

CalSAWS

California Statewide Automated Welfare System

Design Document

SCR CA-49308 [DCFS: Create a task when child goes from AAP to FC]



DOCUMENT APPROVAL HISTORY

Prepared By	Michael Barillas
Reviewed By	Naveen Bhumandla

DATE	DOCUMENT VERSION	REVISION DESCRIPTION	AUTHOR
12/18/18	1.0	Initial Draft	Michael Barillas

Table of Contents

1	Overview	4
1.1	Current Design	4
1.2	Requests.....	4
1.3	Overview of Recommendations	4
1.4	Assumptions.....	4
2	Recommendations	5
2.1	Child AAP to FC Task.....	5
2.1.1	Overview.....	5
2.1.2	Description of Change	5
2.1.3	Execution Frequency	6
2.1.4	Key Scheduling Dependencies	6
2.1.5	Counties Impacted	6
2.1.6	Data Volume/Performance	6
2.1.7	Interface Partner.....	6
2.1.8	Failure Procedure/Operational Instructions.....	6
3	Requirements.....	6
3.1	Project Requirements.....	7

1 OVERVIEW

CalSAWS will create a task for the worker when a child is simultaneously Active on Adoption Assistance Program(AAP) and Foster Care (FC) programs.

1.1 Current Design

No task is being created for the worker when a child is simultaneously Active on AAP and FC programs.

1.2 Requests

CalSAWS will create a task for the worker when a child is simultaneously Active on AAP and FC programs.

1.3 Overview of Recommendations

Create a task for the worker when a child goes from AAP to FC.

1.4 Assumptions

A "child" is any person Active on the FC or AAP programs; Each program may have it's own definition of what constitutes a "child". The intent of this SCR is to identify the scenario in which an Active AAP person is simultaneously Active on the FC program. The assumption is that if the person is Active on both programs, they meet the definition of a "child" per each program's rules.

2 RECOMMENDATIONS

CalSAWS will create a task for the worker when a child is simultaneously Active on Adoption Assistance Program(AAP) and Foster Care (FC) programs.

2.1 Child AAP to FC Task

2.1.1 Overview

CalSAWS will create a task for the worker when a child is simultaneously Active on Adoption Assistance Program(AAP) and Foster Care (FC) programs .

2.1.2 Description of Change

- 1) Create a new Batch Job to generate a task and assign it to the AAP program's case carrying worker when all the following conditions are true:
 - a. The child is an Active Member on the AAP program as of the Batch Date
 - b. The same child is an Active Member on the FC program as of the Batch Date. Note: The person match will be on PERS.ID
 - c. The AAP program and the FC program exist in the same County.
 - d. The FC program active begin date is after the AAP program active begin date
 - e. There does not already exist the same task in which the due date is a future date (as of the Batch Date).

Automated Task Details (LRS Only)	
Trigger Condition	<i>Child is simultaneously Active on AAP and FC programs.</i>
Task Type	<i>Child AAP to FC</i>
Task Category	<i>DCFS</i>
Task Priority	<i>Medium</i>
Task Due Date	<i>3 Days</i>
Task Expiration Date	<i>60 Days</i>
Task Long Description	<i>Child is Active in Adoptions Assistance Program <AAP Case Number> and Foster Care Program <FC Case Number>. Please re-evaluate eligibility.</i>
Office Distribution	<i>No</i>

Task Initial Assignment	<i>AAP Case Carrying Worker</i>
Task Navigation Template	<i>Case Summary</i>

2.1.3 Execution Frequency

Daily – Business Days

2.1.4 Key Scheduling Dependencies

Predessor: DCFS Batch EDBC

Successor: Task Generation

2.1.5 Counties Impacted

All county job, only counites with AAP programs will be included for batch processing

2.1.6 Data Volume/Performance

N/A

2.1.7 Interface Partner

N/A

2.1.8 Failure Procedure/Operational Instructions

Batch Support Operations staff will evaluate transmission errors and failures and determine the appropriate resolution (i.e., manually retrieving the file from the directory and contacting the external partner if there is an account or password issue, etc...)

3 REQUIREMENTS

CalSAWS will create a task for the worker when a child is simultaneously Active on AAP and FC programs.

3.1 Project Requirements

REQ #	REQUIREMENT TEXT	How Requirement Met
2.20.1.8	The LRS shall alert and provide COUNTY-specified details to the worker of discrepancies between LRS Data received via external interfaces and existing applicant, participant, and/or case records, so the worker can take the necessary action(s) to resolve the discrepancies.	CalSAWS is creating a task for the worker when a child is simultaneously Active on AAP and FC programs.

