CENTER FOR DATA INSIGHTS AND INNOVATION
CALIFORNIA HEALTH & HUMAN SERVICES AGENCY

View xForm - Unanticipated Problem or Adverse Event Form v2

Use this form to report unanticipated problems (including breach of data security) or adverse events involving risks to human subjects while the research is being conducted.

Data Entry
- Submitted 10/24/2025 1:43 PM ET by Marykate Miller

UP or AE Questions

Submitter

December 2025 cycle.

10/21/2025 • Sussan Atifeh • Internal

Primary reviewer of the initial submission of this project is Ms. Kurtural. Secondary reviewer of the initial submission of this project is Dr. Dickey.

This Adverse Event will be assigned to Dr. Dickey to be discussed in the December 5th, 2025, Full Board meeting.

10/21/2025 • Sussan Atifeh • Internal

Hi Drs. Hess and Dickey,

This adverse event appears to be a serious one that should be addressed in the December meeting. If you agree and also believe the research team should explain any corrective actions to prevent such events in the application, please let me know. I will then reject the application to data entry with a note asking the researchers to list their corrective actions.

10/21/2025 • Sussan Atifeh • Internal

Marykate Miller

Email: mkemiller@ucdavis.edu **Business:** (916) 734-2877

Project number

2025-038

Principal Investigator

Joshua Fenton, MD, MPH

Email: jjfenton@ucdavis.edu **Business:** (916) 734-2820

Study title

Rigorous Evaluation of California Policies to Disseminate Emergency Department-based Services for Opioid Use Disorder

Study personnel

Name	Role
Aimee Moulin, MD	Research Team
Alicia Agnoli, MD, MPH, MHS	Research Team
Anthony Jerant, MD	Responsible Official
Daniel Tancredi, PhD	Research Team
Joshua Fenton, MD, MPH	Research Team
Joshua Fenton, MD, MPH	Principal Investigator
Marykate Miller	Research Team
Shao-You Fang, Doctorate	Research Team
Stephen Henry, MD, MSc	Research Team

Monitoring Entity

Principal Investigator

Report Type

Unanticipated Problem involving risks to participants or others

Provide a brief description of event or information for your selection above

Please update the application by addressing the following items and resubmit it as soon as possible:

• Prevention Measures:
Provide a list of corrective actions to be taken to prevent similar incidents in the future.

• Encryption Details:
Clarify the level of protection provided by the encryption used on the flash drive (e.g., encryption type, strength, and compliance with applicable standards).

• CMS role:
Specify whether the Centers for Medicare and Medicaid Services (CMS) may have any responsibility or shared procedures related to the mailing and receipt of the data.

• Security Context:
Provide any insight into how the flash drive may have been identified or targeted (e.g., external labeling, packaging, or recognizable indicators of data content).

• Security Context:
Provide any insight into how the flash drive may have been identified or targeted (e.g., external labeling, packaging, or recognizable indicators of data content).

• Notifying Data owner Department:
Confirm that CDPH (the data owner) has been notified of the incident, and upload documentation verifying the notification (e.g., a copy of the email, confirmation receipt, or any related application submitted to CDPH).

10/22/2025 • Sussan Atifeh • *Not* Internal

On October 7th, 2025, a study team member mailed an encrypted flash drive via UPS with tracking to the CMS team conducting the linkage between Medicaid claims data and death records. The flash drive included a file that included the following variables: last 4 of SSN, last name, DOB, gender, and zip code. The mailing arrived at its destination site on October 20, 2025, torn, and with the flash drive missing. The flash drive was encrypted, and the password was not included in the mailing.

Prevention measures: When we re-mail the encrypted data on a password-protected thumbdrive, we will use a small box to provide more durable package protection. We will also send the package using an overnight carrier that will require a signature from the receiving CMS contractor.

Encryption Details: The flash drive is encrypted with a 13-digit password with upper- and lower-case letters, and numbers via 7-Zip File Manager. The encryption level of 7-Zip is AES-256 (Advanced Encryption Standard with a 256-bit key) which is the same standard used by the U.S. government for top-secret information. 7-Zip creates the encryption key from a user-provided password using a strong hash function (SHA-256) with many iterations to make brute-force attacks more difficult.

CMS role: It is unlikely that CMS had a role in this incident. The mailing had been torn before it arrived at its destination.

Security Context: It is unclear if the mailing was targeted, or simply torn in the otherwise standard process of sorting and transporting mail. The flash drive was mailed in a standard envelope, with no other markings other than the shipping and return addresses.

