HUMAN RESOURCES POLICY/PROCEDURE	
OFFICE OF PRIMARY RESPONSIBILITY: **Human Resources**	**EFFECTIVE DATE: 10/22/26** **Revision Date:** **Replaces: Health Insurance Portability and Accountability Act (HIPAA) Policy (HR-044)**
SUBJECT: Health Insurance Portability and Accountability Act (HIPAA)	
Approved By **Tiffany Homler Hawkins** **Chief Executive Officer, LYNX**	

SCOPE:

This Policy is implemented in accordance with the Authority's Administrative Rule 3 which governs Human Resources. With respect to Authority employees who hold positions represented by the Amalgamated Transit Union (Local 1749 and Local 1596), to the extent there is a discrepancy between a policy or practice in this Policy, or a separate governing Administrative Rule, and a provision within the operative collective bargaining agreement ("CBA"), the CBA shall prevail only with respect to specific provisions relating to an employee represented through such an agreement.

POLICY:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), is a federal law intended to strengthen the privacy and security of individuals' health information. HIPAA applies to "covered entities," as defined under the privacy, security, breach notification, and enforcement rules at 45 C.F.R. Part 160 and Part 164 ("HIPAA Rules"). HIPAA covered entities include health plans, health plan clearinghouses, and health care providers that transmit health information electronically in certain types of transactions.

Designation as a Hybrid Entity

A single legal entity that conducts both HIPAA-covered and non-covered functions may designate itself as a hybrid entity for HIPAA compliance purposes. The Central Florida Regional Transportation Authority (hereinafter "Authority") may perform certain activities or functions that bring them within the definition of a covered entity for HIPAA purposes. The Authority therefore chooses to invoke hybrid entity status and must designate and document as its "health care components" those components within the Authority that would meet the definition of a covered entity if they were a single legal entity.

Although the Authority is responsible for HIPAA oversight, compliance, and enforcement requirements, as applicable, the HIPAA Rules apply only to the Authority's designated health care components.

This HIPAA Hybrid Entity Policy specifically addresses the requirements of 45 C.F.R. Sections 164.103 and 164.105, which involve organizational requirements for hybrid entities under HIPAA, among other issues.

1. Designation of Employee Group Health Plan as a Health Care Component

1.1 The Authority has designated its employee group health plan as a health care component based on one or more of the following factors:

- The employee group health plan would meet the definition of a covered entity if it were a separate legal entity.
- The employee group health plan would meet the definition of a business associate if it were a separate legal entity.
- The employee group health plan may perform covered functions.

2. Required Safeguards

2.1 The Authority shall ensure that its employee group health plan complies with the HIPAA Rules, as applicable. In particular, the Authority shall ensure that:

(a) Its employee group health plan does not disclose protected health information to another component of the Authority in a manner that would be prohibited under the HIPAA Privacy Rule (45 C.F.R. Part 164, Subpart E) if the employee group health plan and other component were separate legal entities;

(b) The employee group health plan protects electronic protected health information regarding other components of the Authority to the same extent that they would be required to protect this information under the HIPAA Security Rule (45 C.F.R. Part 164, Subpart C) if the employee group health plan and other components were separate legal entities; and

(c) If a person performs duties as a workforce member for both the Authority's employee group health plan and non-health care components in the same capacity, the person does not use or disclose protected health information created or received in the course of (or incident to) the person's work for the employee group health plan in a way that is prohibited under the HIPAA Privacy Rule (45 C.F.R. Part 164, Subpart E).

2.2 The Authority shall comply with HIPAA's requirements concerning compliance and enforcement (45 C.F.R. Part 160, Subpart C).

2.3 The Authority shall comply with requirements under the HIPAA Privacy Rule and Security Rule regarding implementation of compliance policies and procedures (45 C.F.R. §§ 164.316(a) and 164.530(i)).

2.4 The Authority shall ensure compliance with requirements under the HIPAA Privacy Rule and Security Rule regarding business associate arrangements and other organizational requirements (45 C.F.R. §§ 164.314 and 164.504).

3. Workforce Training

3.1 The Authority will train all workforce members who perform job duties associated with the Authority's employee group health plan on its privacy policies and procedures. The Privacy Officer will develop training schedules and programs so that all required workforce members receive the training necessary and appropriate to permit them to carry out their functions within or on behalf of the Authority's employee group health plan. Newly hired workforce members will be trained within 30 calendar days of joining the Authority. Subsequent training will occur promptly after any material change in these policies and procedures for employees affected by the material change, and all workforce members shall undergo annual refresher training.

3.2 Workforce members undergoing training on the employee group health plan's privacy policies and procedures will be required to document their participation in training sessions. Documentation shall include the date of the training, the participant's name, and the participant's signature. The Privacy Officer shall keep a record of training sessions for six years from the date of training.

3.3 Workforce members shall also be requested to sign an Employee Confidentiality Agreement/Privacy Policy Acknowledgement affirming their obligation to maintain the confidentiality of all PHI of employee group health plan participants.

3.4 The Privacy Officer shall maintain copies of Confidentiality Agreement/Privacy Policy Acknowledgements for six years from the date of execution. Upon termination of employment or access to PHI, whichever is earlier, each Workforce Member shall be reminded of their continued obligation to maintain the confidentiality of all PHI of employee group health plan participants. The Privacy Officer shall maintain copies of Confidentiality Agreement/Privacy Policy Acknowledgements for six years from the date of execution.

3.5 If a HIPAA Workforce Member fails to undergo necessary training within the applicable timeframe, the HIPAA Workforce Member may be able to apply for a position that does not require access to PHI, should another position exist, or appropriate corrective action (up to and including termination of employment) may be taken.

4. Employee Health Records

4.1 Through its human resources office, the Authority maintains employee health records in its capacity as an employer. Employee health records are expressly excluded from the definition of protected health information under the HIPAA regulations, and the human resources office is not one of the Authority's designated health care components.

5. Recordkeeping Requirement

5.1 The Authority shall retain documentation evidencing the designation of its employee group health plan as a health care component for at least six years from the date of any decision to remove the employee group health plan's designation as a health care component. Otherwise, the Authority shall retain documentation evidencing health care component designation indefinitely.

6. HIPAA Privacy Officer

6.1 The Authority has appointed the Senior Human Resources Generalist handling benefits and retirement as the Authority's HIPAA Privacy Officer for its health care components. For any

questions regarding the Authority's compliance with the HIPAA Rules and their implementing regulations concerning the employee group health plan, please contact the HIPAA Privacy Officer at privacyofficer@golynx.com.

7. Consequences of Failing to Follow Hybrid Entity Policy

7.1 An individual who fails to comply with this policy may be subject to sanctions, up to and including disciplinary action, suspension, employment termination, or legal action.