CalSAWS

California Statewide Automated Welfare System

Design Document

SCR CA-200640 DDCR 3157:

MAGI Request Validation for Deceased People

Version 1.0

CalSAWS	DOCUMENT APPROVAL HISTORY	
	Prepared By	Antony Lerner
	Reviewed By	Prashant Goel, Priya Subramaniam, William Baretsky, Akira Moriguchi

DATE	DOCUMENT VERSION	REVISION DESCRIPTION	AUTHOR
09/11/2019	1.0	Design Draft	Antony Lerner

Table of Contents

1	Overview	4
	1.1 Current Design	4
	1.2 Requests.....	4
	1.3 Overview of Recommendations	5
	1.4 Assumptions.....	5
2	Recommendations	6
	2.1 MAGI Determination List page	6
	2.1.1 Overview.....	6
	2.1.2 Description of Changes.....	6
	2.1.3 Page Location	8
	2.2 Batch.....	8
	2.2.1 Overview.....	8
	2.2.2 Description of Change	8
	2.2.3 Execution Frequency	10
	2.2.4 Key Scheduling Dependencies.....	10
	2.2.5 Counties Impacted.....	10
	2.2.6 Data Volume/Performance.....	10
	2.2.7 Failure Procedure/Operational Instructions.....	10
	2.3 eHIT	11
	2.3.1 Overview.....	11
	2.3.2 Description of Change	11
	2.3.3 Counties Impacted	11
	2.3.4 Interface Partner.....	11
3	Requirements.....	12
	3.1 Project Requirements.....	12

1 OVERVIEW

The purpose of this document is to define an enhancement in CalSAWS to appropriately communicate Tax Household information to CalHEERS when a person is deceased, so CalHEERS may correctly determine Advanced Premium Tax Credit (APTC).

CalSAWS will prevent sending an Eligibility Determination Request (EDR) when certain conditions are met relating to a deceased person. CalSAWS will update the conditions for the existing validation which requires a Tax Household record for any person to exclude any person who became deceased in a year prior to the benefit month to send an EDR. CalSAWS will no longer send closed deceased non-Primary Applicants as part of an EDR.

1.1 Current Design

When a Worker requests a MAGI Determination, CalSAWS sends the interpreted Tax Household information for the year of the EDR benefit month. This interpretation is performed as follows:

1. If no person has a Tax Household record for the year of the EDR benefit month, the system uses the Tax Household information from the most recent prior year that contains at least one Tax Household record.
2. Otherwise, if at least one person has a Tax Household record for the year of the EDR benefit month, all Tax Household information is built from that year's Tax Household records.

The interpreted Tax Household information may contain a person with a deceased date prior to the benefit month's calendar year.

A Primary Applicant with a deceased date in a year prior to the benefit month may be sent in an EDR; CalSAWS does not require the Worker close such programs through a Negative Action.

1.2 Requests

1. Prevent the interpreted Tax Household information in an EDR from containing a person with a deceased date in a calendar year prior to the benefit month's calendar year.
2. Prevent sending a Primary Applicant with a deceased date in a calendar year prior to the benefit month year through an EDR.
 - a. Require the Worker close such program through a Negative Action.

1.3 Overview of Recommendations

1. Prevent Request MAGI and Batch MAGI when certain conditions are met relating to deceased people:
 - a. Enforce Negative Action for a household where the Primary Applicant became verified deceased person in a calendar year prior to the benefit month year.
 - b. Prevent a verified deceased person from having a Tax Household record in a year following their death.
 - c. Update the conditions for the existing limitation which requires a Tax Household record for all persons to run MAGI to exclude a person deceased in a prior calendar year.
2. Prevent a person who is not the primary applicant in the benefit month and became a verified deceased person in a calendar year prior to the benefit month year and is not open in the benefit month from being sent as part of an EDR.