Notifying Data owner Department: CDPH has been notified, and has determined that the incident does not trigger notification to any individuals under any of the applicable laws, and has closed the matter on their end. Please see attached PDF of that email exchange for further details.

Date of event
10/20/2025

Date PI learned of event
10/20/2025

Enrolled in OSHPD research (OSHPD campus including Foothills facilities)?
No

Are there proposed changes to the protocol?

No

Attach any relevant documents to the report

CDPH AE Reporting Email_10.22.25 Other Documents

PI Signature for Coordination Submission - Submitted 10/24/2025 3:33 PM ET by Joshua Fenton, MD, MPH

PI Signature

Is this form ready to be reviewed by the IRB? If not, choose no to have the application sent back to the coordinator for revisions.

Yes

To sign this form, enter your IRBManager password. By signing this form, you are indicating that the information within this formis accurate and reflects the proposed research.

Signed Friday, October 24, 2025 3:33:17 PM ET by Joshua Fenton, MD, MPH

Notify IRB for Pre-Screening

IRB pre-screening

Is the AE report ready to be reviewed by the Chair/designee?

No

Detail for the PI what additional information or changes are needed on this AE report (research team will see the information typed into this response).
This Adverse Event Report has been scheduled to be discussed in the CPHS December 5, 2025, Full Board meeting. The application has been returned to data entry to give access to the research team to provide some clarification in the application and address some comments. Please open the adverse event application and clarify about the items listed below and resubmit it as soon as possible:

• Prevention Measures:
Provide a list of corrective actions to be taken to prevent similar incidents in the future.

• Encryption Details:
Clarify the level of protection provided by the encryption used on the flash drive (e.g., encryption type, strength, and compliance with applicable standards).

• CMS role:
Specify whether the Centers for Medicare and Medicaid Services (CMS) may have any responsibility or shared procedures related to the mailing and receipt of the data.

• Security Context:
Provide any insight into how the flash drive may have been identified or targeted (e.g., external labeling, packaging, or recognizable indicators of data content).

Thanks.

.

Outlook

RE: 25-PO-VRR-79505 Missing Encrypted Flash Drive - UPS (Project 25-01-0038-R)

From CDPH Privacy Office <privacy@cdph.ca.gov>
Date Wed 10/22/2025 2:55 PM
To Marykate Miller <mkemiller@health.ucdavis.edu>
Cc Joshua J Fenton <jjfenton@health.ucdavis.edu>; CDPH Privacy Office <privacy@cdph.ca.gov>; Kaempfer-Tong, Diana@CDPH <Diana.Kaempfer-Tong@cdph.ca.gov>

Good afternoon,

Thank you for reporting this incident and providing us with the completed the forms. We have determined this incident does not trigger notification to any individuals under any of the applicable laws and we will be closing this matter. Please let us know should you learn of anything that changes the facts as you have reported to us.

Thank you,

CDPH Privacy Office

CDPH
California Department of Public Health

From: Marykate Miller <mkemiller@health.ucdavis.edu>
Sent: Tuesday, October 21, 2025 3:41 PM
To: White, Emily@CDPH <Emily.White@cdph.ca.gov>
Cc: Joshua J Fenton <jjfenton@health.ucdavis.edu>; CDPH Privacy Office <privacy@cdph.ca.gov>; CDPH Info Security Office <CDPH.InfoSecurityOffice@cdph.ca.gov>; Gill, Maninder@CDPH <Maninder.Gill@cdph.ca.gov>; Harris, Andy@CDPH <Andrew.Harris@cdph.ca.gov>; Inman, Maggie@CDPH <Maggie.Inman@cdph.ca.gov>; Kaempfer-Tong, Diana@CDPH <Diana.Kaempfer-Tong@cdph.ca.gov>; Sarah Folker@CDPH <Sarah.Folker@cdph.ca.gov>; Tai, Annie@CDPH <Annie.Tai@cdph.ca.gov>; Van Wagner, Keith@CDPH <Keith.VanWagner@cdph.ca.gov>
Subject: Re: 25-PO-VRR-79505 Missing Encrypted Flash Drive - UPS (Project 25-01-0038-R)

Hi Emily,
Thank you for the information. Please see attached forms for Privacy Incident Number 25-

PO-VRR-79505.
The individual involved in the incident is a UC Davis employee, please see attached documentation for further information about the incident.
Thanks,
Marykate

