HHSA Provider Fundamentals

Training for HHSA Providers

County of San Diego- Health and Human Services

Business Assurance and Compliance

April 2026

SANDIEGOCOUNTY.GOV/HHSA

Disclaimer

This slide deck is intended as a resource to assist HHSA providers with common topics related to their contractual requirements. This slide deck is not intended to be a comprehensive set of contract requirements nor legal advice. For a comprehensive description of your contractual requirements, review your contract language.

Provider Fundamentals

Who are we and what do we do?

- We are HHSA's Business Assurance & Compliance Department (BAC).
- We work to ensure that the County and its' providers are following local, State and Federal guidelines.
- We also serve as a privacy and confidentiality resource to the County and its' providers.
- We've got your **BAC**!
- To learn more about what we do, visit our website: www.cosdcompliance.org

Provider Fundamentals

- These slides will be covering parts of your service agreement with the County that pertain to compliance, privacy, and confidentiality.
- These slides are a broad overview of these topics, so you should also visit BAC's website where we have resources specifically for Providers.
- Additional Provider resources can be found here:
  Provider Resources

Provider Template

Common Compliance Sections:

- Hotline Poster (Article 10.6)
- Background Checks (Article 10.11)
- Use of Artificial Intelligence (Article 10.13)
- Conflict of Interest (Article 11.1)
- Exclusion, Debarment, and Medi-Cal Checks (Article 12.16)
- False Claims Act (Article 12.17)
- Privacy and Security Provisions (Article 14)

Hotline Posters (10.6)

- As a Provider, you are required to post hotline posters, which will let staff know where to call if they have an ethics complaint / report.
  - These posters can be posted in common work areas, or anywhere an employee can quickly access the info, such as:
    - break rooms
    - kitchens
    - meeting area
    - near the clock-in machine (if that is used)
    - company intranet or internet site
  - If working remotely, you can also email the posters out to staff or keep it in a shared folder.

Ethics Hotline Poster English

Ethics Hotline Poster Spanish

Background Checks (10.11)

Who am I required to run a background check on? What if I receive a result?

Background checks are required for all workforce members who work on the County contract, regardless of whether they will have access to client info (accountants, volunteers, interns, etc). A result on a background check does not automatically disqualify an individual from working on a County contract, but this should be handled on a case-by-case basis with provider accessing risk to operations.

What kind of documentation is good to keep?

In the event of an audit, the County may ask to see your policy for ordering and reviewing background checks, a record that they were completed and for whom, and who gave the review and signed off on the background checks.

Background Checks (10.11)

What is subsequent arrest notification (SAN)? Am I required to apply?

One option to meet the background check requirement is using SAN by applying for a Livescan Account with the Department of Justice. With SAN, you will receive a notification of an arrest within a week of the occurrence. With regular background checks, a result of an arrest may take months to appear on someone's record. Some organizations use vendors to complete background checks. **However, the County does not dictate to you or recommend how you should complete background checks**. The requirement is only for at-hire and annual checks.

More Background check resources:

Background Check Requirements for HHSA Providers

Background Checks & Subsequent Arrest Notification FAQs

Use of Artificial Intelligence (AI) (10.13)

- Compliance with Board Policy A-140 is required.
- Any AI functionality embedded in products or services rendered under your Contract must be disclosed.
- All AI tools used must comply with County standards for security, privacy, and ethical practices.
- Human oversight of AI-generated output for contract-related services is required.
- AI-generated content must be clearly attributed.
- AI systems shall not be used for:
  - Fully automated decisions without meaningful human oversight
  - Covert tracking
  - Social scoring
  - Behavioral manipulation

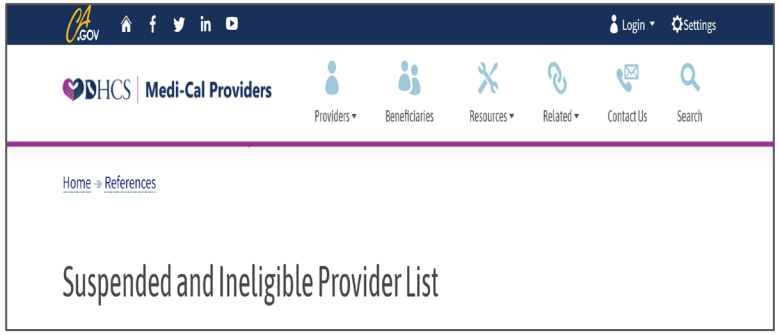
Exclusion, Debarment, & Medi-Cal Checks (12.16)