1.4 Assumptions

1. CalSAWS will not identify nor communicate to CalHEERS deceased persons with existing APTC eligibility.

2 RECOMMENDATIONS

2.1 MAGI Determination List page

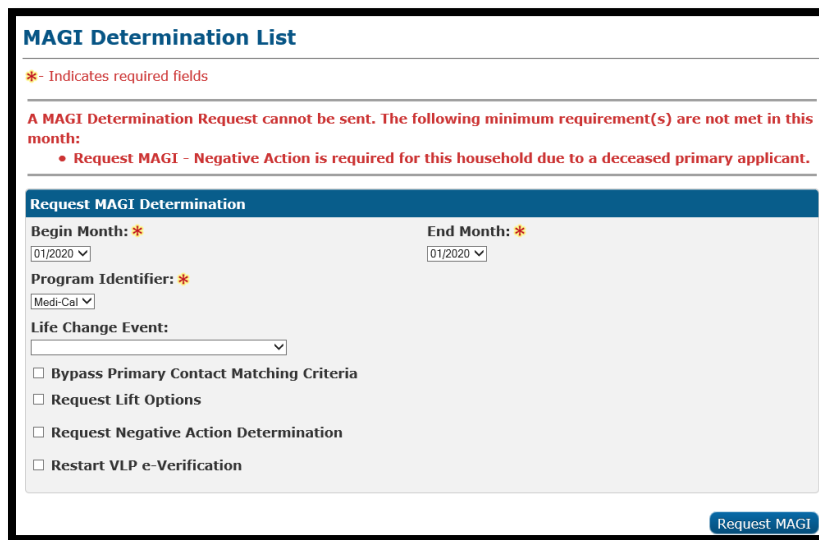
2.1.1 Overview

Add a page validation to require Negative Action for the entire household when a Worker requests MAGI and the Primary Applicant is deceased in a calendar year prior to the benefit month year. Prevent a Worker from requesting MAGI with a person who was deceased in a prior calendar year still included in the Tax Household. Update the existing page validation to allow requesting MAGI for a person without a Tax Household record if the person was deceased in a prior calendar year.

2.1.2 Description of Changes

1. Add the following validation to the "MAGI Determination List" page to prevent Request MAGI where the Primary Applicant became deceased as shown on Figure 2.1.2.1
 - a. Validation Message: "Request MAGI - Negative Action is required for this household due to a deceased primary applicant."
 - b. Validation Trigger: "Request MAGI" button is clicked.
 - c. Validation Condition: When all are true:
 1. The primary applicant for the selected Medi-Cal program became a verified deceased person in a calendar year prior to the benefit month year.
 2. Not every open person is being closed through Negative Action MAGI.

Note: The page validation is a hard stop validation.



The screenshot displays the "MAGI Determination List" page. At the top, there is a legend: "* - Indicates required fields". Below this, a red error message states: "A MAGI Determination Request cannot be sent. The following minimum requirement(s) are not met in this month: Request MAGI - Negative Action is required for this household due to a deceased primary applicant." The main form area is titled "Request MAGI Determination" and contains several fields: "Begin Month: *" with a dropdown menu showing "01/2020", "End Month: *" with a dropdown menu showing "01/2020", "Program Identifier: *" with a dropdown menu showing "Medi-Cal", and "Life Change Event:" with a dropdown menu. Below these fields are four checkboxes: "Bypass Primary Contact Matching Criteria", "Request Lift Options", "Request Negative Action Determination", and "Restart VLP e-Verification". A blue "Request MAGI" button is located at the bottom right of the form.

Figure 2.1.2.1 – Validation message where Primary Applicant became deceased

2. Add the following validation to the "MAGI Determination List" page to prevent Request MAGI where a person deceased in the prior calendar year has a Tax Household record as shown on Figure 2.1.2.2
 - a. Validation Message: "Request MAGI - [person name] is deceased and currently has a Tax Household record for the selected year. Please review Tax Household composition."
 - b. Validation Trigger: "Request MAGI" button is clicked.
 - c. Validation Condition:
 1. At least one of the Tax Household records used in the interpreted Tax Household information belongs to a person who became a verified deceased person in a calendar year prior to the benefit month year.

Note: The page validation is a hard stop validation.

The screenshot shows a web form titled "MAGI Determination List". At the top, there is a legend: "* - Indicates required fields". Below this, a red error message states: "A MAGI Determination Request cannot be sent. The following minimum requirement(s) are not met in this month: Request MAGI - [person name] is deceased and currently has a Tax Household record for the selected year. Please review Tax Household composition." The form itself has a blue header "Request MAGI Determination" and contains several fields: "Begin Month: *" with a dropdown menu showing "01/2020", "End Month: *" with a dropdown menu showing "01/2020", "Program Identifier: *" with a dropdown menu showing "Medi-Cal", and "Life Change Event:" with a dropdown menu. Below these are four checkboxes: "Bypass Primary Contact Matching Criteria", "Request Lift Options", "Request Negative Action Determination", and "Restart VLP e-Verification". A blue "Request MAGI" button is located at the bottom right of the form.

Figure 2.1.2.2 – Validation message for deceased person with Tax Household record

3. Update condition for the following validation which requires a Tax Household record for any person to Request MAGI.
 - a. Validation Message: "Tax household information is missing for the following person(s):"
 - b. Validation Trigger: "Request MAGI" button is clicked.
 - c. Condition: Exclude any person who became a verified deceased person in a calendar year prior to the benefit month year.