From: White, Emily@CDPH <Emily.White@cdph.ca.gov>
Sent: Tuesday, October 21, 2025 10:27 AM
To: Marykate Miller <mkemiller@health.ucdavis.edu>
Cc: Joshua J Fenton <jjfenton@health.ucdavis.edu>; CDPH Privacy Office <privacy@cdph.ca.gov>; CDPH Info Security Office <CDPH.InfoSecurityOffice@cdph.ca.gov>; Gill, Maninder@CDPH <Maninder.Gill@cdph.ca.gov>; Harris, Andy@CDPH <Andrew.Harris@cdph.ca.gov>; Inman, Maggie@CDPH <Maggie.Inman@cdph.ca.gov>; Kaempfer-Tong, Diana@CDPH <Diana.Kaempfer-Tong@cdph.ca.gov>; Sarah Folker@CDPH <Sarah.Folker@cdph.ca.gov>; Tai, Annie@CDPH <Annie.Tai@cdph.ca.gov>; Van Wagner, Keith@CDPH <Keith.VanWagner@cdph.ca.gov>
Subject: 25-PO-VRR-79505 Missing Encrypted Flash Drive - UPS (Project 25-01-0038-R)

Hello Marykate,

Thank you for the notification. Privacy Incident Number ***25-PO-VRR-79505*** has been assigned by the CDPH Privacy Office. *Please reference the Privacy Incident Number in all further communications regarding this matter*.

Attached you will find the following forms and instructions:

- *CDPH Breach/Incident Reporting Form INSTRUCTIONS*
- CDPH Breach/Incident Reporting Form (2 pages)
- Security Incident Determination Checklist (3 pages)
- State Breach Notification Checklist (1 page)

PLEASE DO THE FOLLOWING:

1. **Please read the attached form instructions before completing steps 2 and 3 below.**

2. **Complete all documents and return them to the Privacy Office no later than CLOSE OF BUSINESS TODAY.**

3. **Provide responses to the following questions**:

Was the individual(s) who caused and/or was involved in this incident:

A CDPH employee?
If so, please list:

- Employee(s) name and title
- The employee(s) supervisor's name and title
- The Chain of Command for the Program, starting with supervisor of employee and above

A Contract Employee?
If so, please list:

- Employee(s) name and title
- Name of contractor
- Address of contractor (location breach occurred)

- Contact person for the contractor
- CDPH Program Manager for contractor
- *If a contract is involved, please provide the current contract between CDPH and the contractor.*

When the Privacy Office receives the completed forms and responses to the questions, a determination will be made as to whether a breach and/or a violation of the Department Information Security Policies has occurred and if notification to the affected individual(s) is warranted. If notification is warranted, the Privacy Office will prepare the draft notification letter(s) for Program's review prior to sending to the State Information Security Office for final review and approval.

If you have any questions, please do not hesitate to contact me.

Again, thank you for the notification.

Emily White
Privacy Analyst
Office of Legal Services, Privacy Office
California Department of Public Health

From: Marykate Miller <mkemiller@health.ucdavis.edu>
Sent: Monday, October 20, 2025 4:33 PM
To: CDPH Privacy Office <privacy@cdph.ca.gov>; CDHP.InfoSecurityOffice@cdph.ca.gov
Cc: Joshua J Fenton <jjfenton@health.ucdavis.edu>
Subject: Project 25-01-0038-R

Good afternoon,

I am writing to report an incident that we became aware of today.

On October 7th, 2025, a study team member mailed an encrypted flash drive via UPS with tracking to the CMS team conducting the linkage between Medicaid claims data and death records.

The flash drive included a file that included 56,832 rows of the following variables: last 4 of SSN, last name, DOB, gender, and zip code. The mailing arrived at its destination site on October 20, 2025, torn, and with the flash drive missing. The flash drive was encrypted, and

the password was not included in the mailing.

We do not know if the mailing was intentionally or accidentally opened, or where the opening occurred along its mailing route. We do not know if anyone has attempted to access the materials of the encrypted flash drive.

We do not believe that Civil Code section 1798.29 or any other state or federal laws requiring individual notifications of breaches have been triggered, given that the drive is encrypted, and that all individuals in that encrypted data file are deceased.

Thanks,

Marykate Miller, M.S.
Health Policy Analyst IV

UC Davis Center for Healthcare Policy and Research
4480 2nd Ave, Suite 4152
Sacramento, CA 95817

916-734-2877 tel
mkemiller@health.ucdavis.edu

UCDAVIS
Center for Healthcare
Policy and Research

Upcoming out of office days: November 10th - 12th