action may be taken, as appropriate.

f. For Business Associates, review and application of Indemnification clauses in the Business Associate Agreement may be enacted.

4. When making a determination of disciplinary action, consideration should always be made as to the employee's past record of disciplinary action, counseling or other corrective action. The corrective action listed in this policy should not be evaluated in isolation if an employee has a track record of other concerns not related to privacy or security infractions that may prompt more stringent action.

5. Another key factor used in determining disciplinary action will be the employee's cooperation during the course of the investigation. Human Resources policy and procedure HR1303 titled "Employee Standards of Conduct," requires that during an organizational investigation, employees must speak the truth with no intent to deceive or mislead by technicalities or omissions and cooperate with all work-related investigations including compliance investigations. If, through the course of the investigation, the employee misleads or lies to those conducting an investigation for an alleged privacy breach, disciplinary action may be escalated (e.g., a Level I disciplinary action may be raised to a Level II disciplinary action or a Level II may be raised a Level III).

6. All infractions of this policy, regardless of level, should be documented in the User's record for tracking and in Compliatric for tracking of HIPAA breeches. All infractions requiring corrective action should be conducted in concert with the respective Human Resources Business Partner.