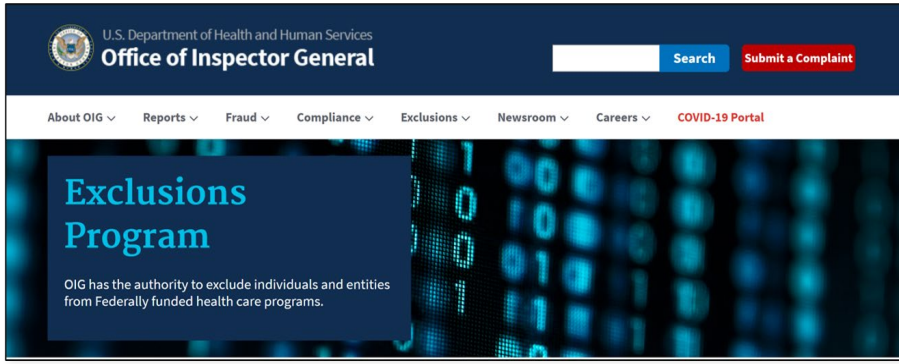
What is an EDM check?

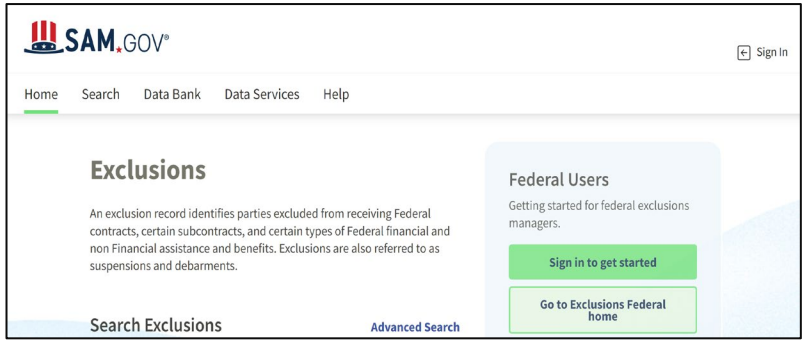
The Exclusion, Debarment and Medi-Cal (EDM) check reviews 3 databases (2 Federal, 1 State) for individuals who are excluded from working on government contracts. As a provider, it is your responsibility to check these three databases monthly to see if any of your employees' names are in any of these databases.

Who gets checked?

Just like with background checks, this check applies to all employees working on County contracts, paid or unpaid.







Exclusion, Debarment, & Medi-Cal Checks (12.16)

What kind of documentation is good to keep?

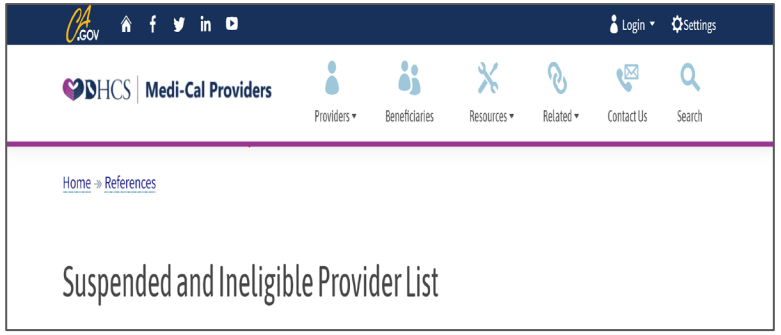
The County will not normally ask you to keep documentation of every EDM check you complete every month. However, the County may ask to see documentation or data to provide assurance that checks for all staff working on County contracts are cleared monthly. Please work with your COR to determine exactly what kind of documentation may be requested.

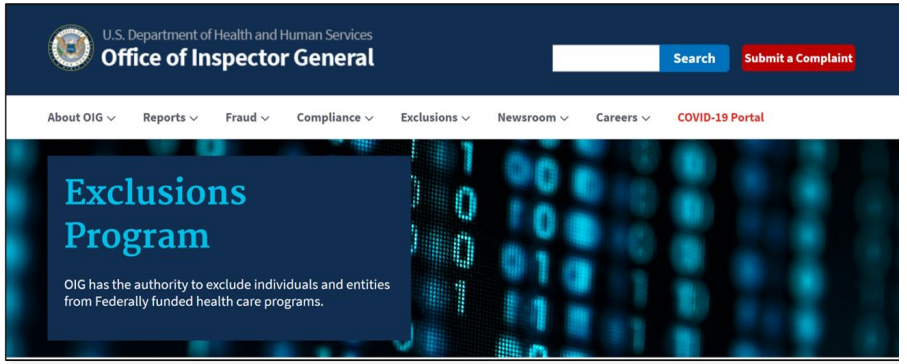
More EDM check resources:

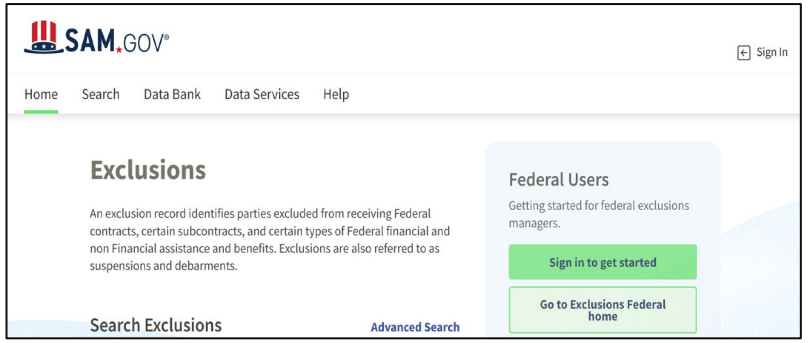
[Exclusion, Debarment, & Medi-Cal Sanction Checks Requirements for HHSA Providers]

[Exclusion, Debarment, & Medi-Cal Sanction Checks Helpful Hints for HHSA Providers]

[Exclusion, Debarment & Medi-Cal Sanction Checks FAQ]







Privacy, Confidentiality, and Data Security (Article 14)

Annual Article 14 monitoring tool:

- Article 14, the Information Privacy and Security Provisions Article, is a collection of clauses that protect private data and information.
- It is the HHSA-approved set of provisions that encompass Federal and State requirements related to the Privacy and Security of Protected Information.
- It has three sections, including the privacy and security requirements established under the Health Insurance Portability and Accountability Act (HIPAA) as well as applicable State requirements.
- Know your State Agreement requirements (not just HIPAA).

More info about Article 14 and the requirements for handling data (how to store, transfer information, encryption, etc.) can be found here:

HHSA: Priv and Sec. FAQs

HHSA: Article 14 and state agreements

Privacy Incident Reporting

- As a Provider, you need to report violations of privacy requirements to the County.
- Breaches or suspected security incidents must be reported within one business day.
- While most reporting happens within 24 hours of the incident, some need to happen immediately upon discovery (500 or more individuals involved).
- Reports may be accompanied by a Serious Incident Report to COR.

Access our Privacy and Security Incident Reporting system (PIRD), where you can submit these privacy reports here:
Submit a Privacy Incident Report

Please keep your COR informed of all privacy incidents as you submit a report to PIRD

False Claims Act (12.17)

- As a Provider, you are required to provide your staff with an annual training (at minimum) on False Claims.
- This training should, at minimum, discuss what a False Claim is, how to identify them, how to report them, and whistleblower protections.
- The County does not require a specific training format. The content is what is essential. If your organization does not have a training template, you may use the County's template. If you use the County's template, make sure that you switch out the County's logos with your organization's.
- For documentation's sake, keep a record of when the training was completed and who was in attendance. Please work with your COR if you have any questions.

The County's training template and more info about False Claims:

HHSA False Claims Act Requirements

HHSA Provider Training: False Claims Act

Encrypted Email Tunnels, or TLS (Transport-layer Security)

- All emails containing County client information must be encrypted prior to sending.
- This is usually a one-click process that requires you pressing the ‘encrypt’ button before sending an email.
- To skip this step, you can establish an encryption tunnel between your organization and the County, so all emails sent between these two entities are automatically encrypted.
- If your organization does not currently have an encryption tunnel, and you are interested in setting one up, reach out to us. There is a 1-page form that can be filled out by your IT department to establish an encrypted connection.

How can we help?

- We are happy to provide targeted consultancy to your organization and can help with:
  - Walk throughs
  - Trainings for staff
  - Trainings for Privacy/Security Officers
  - Advise on Policies, Procedures, and Forms
- If you have any concerns that your organization's policies, procedures, and/or forms are in need of a refresh to meet the County's regulatory standards, please reach out to us early on. We are here to help!

More resources for compliance, information security, and privacy policies:

Compliance

Information Security

Privacy

Provider Fundamentals

More questions? Ask us!

Website:

www.cosdcompliance.org

Phone Number:

(619) 237-8571

Mailbox:

PrivacyOfficer.HHSA@sdcounty.ca.gov

Compliance.HHSA@sdcounty.ca.gov