	SECURITY AND PRIVACY REQUIREMENTS FOR L.A. CARE HEALTH PLAN BUSINESS ASSOCIATES	**CMPP-036**

DEPARTMENT	COMPLIANCE – PRIVACY
Supersedes Policy Number(s)	

DATES					
Effective Date	7/15/2024	Review Date	7/15/2024	Next Annual Review Date	7/15/2025
Legal Review Date	8/1/2024	Committee Review Date	8/1/2024		

LINES OF BUSINESS

☒ Medicare D-SNP ☒ L.A. Care Covered ☒ L.A. Care Covered Direct ☒ MCLA
☒ PASC-SEIU Plan ☒ Internal Operations

DELEGATED ENTITIES / EXTERNAL APPLICABILITY

☐ PP – Mandated ☐ PP – Non-Mandated ☐ PPGs/IPA ☐ Hospitals
☐ Specialty Health Plans ☐ Directly Contracted Providers ☐ Ancillaries ☐ Other External Entities

ACCOUNTABILITY MATRIX			
Information Security	§§ 3.1, 4.1		
Health Care Legal Services	§§ 3.1, 4.1		

ATTACHMENTS

- Provider/Vendor Attestation (Offshore Subcontractor Access to Protected Health Information/Member Information)

ELECTRONICALLY APPROVED BY THE FOLLOWING		
	OFFICER	**DIRECTOR**
NAME	Todd Gower	Serge Herrera
DEPARTMENT	Compliance	Compliance
TITLE	Chief Compliance Officer	Director/Privacy Unit

AUTHORITIES
➢ Code of Federal Regulation, Title 42, Sections 422.504 and 423.505 ➢ Code of Federal Regulations, Title 45, Parts 160 and 164 ➢ Cal Medi-Connect 3-way Agreement ➢ Confidentiality of Medical Information Act (CMIA), California Civil Code 56 - 56.37 ➢ Department of Health Care Services Contract ➢ Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009

REFERENCES
➢ Centers for Medicare and Medicaid Services, Medicare Managed Care Manual (Chapter 21, Section 40.1.3) ➢ Centers for Medicare and Medicaid Services, Prescription Drug Benefit Manual (Chapter 9, Section 20.4.1) ➢ Nation Institute of Standards and Technology (NIST) Special Publication 800.53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations. ➢ Federal Information Processing Standard (FIPS)140-2, Security Requirements for Cryptographic Modules

HISTORY

REVISION DATE	DESCRIPTION OF REVISIONS
07/15/2024	New policy to communicate security and privacy requirements for vendors

1.0 OVERVIEW:

1.1 The purpose of this policy is to provide L.A. Care's expectations for our vendors regarding the protection, privacy, and security of sensitive health information, such as Protected Health Information (PHI), Electronic Protected Health Information (ePHI), and Personal Information (PI) as defined in Section 2.0 below. This policy outlines the regulatory requirements to safeguards our members' information and maintain a strong and secured vendor ecosystem by safeguarding the Confidentiality, Integrity, and Availability of our members' information.

1.2 As a Medicaid managed care contractor, L.A. Care is required to downstream certain requirements applicable to L.A. Care and any vendor that creates, receives, maintains, transmits, uses or discloses L.A. Care PHI/PII.

1.3 Any deviations from this policy shall require express written approval of L.A. Care's Privacy Officer or Chief Information Security Officer, as appropriate.

2.0 DEFINITIONS:

Whenever a word or term appears capitalized in this policy and procedure, the reader should refer to the "Definitions" below.

2.1 **"Breach"** shall have the same meaning given to such term in 45 C.F.R. §164.402 and HITECH §13400.

2.2 **"Business Associate"** shall have the same meaning given to such term under the HIPAA and the HITECH Act, 45 C.F.R. §160.103 and HITECH §13400.

2.3 **"Electronic Protected Health Information" or "Electronic PHI"** shall have the same meaning given to such term under the HIPAA Regulations, including 45 C.F.R. §160.103, as applied to the information that Business Associate creates, receives, maintains or transmits from or on behalf of L.A. Care.

