| HUMAN RESOURCES POLICY/PROCEDURE | |
|---|---|
| **OFFICE OF PRIMARY RESPONSIBILITY:**<br><br>**Human Resources** | **EFFECTIVE DATE: 10/22/26**<br>**Revision Date:**<br>**Replaces:** |
| **SUBJECT: Business Associate Policy** | |
| Approved By<br><br>**Tiffany Homler Hawkins**<br>**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 Central Florida Regional Transportation Authority (hereinafter "Authority") will enter into business associate agreements in compliance with the relevant provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended. The Authority will allow its business associates to create, receive, maintain, or transmit protected health information (PHI) on its behalf, if the Authority obtains satisfactory written assurance that the business associate will appropriately maintain the privacy and security of the PHI and fulfill HIPAA business associate obligations.

HIPAA was amended by the American Recovery and Reinvestment Act of 2009 (ARRA), to provide that business associates must adopt 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316 (Administrative, Physical, and Technical Safeguards, and related documentation of policies and procedures). These procedures reflect the requirements of ARRA.

**1. Procedures**

1.1 The Authority will enter into business associate agreements in compliance with the relevant provisions of HIPAA, as amended, to establish the permitted and required uses and disclosures of PHI. These business associate agreements must be entered into following the specifications of 45 C.F.R. § 164.504(e).

1.2 Business associates include (other than a member of the workforce of the Authority): anyone who provides a service on behalf of the Authority that involves creating, receiving, maintaining, or transmitting PHI for a function or activity regulated by the HIPAA Privacy Rule, including claims processing or administration, cloud service providers, data analysis, processing or administration, utilization review, quality assurance, certain patient safety activities, billing, benefit management, practice management, and repricing; or a person who provides legal, actuarial, accounting, consulting, data aggregation, research, management, administrative, accreditation, IT support, or financial services to the Authority. Subcontractors that create, receive, maintain, or transmit PHI on behalf of a business associate also are business associates. In addition, if the Authority conducts business with a contractor that provides data transmission services of PHI and requires access to such information (for example, Health Information Exchange; Regional Health Information Organization or e-Prescribing Gateway) or a vendor that allows the Authority to offer workforce members access to a Personal Health Record, that contractor will be treated as a business associate.

At a minimum, persons and organizations that provide the following types of services involving the use or disclosure of PHI to or on behalf of the Authority are considered business associates:

- Health care clearinghouse.
- Fundraising or marketing entity.
- Data analysis or data aggregation of any kind, including services that de-identify PHI.
- Professional services, such as consulting, legal, accounting, auditing, actuarial, management or administration, or financial.
- Accreditation.
- Electronic data processing, including hardware and software maintenance.
- Photocopying medical records and other sources of PHI.
- Document shredding.
- Repricing (such as services performed by a preferred provider organization (PPO) to apply negotiated discounts to claims).
- Storage of PHI, whether in paper or electronic form.
- Outsourcing services, such as billing or collections.
- Website hosting.
- Collection of PHI from patients.
- Claims-related external review activities.
- Vendor of PHI for Central Florida Regional Transportation Authority.
- Health Information Exchange Organization.
- Regional Health Information Organization.
- E-Prescribing Gateway.
- Other persons that facilitate data transmissions for PHI and that require routine access to PHI.
- Persons that offer a personal health record to one or more individuals on behalf of the Authority.

1.3 No member of the Authority's workforce is permitted to disclose PHI to a business associate or subcontractor (collectively, BA), or to allow a BA to obtain PHI on behalf of the Authority unless a written contract (or other written arrangement) has been executed between the and the BA. This agreement/written document must include provisions that meet the standards listed in this policy.

## 2. Obligations and Activities of BA

2.1 Use and Disclosure Obligations: A BA must not use or further disclose PHI other than as permitted or required by the BA agreement or as required by law.

2.2 Reporting Obligation: Upon report of an unauthorized use or disclosure of PHI or other material breach of the BA agreement, the Authority will initiate appropriate action up to, and including, the termination of services of the BA or vendor and/or reporting of the breach to the Secretary of the U.S. Department of Health and Human Services (Secretary). The Authority's Privacy Officer will determine the level of sanction required for a particular breach.