2.1.3 Page Location

- **Global: Eligibility**
- **Local: Customer Information**
- **Task: MAGI Eligibility > MAGI Determination List > Request MAGI**

2.2 Batch

2.2.1 Overview

Add a skip reason to Batch MAGI to skip the case if the Primary Applicant is deceased in a calendar year prior to the benefit month year and the EDR does not include a Negative Action for the program. Add a skip reason to Batch MAGI to skip the case if a person who was deceased in a prior calendar year is still included in the Tax Household. Update the existing skip criteria that requires all individuals on an EDR to have a Tax Household record to exclude a person without a Tax Household record if that person was deceased in a prior calendar year.

2.2.2 Description of Change

1. Add a new Batch MAGI Skip Reason to enforce Negative Action for a household where the Primary Applicant became deceased.

Note: This new Batch MAGI skip logic is the same validation logic as when the worker Requests MAGI online as described in Recommendation 2.1.2.1.

Batch MAGI Skip Reason	Description
New/Update	New
Category Id	707
Short Decode Name	<i>Deceased Primary Applicant.</i>
Long Decode Name	<i>Deceased Primary Applicant and not all persons are in negative action.</i>
Begin date	<i>Default System Min Date / 01-JAN-00 00:00:00</i>
End date	<i>Default System High Date /31-DEC-99 00:00:00</i>

2. Update Batch MAGI skip logic to skip cases where the Primary Applicant became deceased and not all persons are Negative Actioned when running Batch MAGI.
 - a. Skip Criteria: When all are true:
 1. The primary applicant for the selected Medi-Cal program became a verified deceased person in a calendar year prior to the benefit month year.
 2. Not every open person is being closed through a Negative Action.
3. Add a Batch MAGI Skip Reason to prevent a deceased person from having a Tax Household record.

Note: This new Batch MAGI skip logic is the same validation logic as when worker Requests MAGI online as described in Recommendation 2.1.2.2

Batch MAGI Skip Reason	Description
New/Update	New
Category Id	707
Short Decode Name	<i>Deceased person has Tax Household record.</i>
Long Decode Name	<i>Deceased person has Tax Household record.</i>
Begin date	<i>Default System Min Date / 01-JAN-00 00:00:00</i>
End date	<i>Default System High Date /31-DEC-99 00:00:00</i>

4. Update Batch MAGI skip logic to skip cases where deceased person has a Tax Household record.
 - a. Skip Criteria:

At least one of the Tax Household records used in the interpreted Tax Household information belongs to a person who became a verified deceased person in a calendar year prior to the benefit month year.
5. Update existing Batch MAGI skip logic that generates existing Batch MAGI skip reason, "Missing Tax Household information" from taking into consideration any person who became a verified deceased person in a calendar year prior to the benefit month year.

2.2.3 Execution Frequency

No change

2.2.4 Key Scheduling Dependencies

No change

2.2.5 Counties Impacted

LA County

2.2.6 Data Volume/Performance

No change

2.2.7 Failure Procedure/Operational Instructions

No change

2.3 eHIT

2.3.1 Overview

Update eHIT from sending a deceased person in an EDR when the person is deceased in the prior calendar year.

2.3.2 Description of Change

1. Prevent a person from being sent as part of a MAGI Determination Request if that person meets all of the following conditions:
 - a. Became a verified deceased person in any calendar year prior to the benefit month year.
 - b. Is not open in the benefit month.
 - c. Is not the primary applicant in the benefit month.

Note: Existing conditions which prevent the person from being sent remain unchanged.

2.3.3 Counties Impacted

LA County

2.3.4 Interface Partner

CalHEERS

3 REQUIREMENTS

3.1 Project Requirements

REQ #	REQUIREMENT TEXT	How Requirement Met
3.5.2.1	The LRS shall enable the sharing of information across multiple agencies.	With this enhancement CalSAWS will communicate updated Tax Household information to CalHEERS to correctly determine persons to be eligible to APTC.

CalSAWS

California Statewide Automated Welfare System

Design Document

CA-208930: Outbound Text Campaign –
Inbound File Reader

CalSAWS	DOCUMENT APPROVAL HISTORY	
	Prepared By	Michael Barillas
	Reviewed By	Balakumar Murthy

DATE	DOCUMENT VERSION	REVISION DESCRIPTION	AUTHOR
9/19/2019	1.0	Initial Draft	Michael Barillas

