Procedure Number: HS.107.5	**Policy Section:** HIPAA Privacy
Correlating Policy: HS.107 Minimum Necessary Standard	
Effective Date: 01/2024	**Reviewed By:** Quality Improvement Committee
Review Date(s): 01/2024	
Procedure Name: Allowable Access, Use, and Disclosure of Protected Health Information (PHI)	
Purpose: To establish when it is allowable for members of NOAH's workforce to access, use or disclose patient information under the HIPAA Privacy and Security Rules.	

Procedure:

User Access Rules §164.524

1. User access rights and privileges are based on their role or function to ensure they may access only the information necessary to perform the legitimate duties associated with the individual's role. Access of patient information by staff for curiosity and personal business reasons is prohibited. NOAH's role of IT Director, Security Officer, and/or CMIO will be responsible for reviewing and changing user access rights to ensure they are limited to information required by the user's job functions.

2. The HIPAA Privacy and Security Rules were designed to protect the access, use and disclosure of PHI to support patient privacy. Workforce members may access, use or disclose PHI for the following purposes:

    a. Treatment: Workforce members may access, use, or disclose PHI to perform patient care activities related to providing treatment. This includes communications between caregivers and directly with the patient.
    b. Payment: Workforce members may access, use or disclose PHI when securing payment for treatment provided to a patient. This may include such activities as coding, billing, claims processing, communications with insurance companies, etc.
    c. Health Care Operations: Workforce members may access, use or disclose PHI when conducting activities that support the provision of patient care or securing payment provided. Such activities may include quality improvement, ongoing quality assurance, medical review, auditing activities, etc.

3. There are a number of additional "permissible" allowances for accessing, using or disclosing PHI to support public health functions or are otherwise required by law. Such permissible allowances are described in various policies and procedures specific to each use or disclosure permitted by the HIPAA regulations.

4. Workforce members may only access, use or disclose PHI where necessary to perform their job duties. Any access, use or disclosure of PHI that are not directly related to a workforce member's job duties could constitute a breach of patient information and trigger a reporting obligation to the patient and the Office for Civil Rights and could result in disciplinary action, up to termination, to the workforce member accessing such information.

5. Workforce members may not email patient or personally identifiable information to their own personal email account from their NOAH email, even for a legitimate business purpose. Additionally, Workforce members may not email patient or personally identifiable information using their personal email accounts accessed on a NOAH computer or device.

6. Any access, use or disclosure of PHI made by a workforce member whose intent is to satisfy one's curiosity or for malicious intent will result in disciplinary action up to termination of the individual's relationship with NOAH or removal of access to NOAH EMR systems. For more information related to enforcement of the Privacy Rule requirements at NOAH, please see procedure titled Sanctions for HIPAA Violations.

7. Access, use or disclosure of PHI should not exceed the time frame in which such access is required to perform a workforce member's specified job duty. For example, if a medical assistant is assigned to participate in the care of a patient, the medical assistant may access, use or disclosure patient information to fulfill treatment-related activities during the course of providing that care. Once the medical assistant is no longer assigned to participate in that patient's care, further access, use or disclosure may not occur unless for a specific job duty (e.g., documenting in the patient's chart after care is provided). Further access, use or disclosure of the patient's information is not allowed even if made with good intentions.

8. Workforce members may not access, use or disclose patient information of family members, friends or co-workers unless such access, use or disclosure is necessary to perform the individual's job duties. Workforce members may not use the EHR to access an employee’s or patient’s demographic information including age, DOB, address, etc. that does not specifically relate to their job duty. Any use other than those required to perform the individual's job duties could be considered a privacy breach and result in disciplinary action up to termination or removal of access to NOAH EMR systems.

9. Workforce members may not access their own patient information directly through the electronic medical record systems for which they have access to perform their job duties. This also includes additional job duties such as scheduling/canceling appointments, processing a referral, etc. If workforce members would like to obtain their own patient information, they may use the MyChart function available to all patients. They may also request the information directly through the Health Information Management (HIM) Department or from their personal physician. Accessing one's own patient information directly may result in disciplinary action up to termination.

10. Workforce members may not use their personal device, including but not limited to a cell phone, tablet, or digital camera, to take pictures of PHI. This includes taking pictures of a

patient (or any part of a patient even if it does not identify the patient), documents containing PHI, computer monitors displaying PHI, screen shots of any information containing PHI, or any other use of a personal device that stores, captures or transmits an image that contains PHI.

11. Workforce members may not use their personal device, including but not limited to a cell phone or tablet to send texts containing PHI. Capture of PHI through texts may only be conducted on a Workforce Member's personal device through a NOAH approved application (e.g., Spectrum SD texting) designed to store, maintain, or transmit PHI.

12. Any questions or concerns related to the appropriate access, use or disclosure of PHI should be directed to Human Resources and/or Compliance departments for clarification or investigation, as appropriate. Workforce members should not investigate any suspected violations. For example, if a manager suspects an employee has been in their own chart or a family members chart, the manager should not investigate and go into those charts of the employee or family members. Any suspected violations of inappropriate access, use or disclosure should be immediately reported to Human Resources, Information Technology and/or Compliance or through the Compliance Line service. All workforce members are responsible for safeguarding all patients' privacy.

13. The Information Technology team will conduct regular audits on access to PHI by workforce staff. This may include and is not limited to employees accessing employees PHI, employees "breaking the glass" to access patient charts, employees accessing same last name patients, etc. The Information Technology team will investigate along with Human resources and/or Compliance any audit results that reveal possible inappropriate access conducted by an workforce team member.

Routine Uses and Disclosures

1. NOAH will ensure that workforce members comply to the minimum necessary standard for routine uses and disclosures of PHI related to treatment, associated payments, or health care operations for patient care. For all uses, disclosures, and requests, NOAH may not include an entire medical record, except when the use, disclosure, or request specifically requires it as reasonably necessary to accomplish the intended purpose. Workforce members will be trained, on ways they must limit the disclosures they make, through their security training and may face sanctions if they disclose more information than is required.

2. Workforce members will be responsible for reviewing uses and disclosures prior to performing them, to ensure that only the minimum necessary amount of PHI is included for the specific purpose of the use, disclosure, or request. Workforce members should contact their IT Director, Security Officer, CMIO if they have any questions or concerns about specific disclosures.