2.3 Contractors that do not require PHI in order to fulfill their contractual responsibilities to the Authority are not considered BAs. However, because such Contractors may encounter PHI incidentally in the process of performing their duties under their contracts, and because the Authority has a duty to safeguard PHI, all Authority contracts for services will contain a basic confidentiality clause.

## 3. BA Agreements

3.1 The BA must sign the BA agreement prior to performing any services. No access to PHI will be allowed, no account will be set up, and no money will be paid for products or services until the contract is signed.

3.2 Contract renewal will be monitored for continued HIPAA compliance by the Authority's Privacy and Security Officer.

## 4. BA Agreement Provisions

The contract between the Authority and a BA must provide that the BA will:

4.1 Use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for in the agreement. The BA will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the Authority;

4.2 Ensure that any agents, including subcontractors, to whom it provides PHI, agree to abide by the same restrictions and conditions that apply to the BA with respect to PHI, and to implement reasonable and appropriate safeguards to protect it;

4.3 Report to the Authority any use or disclosure of PHI not provided for under the agreement and any security incident, as defined by HIPAA, of which it becomes aware;

4.4 Mitigate, to the extent practicable, any harmful effect that is known to the BA of a use or disclosure of PHI by the BA in violation of the requirements of the agreement;

4.5 Authorize termination of the agreement by the Authority, if the Authority determines that the BA has violated a material term of the agreement;

4.6 Document such disclosures of PHI and information related to such disclosures as would be required for the Authority to respond to a request by an individual for an accounting of disclosure of PHI in accordance with 45 C.F.R. § 164.528;

4.7 Charge fees related to providing individuals access to their PHI in accordance with 45 C.F.R. § 164.524(c)(4);

4.8 Make available to the Authority, in a time and manner designated by the Authority, information necessary for the Authority to give individuals their rights of access, amendment, and accounting in accordance with HIPAA. The BA also must agree to incorporate any amendments made or agreed to by the Authority with respect to PHI in the possession of the BA;

4.9 Report to the Authority any breach of unsecured PHI within five (5) business days of "discovery" in accordance with the Health Information Technology for Economic and Clinical Health (HITECH) Act. Such notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by BA to have been, accessed, acquired, or disclosed in connection with such breach;

4.10 Provide any additional information reasonably requested by Central Florida Regional Transportation Authority for purposes of investigating the breach and any other available information that the Authority is required to include to the individual under 45 C.F.R. § 164.404(c) at the time of notification or promptly thereafter if information becomes available. A BA's notification of a breach of unsecured PHI must comply in all respects with each applicable provision of Section 13400 of Subtitle D (Privacy) of the ARRA and related guidance issued by the Secretary from time to time;

4.11 Agree to provide notification of any breach of unsecured PHI to individuals, the media (if applicable), the Secretary, and/or any other parties as required under HIPAA, the HITECH Act, ARRA, and the regulations thereunder, subject to the prior review and written approval by Central Florida Regional Transportation Authority of the content of such notification;

4.12 Agree that in the event of the BA's use or disclosure of unsecured PHI in violation of HIPAA, the HITECH Act, or ARRA, the BA bears the burden of demonstrating that notice as required to the Authority was provided, including evidence demonstrating the necessity of any delay, or that the use or disclosure did not constitute a breach of unsecured PHI;

4.13 Comply with an individual's request to restrict the disclosure of their personal PHI in a manner consistent with 45 C.F.R. § 164.522, except where such use, disclosure, or request is required or permitted under applicable law;

4.14 Agree that when requesting, using, or disclosing PHI in accordance with 45 C.F.R. § 164.502(b)(1) that such request, use, or disclosure shall be limited to the minimum extent necessary, including the use of a "limited data set" as defined in 45 C.F.R. § 164.514(e)(2), to accomplish the intended purpose of such request, use, or disclosure, as interpreted under related guidance issued by the Secretary from time to time;

4.15 Make its internal practices, books, and records, including policies and procedures regarding PHI, relating to the use and disclosure of PHI and breach of any unsecured PHI received from the Authority, or created or received by the BA on behalf of the Authority, available to the