Table of Contents

1	Overview	3
1.1	Current Design	4
1.2	Requests.....	4
1.3	Overview of Recommendations	4
1.4	Assumptions.....	4
2	Recommendations	5
2.1	Outbound Text Campaign – Inbound File Reader	5
2.1.1	Overview.....	5
2.1.2	Description of Change	5
2.1.3	Execution Frequency	7
2.1.4	Key Scheduling Dependencies	7
2.1.5	Counties Impacted	7
2.1.6	Data Volume/Performance	7
2.1.7	Interface Partner.....	7
2.1.8	Failure Procedure/Operational Instructions.....	8
2.2	Outbound Text Campaign – FTP Batch Job	8
2.2.1	Overview.....	8
2.2.2	Description of Change	8
2.2.3	Execution Frequency	9
2.2.4	Key Scheduling Dependencies	9
2.2.5	Counties Impacted	9
2.2.6	Data Volume/Performance	9
2.2.7	Interface Partner.....	9
2.2.8	Failure Procedure/Operational Instructions.....	9
3	Requirements.....	9
3.1	Project Requirements.....	10

1 OVERVIEW

CALSAWS generates a file containing participant's name, phone, case number, and the message verbiage. CALSAWS then sends that generated file to LA County Information Technology Division (ITD). ITD sends the CALSAWS provided message to the

participant's phone number via text message. Currently ITD does not send CALSAWS a results file for text campaigns.

ITD will send return files to CalSAWS for the following Text Campaigns:

- SAR7 Sent/Reminder
- SAR7 Received
- SAR7 Incomplete
- SAR7 Rescind/Restoration
- SAR7 Processed
- SAR7 Not Received

1.1 Current Design

ITD does not send CALSAWS a results file for text campaigns.

1.2 Requests

Implement an 'Inbound return file interface' for journal purposes.

Note: Reporting will be implemented in a future SCR. Customer's ability to opt-out of text messages will be implemented in a future SCR.

1.3 Overview of Recommendations

CALSAWS will implement an 'Inbound return file interface' that will receive result files from ITD and process each record in the return file.

1.4 Assumptions

- 1) ITD will make the changes necessary to their system to accommodate the new text inbound file location on time for 20.01 release.
- 2) No updates in access/credentials are needed for ITD to send new text return file.

2 RECOMMENDATIONS

CALSAWS will implement an Inbound return file interface that will receive result files from ITD and processes each record in the file. When the 'Inbound return file interface' processes a record, it will translate the result code in the file into a result description for the corresponding cases along with a campaign description and insert a journal entry into the CALSAWS database.

2.1 Outbound Text Campaign – Inbound File Reader

2.1.1 Overview

Create a batch job for each SAR7 campaign to process return files from ITD.

Batch job will do the following; determine if files picked up by the ftp job are valid, process the valid files, add journal entries and log exceptions.

2.1.2 Description of Change

Create a daily batch job that will process the return files from ITD for all the following text campaigns:

Campaign Name	File Name	File Type
SAR 7 Sent/Reminder	237SAR7SentSMS_Normal_MMDDYYYY.csv	Comma Delimited
SAR 7 Received	220ReceivedSMS_Normal_MMDDYYYY.csv	Comma Delimited
SAR 7 Incomplete	226IncompleteSMS_Normal_MMDDYYYY.csv	Comma Delimited
SAR 7 Rescind/Restoration	238RescindSMS_Normal_MMDDYYYY.csv	Comma Delimited
SAR 7 Processed	239ProcessedSMS_Normal_MMDDYYYY.csv	Comma Delimited
SAR 7 Not Received	259NotReceivedSMS_Normal_MMDDYYYY.csv	Comma Delimited

The SAR7 Campaigns will follow the same file format below.

Return File Format for SAR7 Campaigns

Field Name	Field Description	Type	Position	Length	Required
------------	-------------------	------	----------	--------	----------

Phone 1	The message/cell phone number of the participant	Alpha Numeric		10	Y
Text Message	Message given to the participant	Alpha Numeric		139	Y
First Name	First name of the participant	Alpha Numeric		50	Y
Last Name	Last name of the participant	Alpha Numeric		50	Y
Case Number	Case Number	Alpha Numeric		7	Y
Result Message	Text message result	Alpha Numeric		20	Y
Time Stamp	The time stamp in MM/DD/YYYY HH:MM:SS [AM/PM]	Alpha Numeric		22	Y

Result Message

Field Name	Field Description
DELIVRD	Message was delivered
UNDELIV	Network has returned the message. 404
BAD ADDRESS	Invalid address. Could be landline.
INVALID ROUTING	Does not meet required parameters
REJECTD	Message has been rejected

Batch Job will do the following:

- Fetch Files from FTP server
 - Fetch files from CALSAWS FTP server. The file will be stored in the Outbound Text campaign's designated directory for validation check.
- Validate Files
 - Determine inbound file validity with the XSD interface definition file
 - Valid File: File will proceed to process the record
 - Invalid File: System will log exception and end the process
- Check for next record in the Inbound File
 - Check if there is a next record in the inbound file to process
 - If there are no other records, end the process
 - If there are more records Interface continue to be process inbound files

