PETE CERVINKA
DIRECTOR

CALIFORNIA HEALTH & HUMAN SERVICES AGENCY
DEPARTMENT OF DEVELOPMENTAL SERVICES
1215 O Street, Sacramento, CA 95814 • www.dds.ca.gov

GAVIN NEWSOM
GOVERNOR

December 24, 2025 G-2025-Reporting Requirements-004

TO: REGIONAL CENTER EXECUTIVE DIRECTORS

SUBJECT: BEST PRACTICES FOR THE ETHICAL AND RESPONSIBLE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE WITHIN REGIONAL CENTERS

This guidance outlines the best practices for the ethical and responsible use of Generative Artificial Intelligence (GenAI) in regional center and service provider operations. As GenAI technologies become more integrated into commonly used solutions, it is crucial to establish clear guidelines that uphold core values of fairness, dignity, and well-being of the individuals and families served. The purpose of this guidance is to:

- Maximize the benefits of GenAI to improve operational efficiency and enhance service delivery.
- Mitigate the significant risks associated with GenAI, such as bias, privacy breaches, and lack of transparency.
- Allow the use of GenAI as a tool to support, not replace, human judgment and the relationship between individuals and the people who support and serve them.
- Clarify ethical, legal, and privacy obligations in a rapidly evolving technological landscape, as current professional guidelines may not yet fully address GenAI.

Reporting Requirements for GenAI Solutions
Regional centers are required to submit any proposed GenAI solutions to the Department of Developmental Services (Department) for review prior to implementation, and existing systems leveraging GenAI, as outlined in Technical Bulletin #568 (Attachment A). Regional centers need to establish policies and procedures to address use of GenAI solutions by service providers so that any solution used meets all applicable federal and state privacy protections and otherwise complies with this letter, including the components listed below.

Guiding Principles
The use of GenAI must be governed by the following core principles:

- *Person-centered approach*: The well-being and privacy of the individuals and families served are paramount. GenAI tools must be designed and implemented to assist and empower individuals, not to control or marginalize them. The ultimate responsibility for all decisions impacting individuals and families rests with humans.

- *Transparency:* Employees, individuals and families must be informed when and how GenAI is used in authorizing, delivering, and monitoring services. When a GenAI system informs a significant decision, the reasoning behind the algorithm's recommendation should be understandable to the people who are affected.
- *Equity:* GenAI systems must be rigorously tested to mitigate algorithmic bias and achieve equitable outcomes for all populations, regardless of race, gender, religion, or other characteristics. Data used to train GenAI should be diverse and representative to avoid perpetuating systemic inequalities.
- *Privacy and security*: Individuals' data must be protected with the highest level of security. All systems containing protected health information or personally identifiable information must be HIPAA-compliant and only allow role-based access to the information. GenAI adds to the complexity and risk of data leakage and privacy violations.
- Ensure GenAI tools are implemented with contractual and technical safeguards that protect organizational data, restrict access to authorized staff, and prevent any use of data for model training or improvement.
- *Accountability and oversight*: The regional center and service provider are responsible for the performance and outcomes of all GenAI systems they deploy. Robust human oversight is required for any GenAI-driven decisions, with clear procedures for review, intervention, and appeal. All GenAI usage should be auditable.
- *Competence and ongoing evaluation*: Employees must receive comprehensive training on the GenAI tools they use, including their capabilities, limitations, and ethical considerations.
- Continuously monitor and evaluate the performance of GenAI tools, so they remain effective and aligned with best practices.

Practical Guidelines

- *Use GenAI for administrative support:* GenAI may be appropriate for tasks such as summarizing documentation, creating standardized correspondence, or generating educational materials. Human review of the generated product is required before sharing it.
- *Enhance professional judgment*: GenAI outputs may be used to inform professional judgment, but not as a replacement for it. Regional centers and service providers must regularly review the information used to train the GenAI model and critically review all GenAI-generated content for accuracy and relevance before using it. GenAI output should reference source material used so the user and recipient can reference those documents.
- *Practice informed consent*: Always be transparent with individuals and families about the use of GenAI. Explain the risks and benefits in an easy-to-understand way and respect an individual's right to opt out of an GenAI-generated or supported document or process.
- *Follow security protocols*: Establish a clear set of security policies regarding the use of GenAI. This framework should define acceptable use cases and classify data for AI use. It must also assign clear ownership. Building this into existing

compliance policies promotes adherence to well defined enforceable rules. The content of output is another source of issue identification.

- *Verify and fact-check*: Treat all GenAI-generated information with a healthy dose of skepticism. Human review always must check for errors, "hallucinations" (fictitious information), and potential or real biases.

Safeguards

While GenAI offers significant potential for enhancing our work, it also presents risks related to bias, privacy, and accountability. Regional centers and service providers must take measures to mitigate those risks so that GenAI deployment aligns with providing equitable, transparent, and person-centered services. These safeguards apply to all regional centers and GenAI technologies used across platforms, from administrative functions to public-facing applications.

- *Do not use GenAI for direct, unmonitored interaction with individuals and families.* While GenAI could be a great tool to answer questions that today are contained in a lengthy FAQ, it should not be used as a substitute for human-to-human relationships, especially in sensitive situations.
- *Do not rely solely on GenAI for critical decisions*: GenAI output or recommendations never can be the sole basis for a major decision that impacts an individual's rights, services, or well-being.
- *Do not input confidential data into unapproved systems:* This includes names, addresses, health and social services information, and case notes. Use of unvetted, free, or third-party GenAI tools is strictly prohibited.
- *Do not use GenAI for surveillance*: Any use of GenAI for tracking or monitoring individuals is prohibited and violates the human-centered nature of our work.

Service Provider Use of GenAI

Regional centers are required to protect the privacy and security of individuals and families served. The use of GenAI with vendored service providers creates a risk because the AI models might use confidential or sensitive information for training purposes, potentially exposing proprietary or personally identifiable data to unauthorized parties. As such, regional centers must review the terms of Business Associate Agreements, service agreements, and contracts with vendored service providers to include protections for Protected Health Information and Personally Identifiable Information when the provider may be using GenAI. The regional centers must ensure the vendored service providers are contractually obligated to uphold the same data protection standards as the regional center itself, specifying what data can be used, for what purposes, and mandating safeguards to prevent breaches.

The integration of GenAI in human services potentially is a powerful opportunity to augment our work and better serve our community, but comes with serious risks and must be overseen and reviewed by humans for adherence to legal, privacy, and ethical principles and requirements and the maintain the trust of individuals and families. As

GenAI technology continues to evolve, this guidance will be regularly reviewed and updated.

Attachment B contains additional questions and answers. If there are additional questions or additional guidance is needed, please contact the Department's Information Security Office at iso@dds.ca.gov.

Sincerely,

Original Signed by:

AARON CHRISTIAN, Chief
Population Risk, Quality Assurance, and Data Operations

Attachments

Cc: Regional Center Administrators
Regional Center Directors of Consumer Services
Regional Center Community Services Directors
Association of Regional Center Agencies