

THE COALITION OF HOMELESS SERVICES PROVIDERS

Monterey and San Benito Counties HMIS Partner Agency Technical Administrator/Security Officer Agreement

Per the Monterey and San Benito Counties Homeless Management Information System (HMIS) Policies & Procedures HMIS Security Standards, each HMIS Partner Agency must designate a Technical Administrator and Security Officer.

The Partner Agency Technical Administrator is responsible for:

- Overseeing agency compliance with the Memorandum of Understanding and all applicable plans, forms, standards and governance documents,
- Detecting and responding to violations of any applicable HMIS plans, forms, standards and governance documents,
- Serving as the primary contact for all communication regarding the HMIS at this agency and forwarding information to all agency End Users as appropriate,
- Ensuring thorough and accurate data collection by agency End Users as specified by HMIS forms and standards,
- Providing first-level End User support,
- Managing End User licenses,
- Ensuring the agency provides and maintains adequate internet connectivity,
- Maintaining agency and program descriptor data in HMIS,
- Configuring provider preferences (assessments, referrals, services, etc.) in HMIS,
- Completing agency-level HUD reporting and/or supporting agency programs with reporting needs,
- Performing authorized imports of client data.

The Partner Agency Security Officer is responsible for:

- Conducting a thorough quarterly review of internal compliance with all applicable HMIS plans, standards and governance documents,
- Completing the Compliance Certification Checklist, and forwarding the Checklist to the HMIS Lead Agency
- Continually monitoring and maintaining security of all staff workstations used for HMIS data entry,
- Safeguarding client privacy by ensuring End User and agency compliance with confidentiality and security policies,
- Investigating potential breaches of HMIS system security and/or client confidentiality and notifying the Lead Security Officer of substantiated incidents,
- Developing and implementing procedures for managing new, retired, and compromised local system account credentials,
- Developing and implementing procedures that will prevent unauthorized users from connecting to private agency networks,
- Ensuring all agency End Users complete the HMIS End User Agreement and maintaining documentation of all HMIS End User Agreements,

- Ensuring all agency End Users complete mandatory training and forwarding documentation of training to the HMIS Lead Agency.

The Partner Agency must perform a background check on any individual

- Designated as a Partner Agency Technical Administrator,
- Designated as a Security Officer,
- Granted administrator-level access in HMIS.

This check must be completed before that individual is given one of the designations above or granted administrative access, and the results of the background check must be retained by the Partner Agency in the individual's personnel file. A background check may be conducted only once for each person unless otherwise required.

Partner Agency Name: _____

HMIS End User Name: _____

On behalf of the Partner Agency named above, I will be filling the role of (check all that apply):

- Technical Administrator
- Security Officer

By signing, I am agreeing to fulfill all the responsibilities listed above for my role.

End User Signature Date

(To be completed by the Supervisor of the End User named above or the Partner Agency Executive Director)

I certify that a background check has been completed on the End User named above and that a copy of the results of that background check is filed with his/her personnel file.

Supervisor/Executive Director Signature

Date

Supervisor/Executive Director Printed Name

Supervisor/Executive Director Title

Return a signed copy of this form to: Oliver Elbert | oeibert@chsp.org.