GENERATIVE ARTIFICIAL INTELLIGENCE USAGE BY SERVICE PROVIDERS

Purpose: This policy establishes minimum requirements for Service Providers using or considering the use of Generative Artificial Intelligence (GenAI) while delivering services funded or overseen by San Andreas Regional Center (SARC). The purpose is to ensure compliance with DDS guidance, protect individual rights and privacy, and maintain person-centered, human- led decision-making. This policy is a material component of the Service Provider's contractual agreement with SARC.

Scope: This policy applies to all SARC-vendored Service Providers and to all GenAI tools, platforms, or software with generative AI functionality used in connection with SARC-funded services or SARC-related administrative, operational, or service activities. Any use of artificial intelligence in connection with SARC services remains subject to all applicable confidentiality obligations, contractual requirements, and federal and state privacy and health information laws, including Health Insurance Portability and Accountability Act (HIPAA), Confidentiality of Medical Information Act (CMIA), and other laws governing Protected Health Information (PHI), Personally Identifiable Information (PII), and SARC- related confidential information.

Definitions:

The following definitions apply to this policy and are intended to align with Department of Developmental Services (DDS) guidance, Technical Bulletin #568, and Reporting Requirements G-2025-004. These definitions are provided to ensure consistent understanding and application by all service providers.

- *Generative Artificial Intelligence (GenAI)* means any artificial intelligence system capable of generating content including text, images, audio, video, data summaries, or recommendations based on patterns learned from existing data. GenAI is intended to support, not replace, human judgment.

- *GenAI Solution* means any software, application, platform, or system that incorporates Generative Artificial Intelligence functionality, whether purchased, licensed, embedded within another product, or accessed via third-party services.

- *Human Oversight* is the requirement that qualified staff review, validate, and take responsibility for all GenAI-generated outputs before they are

used, shared, or relied upon for decision-making. GenAI outputs may inform professional judgment but may not serve as the sole basis for decisions affecting individuals or families.

- *Informed Consent* is a process by which individuals and/or their legally authorized representatives are clearly informed, in understandable language, of when and how GenAI is used, including potential risks and benefits, and are provided the opportunity to consent to or opt out of GenAI-supported activities when applicable.

- *Protected Health Information (PHI)* is any individually identifiable health information that is protected under the Health Insurance Portability and Accountability Act (HIPAA), including but not limited to medical records, service information, diagnoses, and treatment data.

- *Personally Identifiable Information (PII)* is any information that can be used to identify an individual, either alone or in combination with other data, such as name, address, date of birth, contact information, identifiers, or service records.

- *Confidential Information* is any PHI, PII, case notes, assessments, service data, or other sensitive information related to individuals and families served, regardless of format or storage method. This includes any information that, even if de-identified, could be re- identified or used to infer information about an individual or group of individuals served by SARC.

- *Transparency* is the obligation to clearly disclose the use of GenAI in documentation, communications, authorizations, service delivery, or decision-making processes, including identifying when GenAI has contributed to content or recommendations.

- *Accountability* is the responsibility of the service provider and regional center to ensure GenAI tools are used ethically, lawfully, and in accordance with policy, and to remain fully and ultimately liable for all outcomes, decisions, errors, and impacts associated with GenAI use. This accountability cannot be delegated to the AI tool, the AI vendor, or an individual staff member.

- *Bias* means systematic errors or unfair outcomes produced by GenAI systems that may disproportionately impact individuals or groups based on characteristics such as disability, race, ethnicity, gender, age, language, or other protected attributes.

- *Data Handling* means the methods by which data is collected, input, stored, processed, shared, retained, or used for model training or improvement by a GenAI system.

- An *Approved System* is a GenAI Solution that has undergone a formal review by SARC in accordance with this Policy and has been explicitly authorized in writing for use by a Service Provider for specified purposes. A system will only be approved if the Service Provider furnishes sufficient evidence that the solution meets all SARC requirements for data security, privacy, transparency, human oversight, equity, and contractual safeguards, including a contractual prohibition against using any Confidential Information for third- party model training. Approval may be revoked by SARC at any time if the system's compliance with these standards is compromised.

- An *Unapproved System* is any GenAI Solution that has not received written approval from SARC, or for which approval has been revoked. This includes, but is not limited to, all publicly available, free-to-use, or consumer-grade GenAI tools (e.g., standard versions of ChatGPT, Gemini, Copilot) not operating under a HIPAA-compliant Business Associate Agreement and SARC-approved data protection terms. The entry of any Confidential Information into an Unapproved System is strictly prohibited and constitutes a material breach of contract.

- *Role-Based Access* is a security practice that limits access to data and GenAI systems based on an individual's job role and authorized responsibilities.

