PARTNERSHIP FOR ACHIEVING TOTAL HEALTH
Greater New Orleans Health Information Exchange

Section: HIPAA		**Subject:** USER ACCESS CONTROL POLICY		
Controls Addressed:	**Regulations**	**Controls**		
	Security (A)	45 CFR 164.308(a)(4) , 45 CFR 164.502(b) , 45 CFR 164.514(d)		
Applies to: ☐ LPHI ☒ PATH ☐ Business Partner		**Effective from:** 5-20-2014	**Revised on:** 1-16-2019	**Page** 1 of 4
Approved: 1/16/2019				

I. PURPOSE

The User Access Control Policy aims to ensure that the GNOHIE, which is administered by PATH, and its participating members (the "Participant" or "Participants") comply with all applicable laws in allowing Authorized Users (as defined in definitions, and Terms and Conditions) to view protected health information. This policy also reinforces adherence to the HIPAA Security Rule [45 CFR Part 160 and Subparts A and C of Part 164] for e-PHI. Establishing protocols related to Authorized User access of PHI is essential to build trust among members and remain in compliance with federal and state laws.

II. SCOPE

This policy applies to use of the GNOHIE and the data stored within the GNOHIE by Participants and the transmission of e-PHI from Participants to the GNOHIE.

III. POLICY STATEMENT

1) The GNOHIE shall periodically, or upon request, provide a user access log to the Participant, and it is the responsibility of the Participant to notify PATH of an occurrence of misuse or accounts that should be suspended or revoked.

2) Each Participant shall notify their account manager or GNOHIE Staff within seven (7) business days of an Authorized User who is no longer employed or contracted by the respective Participant.

3) All passwords must be changed every 90 days, as appropriate, or immediately upon any breach of the company's security system that is known to the Security Officer

4) The transmission of e-PHI by Participants to the GNOHIE shall be HIPAA-compliant.

5) A patient's consent status affects the ability of the GNOHIE to send Data Services to a Participant. The following table outlines the rules:

Consent Status	Patient Data Sent?
Yes (i.e., opted in)	Yes
No (i.e., opted out)	No
Unknown (i.e., No consent status)	No

Definitions:

Audit: defines the ability of GNOHIE Staff, or other business associates, may inspect and review any or all user access logs for any reason, including but not limited to the following:

- Participant requests;
- Patient complaints; and
- GNOHIE user access review.

Authorized User(s): means a Participant or an individual who has been authorized by a Participant to access data via the GNOHIE in accordance with the Terms and Conditions and the Policies and Procedures listed on the GNOHIE website.

Direct Mail (or Direct Protocol): is a technical standard for exchanging health information between health care entities within a trusted network. Direct Mail is approved for use by nationally recognized experts and organizations. Direct Mail utilizes security measures to ensure that messages are only accessible to the intended recipient, per the protection regulations of the Health Insurance Portability and Accountability Act (HIPAA).

ePHI: refers to electronic protected health information.

GNOHIE: means the Greater New Orleans Health Information Exchange.

GNOHIE Staff: is a GNOHIE employee that administers and grants access to Participant's employees, who are designated Authorized Users.

PATH: means Partnership for Achieving Total Health and is the managing organization of the GNOHIE.

PHI: refers to protected health information.

Provider: is a person working for a Participant who provides health care to patients on behalf of the Participant.

Site: is the location where a Provider treats patients and where data may originate to populate the GNOHIE.

IV. ASSOCIATED POLICIES / AGREEMENTS

- Member BAA
- Patient Consent Policy
- Opt-out Consent Attestation
- Breach Notification Policy
- Data Use, Retention and Disclosure Policy