- Process the Record
 - Read the 'Result Message' field in the record and create a journal entry using a reference table to get result code description.
 - If the 'Result Message' received is not in the reference table, system will log exception and stop the process
- Create Journal Entry after processing record
 - Create new Journal Entry into CALSAWS database for the corresponding case using the outbound campaign name, results code, and results code description.
 - Example: 'SAR 7 Sent/Reminder: DELIVRD - Message was delivered'

Journal Entry	Description
New/Update	New
Name	Inbound Text Campaign Return File
Short Description	Outbound <Campaign Name>: <Result Code> - <Result Code Field Description>
Long Description	Outbound <Campaign Name>: <Result Code> - <Result Code Field Description>
Trigger Condition	Batch successfully processed outbound text return file record

2.1.3 Execution Frequency

Daily – Every Business Day

2.1.4 Key Scheduling Dependencies

Predecessor: Outbound Text Campaign – FTP Batch Job

2.1.5 Counties Impacted

19 – Los Angeles

2.1.6 Data Volume/Performance

N/A

2.1.7 Interface Partner

ITD

2.1.8 Failure Procedure/Operational Instructions

Batch Support Operations staff will evaluate transmission errors and failures and determine the appropriate resolution (i.e., manually retrieving the file from the directory and contacting the external partner if there is an account or password issue, etc...)

2.2 Outbound Text Campaign – FTP Batch Job

2.2.1 Overview

Create a Batch Job to fetch files from the CALSAWS FTP server to be processed by the 'Outbound Text Campaign – Inbound File Reader'.

2.2.2 Description of Change

Create a batch job to fetch files sent by ITD from the CalSAWS FTP server to be processed by the 'Outbound Text Campaign Inbound File Reader'.

Note: If CalSAWS receives a return file before 8pm, system will process the file that same day. Otherwise, file will be processed the following business day.

Campaign Name	File Name	File Type	File Location	Message Format	Transfer Method
SAR 7 Sent/Reminder	237SAR7SentSMS_Normal_MMDDYYYY.csv	Comma Delimited	/ProdServer/HHSDC-SFTP/OutboundText_Inbound_Interface/Inbound	ASCII	SFTP
SAR 7 Received	220ReceivedSMS_Normal_MMDDYYYY.csv	Comma Delimited	/ProdServer/HHSDC-SFTP/OutboundText_Inbound_Interface/Inbound	ASCII	SFTP
SAR 7 Incomplete	226IncompleteSMS_Normal_MMDDYYYY.csv	Comma Delimited	/ProdServer/HHSDC-SFTP/OutboundText_Inbound_Interface/Inbound	ASCII	SFTP
SAR 7 Rescind/Restoration	238RescindSMS_Normal_MMDDYYYY.csv	Comma Delimited	/ProdServer/HHSDC-SFTP/OutboundText_Inbound_Interface/Inbound	ASCII	SFTP

SAR 7 Processed	239ProcessedSMS_Normal_MMDDYY.csv	Comma Delimited	/ProdServer/HHSDC-SFTP/OutboundText_Inbound_Interface/Inbound	ASCII	SFTP
SAR 7 Not Received	259NotReceivedSMS_Normal_MMDDYY.csv	Comma Delimited	/ProdServer/HHSDC-SFTP/OutboundText_Inbound_Interface/Inbound	ASCII	SFTP

2.2.3 Execution Frequency

Daily – Every Business Day

2.2.4 Key Scheduling Dependencies

N/A

2.2.5 Counties Impacted

19 – Los Angeles

2.2.6 Data Volume/Performance

N/A

2.2.7 Interface Partner

ITD

2.2.8 Failure Procedure/Operational Instructions

Batch Support Operations staff will evaluate transmission errors and failures and determine the appropriate resolution (i.e., manually retrieving the file from the directory and contacting the external partner if there is an account or password issue, etc...)

3 REQUIREMENTS

CALSAWS generates a file containing participant's name, phone, case number, and the message verbiage. CALSAWS then sends that generated file to LA County Information Technology Division (ITD). ITD sends the CALSAWS provided message to the

participant's phone number via text message. ITD will now send CALSAWS a results file for text campaigns and CalSAWS will process those files with new interface 'Inbound return file interface' for journal purposes.

3.1 Project Requirements

REQ #	REQUIREMENT TEXT	How Requirement Met
2.20.3.1	The LRS shall support one-way interfaces, as described in Section 4 (Summary of Required LRS Interfaces) of this Exhibit B.	CalSAWS is implementing an inbound reader for the purpose of receiving and processing files from ITD.