- *Verified Staff* are staff members who have been formally authorized by the service provider to use or oversee Generative Artificial Intelligence (GenAI) systems. Verified Staff have completed required training on GenAI use, including limitations, risks, privacy protections, and ethical considerations; understand applicable DDS and SARC requirements; and are designated to review, validate, and take responsibility for all GenAI-generated outputs prior to use in documentation, communication, or decision-making. GenAI outputs may not be used by unverified staff.

Policy:

1. General Principles

GenAI may be used only as a supportive tool. It must not replace professional judgment or human decision-making. Any decision that affects an individual must be made and handled by trained, verified staff, together with the individual (and their representative when appropriate).

2. Prohibited Uses

The use of any GenAI Solution for the following purposes is strictly prohibited and constitutes a material breach of the Service Provider's contract with SARC:

a. *Unmonitored Interaction*: Using GenAI for direct, unmonitored interaction or communication with individuals or families.

b. *Critical Decisions*: Relying on GenAI output as the sole basis for any major decision impacting an individual's rights, services, eligibility, health, or well-being.

c. *Surveillance*: Using GenAI for tracking or monitoring individuals.

d. *Unapproved Systems*: Entering any Confidential Information, PHI, or PII into any Unapproved System (including free, public, or consumer-grade AI tools).

e. *Model Training*: Utilizing any GenAI Solution that does not contractually guarantee that Service Provider data will not be used to train or improve any AI model for the benefit of the GenAI vendor or any third party.

3. Privacy and Data Protection

3.1. *Compliance with Law*: All GenAI use must comply with HIPAA, CMIA, CCPA, and all directives and guidance issued by the California Department of Developmental Services ("DDS").

3.2. *Contractual Guarantees*: The Service Provider must furnish a contract or Business Associate Agreement (BAA) from its GenAI vendor that legally guarantees:

a. The GenAI vendor is explicitly prohibited from using any submitted data to train, retrain, or otherwise improve its AI models.

b. Data is logically and/or physically segregated from the data of other customers.

c. Data is encrypted both in transit and at rest.

d. Data is stored within the geographic boundaries of the United States and is not otherwise transmitted to offshore locations.

3.3. *Technical Safeguards*: The Approved System must operate within a HIPAA- compliant environment, provide role-based access controls, and maintain immutable audit logs.

4. Transparency and Informed Consent

4.1. *Duty of Transparency*: When GenAI is used to generate documentation or communications shared with an individual, their family, or SARC, the document must include a clear notice: "This document was prepared with

the assistance of a Generative AI tool and has been reviewed for accuracy and verified by a qualified professional."

4.2. *Informed Consent*:

a. For any process where GenAI directly supports a service or decision-making interaction, the Service Provider must obtain informed consent, explaining risks and benefits in plain language.

b. Use of GenAI to record or transcribe meetings requires appropriate consent before recording, consistent with applicable state and federal law.

4.3. Right to Opt Out: Individuals must be explicitly informed of their right to opt out of GenAI-supported processes without penalty.

5. Human Oversight and Accountability

5.1. *Mandatory Review*: All GenAI-generated content must be subject to substantive review and validation by Verified Staff before it is finalized, shared, or used.
5.2. *Substantive Review Standards*: A review must consist of:

a. *Fact Checking*: Verifying all information against source material to correct errors.

b. *Source Referencing*: Ensuring that GenAI output references the source material used so the user and recipient can reference those documents, as required by DDS Directive: G-2025-Reporting Requirements-004.

c. *Bias Check*: Scrutinizing language for potential bias or inequitable treatment.

d. *Final Approva*l: The Verified Staff member must affirmatively approve the content, assuming full professional responsibility for its accuracy.

6. Training and Competency

Service Providers must implement a mandatory, role-based GenAI training program covering this Policy, DDS guidance, privacy obligations, bias identification, and human oversight. Staff may not use GenAI tools until training is completed.

7. SARC Review and Approval of GenAI Solutions

7.1. Mandatory Pre-Implementation Review. Service Providers are prohibited from implementing any GenAI Solution for SARC-funded services without prior written approval from SARC.

7.2. Submission Documentation. To obtain approval, the Service Provider must submit a "GenAI Solution Review Request" form. SARC's review is documentary in nature: SARC relies on the Service Provider's binding

attestations and submitted contractual documentation (BAAs, Terms of Service) to verify compliance with DDS data protection standards.

8. Contractual Parity and Business Associate Agreement (BAA) Requirements

8.1. Parity of Standards: Pursuant to DDS guidance, Service Providers are contractually obligated to uphold the exact same data protection standards as SARC when implementing GenAI. Compliance with this Policy is a material term of the Service Provider's contract.

8.2. BAA Obligations: All BAAs with GenAI vendors must explicitly prohibit the use of Confidential Information for AI model training.

9. Attestation and Audit Rights

Service Providers must complete an annual attestation of compliance. SARC reserves the right to audit compliance at any time, including review of system logs, training records, and vendor contracts.

Date of Approval: June 11, 2026
Revision: 1st