2.4 **"HIPAA Rules"** shall mean the Privacy, Security, Breach Notification and Enforcement Rules at 45 C.F.R. Parts 160 and 164.

2.5 **"HITECH Act"** shall mean the Health Information Technology for Economic and Clinical Health Act (Subtitle D), of the American Recovery and Reinvestment Act of 2009, including its implementing regulations, as such may be amended from time to time.

2.6 **"Offshore"** refers to any country that is not one of the fifty United States or one of the United States Territories. Vendors that are considered Offshore can be either American-owned companies with certain portions of their operations performed outside of the United States or foreign-owned companies with their operations performed outside of the United States. Offshore subcontractors provide services

that are performed by workers located in Offshore countries, regardless of whether the workers are employees of American or foreign companies.

2.7 **"Personal Information"** as defined in the Information Practices Act (IPA) at California Civil Code section 1798.3(a).

2.8 **"Privacy Rule"** shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and Part 164 (Subparts A & E).

2.9 **"Protected Health Information" or "PHI"** shall have the same meaning given to such term in 45 C.F.R. §160.103, as applied to information created or received by Business Associate from or on behalf of L.A. Care.

2.10 **"Security Incident"** shall have the same meaning given to such term in 45 C.F.R. §164.304.

2.11 **"Security Rule"** shall mean the Security Standards at 45 C.F.R. Parts 160 and Part 164 (Subparts A & C).

2.12 **"Unsecured PHI"** shall have the meaning given to such term under the HITECH Act, 42 U.S.C. §17932(h), any guidance issued pursuant to such Act and the HIPAA regulations.

2.13 **"Unsuccessful Security Incidents"** include pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI.

3.0 POLICY:

3.1 L.A. Care vendors that create, receive, maintain, transmit, use, or disclose L.A. Care's PHI/PI must comply with the requirements outlined below.

3.1.1 Business Associate shall, at a minimum, align to the National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Rev 5 compliant security framework when selecting and implementing its security controls and maintain continuous compliance with NIST SP 800- 53 Rev. 5 as it may be updated from time to time.

3.1.2 Business Associate shall employ FIPS 140-2 validated encryption of PHI at rest and in motion unless Business Associate determines it is not reasonable and appropriate to do so based upon a risk assessment, and equivalent alternative measures are in place and documented as such. In addition, Business Associate maintain, at a minimum, the most current industry standards for transmission and storage of PHI and other confidential information.

3.1.3 Business Associate shall apply security patches and upgrades, and keep virus software up-to-date, on all systems on which PHI and other confidential information may be used.

3.1.4 Business Associate shall ensure that all members of its workforce with access to PHI and/or other confidential information sign a confidentiality statement prior to access to such data. The statement shall be renewed annually.

3.1.5 Business Associate shall identify the security official who is responsible for the development and implementation of the policies and procedures required by the Security Rule.

3.1.6 Business Associate shall, within ten (10) calendar days of a written request by L.A. Care, make available to L.A. Care during normal business hours at Business Associate's offices all records, books, agreements and policies and procedures relating to the use or disclosure of PHI/PI for purposes of enabling L.A. Care to determine Business Associate's compliance with the terms of the Business Associate Agreement ("BAA"). In addition, upon reasonable notice, Business Associate shall make its premises, facilities, computer and other electronic systems pertaining to the services provided pursuant to the underlying Agreement with L.A. Care available to L.A. Care during regular business hours for the purposes of L.A. Care determining, investigating or auditing Business Associate's compliance with the Privacy and Security Rules and/or HITECH, subject to any applicable legal restrictions.