Design Document

SCR 210134 – Redeliver: EDMS: LRS Update –
Image and View Image Button URL Security
Updates



DOCUMENT APPROVAL HISTORY	
Prepared By	Gillian Noelle Bendicio, Howard Suksanti
Reviewed By	Carl Moore, Long Nguyen, Balakumar Murthy, Abel Lopez, Raheem Raasikh, Christine Altavilla

DATE	DOCUMENT VERSION	REVISION DESCRIPTION	AUTHOR
03/29/2019	.1	Initial Revision	Gillian Noelle Bendicio
04/1/2019	.2	Updated with Interface recommendation.	Howard Suksanti
05/22/2019	1.1	Content Revision <ul style="list-style-type: none"> - Clarification on one-time login token in overview - Replaced one-time use token to one-time login token 	Gillian Noelle Bendicio
07/09/2019	1.2	Content Revision <ul style="list-style-type: none"> - Adding updates to the Select VLP Step 3 Image page - Adding updates to the VLP Step 3 Initiate Third Verification Request Detail page - Pass constant username in getLoginToken operation 	Gillian Noelle Bendicio
09/23/2019	2.0	Updated title to coincide with CA-210134 where this SCR will be redelivered	Gillian Noelle Bendicio

Table of Contents

1	Overview	6
1.1	Current Design.....	6
1.2	Requests	6
1.3	Overview of Recommendations	6
1.4	Assumptions	6
2	Recommendations	8
2.1	Global Navigation – Images	8
2.1.1	Overview.....	8
2.1.2	Description of Changes.....	8
2.1.3	Page Location	9
2.1.4	Security Updates.....	9
2.1.5	Page Mapping.....	9
2.1.6	Page Usage/Data Volume Impacts	9
2.2	e-Application Summary	9
2.2.1	Overview.....	9
2.2.2	Description of Changes.....	9
2.2.3	Page Location	10
2.2.4	Security Updates.....	10
2.2.5	Page Mapping.....	11
2.2.6	Page Usage/Data Volume Impacts	11
2.3	Special Investigation Detail	11
2.3.1	Overview.....	11
2.3.2	Description of Changes.....	11
2.3.3	Page Location	12
2.3.4	Security Updates.....	12
2.3.5	Page Mapping.....	12
2.3.6	Page Usage/Data Volume Impacts	13
2.4	Task Detail	13
2.4.1	Overview.....	13
2.4.2	Description of Changes.....	13
2.4.3	Page Location	14
2.4.4	Security Updates.....	14

2.4.5	Page Mapping.....	14
2.4.6	Page Usage/Data Volume Impacts	14
2.5	Point of Service Image List	15
2.5.1	Overview.....	15
2.5.2	Description of Changes.....	15
2.5.3	Page Location	15
2.5.4	Security Updates.....	16
2.5.5	Page Mapping.....	16
2.5.6	Page Usage/Data Volume Impacts	16
2.6	VLP Step 3 Initiate Third Verification Request Detail	16
2.6.1	Overview.....	16
2.6.2	Description of Changes.....	16
2.6.3	Page Location	17
2.6.4	Security Updates.....	17
2.6.5	Page Mapping.....	18
2.6.6	Page Usage/Data Volume Impacts	18
2.7	Select VLP Step 3 Image	18
2.7.1	Overview.....	18
2.7.2	Description of Changes.....	18
2.7.3	Page Location	19
2.7.4	Security Updates.....	19
2.7.5	Page Mapping.....	20
2.7.6	Page Usage/Data Volume Impacts	20
2.8	Set up a new Web Service Operation on the EDMS web service.....	21
2.8.1	Overview.....	21
2.8.2	Description of Change	21
2.8.3	Execution Frequency	22
2.8.4	Key Scheduling Dependencies.....	22
2.8.5	Counties Impacted	22
2.8.6	Data Volume/Performance	22
2.8.7	Interface Partner.....	22
2.8.8	Failure Procedure/Operational Instructions.....	22
3	Supporting Documents	23
4	Requirements.....	24
4.1	Project Requirements	24

4.2 Migration Requirements..... 24
5 Migration Impacts 25

DRAFT

1 OVERVIEW

This System Change Request (SCR) will document the updates made to the Electronic Document Management System (EDMS) web services which allows the worker to view the application and case images. The SCR will be a joint effort between Accenture and the Information Technology Department (ITD).

1.1 Current Design

Currently, the application and case images are available for viewing through the global navigation if they are within a context of a case and through the following pages with a 'View Images' button:

1. E-Application Summary
2. Special Investigations Detail
3. Task Detail

Additionally, the Point of Service Scan Image List, VLP Step 3 Initiate Third Verification Request Detail and Select VLP Step 3 Image pages allow a worker to view individual scanned images from EDMS.

When accessing these images through these pages, a new window will appear and direct the user to EDMS.