Authority (or the Secretary) for the purpose of the Authority (or the Secretary) determining compliance with the HIPAA Privacy Rule (as defined in 45 C.F.R. Part 160 and Subparts A and E of Part 164);

4.16 Maintain and document disclosures of PHI and breaches of unsecured PHI and any information relating to the disclosure of PHI and breach of unsecured PHI in a manner as would be required for the Authority to respond to a request by an individual or the Secretary for an accounting of PHI disclosures and breaches of unsecured PHI;

4.17 Provide to the Authority, or to an individual at the Authority request, any relevant information collected by the BA, to permit the Authority to respond to a request by an individual or the Secretary for an accounting of PHI disclosures and breaches of unsecured PHI;

4.18 Account for any disclosure of PHI used or maintained as an electronic health record (EHR) in a manner consistent with 45 C.F.R. § 164.528 and related guidance issued by the Secretary from time to time; provided that an individual shall have the right to receive an accounting of disclosures of EHR by the BA made on behalf of the Authority only during the three years prior to the date on which the accounting is requested [from the Authority /directly from the BA;]

4.19 Comply with the "Prohibition on Sale of Electronic Health Records or Protected Health Information," as provided in Section 13405(d) of Subtitle D (Privacy) of ARRA, and the "Conditions on Certain Contacts as Part of Health Care Operations," as provided in Section 13406 of Subtitle D (Privacy) of ARRA and related guidance issued by the Secretary from time to time;

4.20 Acknowledge that, as of the effective date of the Agreement, it shall be liable under the civil and criminal enforcement provisions set forth at 42 U.S.C. §§ 1320d-5 and 1320d-6, as amended, for failure to comply with any of the use and disclosure requirements of the agreement and any guidance issued by the Secretary from time to time with respect to such use and disclosure requirements;

4.21 To implement administrative safeguards set forth at 45 C.F.R. § 164.308, the physical safeguards set forth at 45 C.F.R. § 164.310, the technical safeguards set forth at 45 C.F.R. § 164.312, and the policies and procedures set forth at 45 C.F.R. § 164.316 to reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the Authority as required by the HIPAA Security Rule (as defined in 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316). Acknowledge that, (i) the foregoing safeguards, policies, and procedures requirements apply to the BA in the same manner that such requirements apply to the Authority, and (ii) the BA is liable under the civil and criminal enforcement provisions set forth at 42 U.S.C. §§ 1320d-5 and 1320d-6, as amended from time to time, for failure to comply with the safeguards, policies, and procedures requirements and any guidance issued by the Secretary from time to time with respect to such requirements;

4.22 Require that any agent, including a subcontractor, to whom it provides such PHI agrees to implement reasonable and appropriate safeguards to protect the PHI;

4.23 Retain the documentation required by the agreement for six years from the date of its creation or the date when it last was in effect, whichever is later;

4.24 Termination for Cause. If either party discovers a material breach by the other party, the breaching party will have the opportunity to cure the breach or end the violation. If the breaching party does not cure the breach or end the violation within a reasonable time not to exceed thirty (30) days from the notification of the breach, or if a material term of the agreement has been breached and

a cure is not possible, the non-breaching party may terminate the agreement, upon written notice to the breaching party;

4.25 Return all of the PHI received from the Authority, or created or received by the BA on behalf of the Authority, to the Authority, in a format that preserves the PHI's accessibility and usability, upon termination of the agreement. All PHI that cannot be returned shall be destroyed. This requirement also applies to all PHI that is in the possession of agents or subcontractors of the BA. The BA, including its agents and subcontractors, should not retain any copies of the PHI. If the BA determines that returning or destroying the PHI is not feasible, the BA will provide Central Florida Regional Transportation Authority has agreed that the BA agreement will be subject to such indemnification provisions, then the Authority should ensure that it is specifically indemnified in the BA agreement for particular breaches of the agreement, such as failure to comply with the breach notification requirements. Otherwise, the Authority should be indemnified in the BA agreement for claims arising out of the BA's breach of the agreement, negligence, or wrongful acts or omissions by the BA or its agents or subcontractors.