3.1.7 To the extent that other State and/or federal laws, including but not limited to the Information Practices Act, California Civil Code §§1798-1798.78, Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. part 2, Welfare and Institutions Code §5328, and Health and Safety Code section 11845.5, provide additional, stricter and/or more protective (collectively, more protective) privacy and/or security protections to PHI/PI or other confidential information covered under the BAA beyond those provided through HIPAA, Business Associate shall:

3.1.7.1 To comply with the more protective of the privacy and security standards set forth in applicable State or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA or are otherwise more favorable to the individuals whose information is concerned; and

3.1.7.2 To treat any violation of such additional and/or more protective standards as a breach or security incident, as appropriate, pursuant to the BAA.

3.1.8 Unless otherwise specified in the Agreement and/or the BAA with L.A. Care pursuant to applicable L.A. Care policies, Business Associate shall not, and shall ensure that any employee, agent, or subcontractor, shall not access, transmit, maintain, export, store or transfer any PHI from or outside of the United States for any purpose whatsoever, whether for access, storage, testing, or processing or otherwise, without the express prior written consent of L.A. Care's Privacy Officer or Chief Information Security Officer. In addition, Business Associate shall not, and shall ensure that any employee, agent or subcontractor shall not, make any PHI available to any entity or individual outside of the United States for any purpose whatsoever, including for access, storage, testing, or processing or otherwise, without the express prior written consent of L.A. Care's Privacy Officer or Chief Information Security Officer.

3.1.9 First Tier, Downstream or Related Entities (FDR) Compliance

3.1.9.1 **Due Diligence.** L.A. Care will evaluate and select vendors and FDRs based on their compliance history, reputation, and ability to meet regulatory requirements.

3.1.9.2 **Contractual Obligations.** Offshore contracts with vendors and FDRs include provisions that require compliance with all applicable state and federal laws, regulations, and contractual requirements.

3.1.9.3 **Training and Education.** Vendors and FDRs are required to provide relevant training and education to ensure offshore workforce understand their obligations and compliance requirements.

3.1.9.4 **Monitoring and Auditing.** Regular audits, site visits, and performance reviews should be conducted to ensure ongoing compliance. Copies of audit results must be shared with L.A. Care to demonstrate compliance.

3.1.9.5 **Initial FDR Provider/Vendor Attestation.** Required prior to offshoring L.A. Care's PHI/PI.

3.1.9.6 **Non-Compliance.** Failure to comply with this policy may result in contractual penalties, termination of Agreement, or other appropriate actions.

3.1.10 PHI/PI are strictly limited for the uses and disclosures to the specific functions, activities, or services outlined in the agreement and solely on behalf of the Medicare/Medicaid programs.

3.1.11 PHI/PI covered under the Agreement cannot be used for commercial purposes such as product development.

3.1.12 Business associate shall not receive direct or indirect remuneration in exchange for PHI/PI.

3.1.13 All PHI/PI and any other data provided by L.A. Care to the Business Associate, including any data that is created, received maintained, or transmitted by the Business Associate on behalf of L.A. Care, shall remain the exclusive property of L.A. Care.

4.0 MONITORING:

4.1 L.A. Care, at its discretion, may submit to Business Associate a detailed questionnaire for the purposes of evaluating whether Business Associate has complied with its obligations under the BAA, HIPAA and applicable laws, including verification of any required certifications or minimum security requirements. Business Associate shall provide written answers to the questionnaire no later than thirty (30) days from the date of L.A. Care's request.

4.2 Audit language. Need right to audit within 30 days of notice. Immediately upon breaches.

4.3 Rights to audit (for all contracts industry standards and if a breach immediate. (onsite/desktop). We reserve the right to use a third party auditor.

5.0 REPORTING:

5.1 Business Associate shall notify L.A. Care in writing of any use or disclosure of PHI not provided for by the Agreement and the BAA of which it becomes aware, including Breaches of Unsecured PHI as required by 45 C.F.R. § 164.410, incidents that pose a risk of constituting Breaches and any Security Incident. Such notifications shall be directed to the attention of L.A. Care's Privacy Officer (email to PrivacyOfficer@lacare.org or another method may be used as agreed to by the Privacy Officer and Business Associate) within twenty-four (24) hours within the work week of discovery.