1.2 Requests

The current design does not prevent the worker from copying the EDMS link and sending it to unauthorized users. This impacts confidential cases. The following request have been made to address this issue:

- Provide a one-time authentication with a timeout when accessing EDMS.
- Set up a new Web Service Operation that will be used to get a one-time login token for authentication.

1.3 Overview of Recommendations

The following recommendation has been made to address the security issue:

- Update the link generated to contain an authentication token.
- Set up a new Web Service Operation that will be used to get a one-time login token for authentication. The one-time login token expires after creating a browser session once. The session is maintained in the browser window until it is closed.

1.4 Assumptions

1. The 'DCFS Images' found in the global hyperlink will not be in scope for this SCR.
2. ITD Test Environments will be available to Accenture development team on or before June 23 2019.

3. The changes required from ITD will be deployed to production on or before September 23, 2019.

DRAFT

2 RECOMMENDATIONS

2.1 Global Navigation – Images

2.1.1 Overview

The 'Images' link is located on the global navigation of the system. This allows the user to access EDMS and view the case documents if they are within the context of a case.

2.1.2 Description of Changes

1. Call the new EDMS web service when the user clicks on the 'Images' link to obtain the one-time login authentication token.
 - a. The new EDMS web service will call the 'getLoginToken' endpoint of the EDMS service to obtain the one-time login authentication token.
 - b. After obtaining the token, a new window will open and send a subsequent request to EDMS with the token appended to the base64 encoded URL.
2. Update the EDMS URL that gets generated to contain the authentication token obtained from the new webservice and use the 'https' protocol.
 - a. When the user copies the updated link to a new browser window, the EDMS page will display an error message. Refer to the below scenario table for the EDMS messages that will display:

Scenario	EDMS Error Message
The new EDMS web service is down or has failed while the EDMS server is up	The default HTTP 404 will be displayed.
The new EDMS web service is down or has failed while the EDMS server is down	Error: Failed to connect to EDMS
The username sent by the new EDMS web service is invalid	Error: Invalid user (username)
The token appended to the EDMS URL is invalid	Error: Authentication failed. The token is invalid.
The one-time login token has already been used	Error: Authentication failed. The token is invalid.

Technical Note: The existing URL will be appended with a new request attribute, DM_TICKET, followed by an equal sign and then the encrypted authentication token. The default value of DM_TICKET is null until it gets populated by the new EDMS web service. If the new web service is down, the default value will remain as null.

2.1.3 Page Location

Global: Images

Local:

Task:

2.1.4 Security Updates

Security Rights

Security Right	Right Description	Right to Group Mapping

Security Groups

Security Group	Group Description	Group to Role Mapping

2.1.5 Page Mapping

No impact to this section.

2.1.6 Page Usage/Data Volume Impacts

No impact to this section.

2.2 e-Application Summary

2.2.1 Overview

The 'View Images' button is located at the top right of the e-Application Summary page. Clicking this button will open a new EDMS window which contains the documents associated to the e-application.

2.2.2 Description of Changes

1. Call the new web service when the user clicks on the 'View Images' button to obtain the one-time login authentication token.

- a. The new EDMS web service will call the 'getLoginToken' endpoint of the EDMS service to obtain the one-time login authentication token.
 - b. After obtaining the token, a new window will open and send a subsequent request to EDMS with the token appended to the base64 encoded URL.
2. Update the EDMS URL that gets generated to contain the authentication token obtained from the new webservice and use the 'https' protocol.
- a. When the user copies the updated link to a new browser window, the EDMS page will display an error message. Refer to the below scenario table for the EDMS messages that will display:

Scenario	EDMS Error Message
The new EDMS web service is down or has failed while the EDMS server is up	The default HTTP 404 will be displayed.
The new EDMS web service is down or has failed while the EDMS server is down	Error: Failed to connect to EDMS
The username sent by the new EDMS web service is invalid	Error: Invalid user (username)
The token appended to the EDMS URL is invalid	Error: Authentication failed. The token is invalid.
The one-time login token has already been used	Error: Authentication failed. The token is invalid.

Technical Note: The existing URL will be appended with a new request attribute, DM_TICKET, followed by an equal sign and then the encrypted authentication token. The default value of DM_TICKET is null until it gets populated by the new EDMS web service. If the new web service is down, the default value will remain as null.

2.2.3 Page Location

Global: Case Info, e-Tools

Local: e-Application Search

Task:

2.2.4 Security Updates

Security Rights

Security Right	Right Description	Right to Group Mapping

Security Groups

Security Group	Group Description	Group to Role Mapping

2.2.5 Page Mapping

No impact to this section.

2.2.6 Page Usage/Data Volume Impacts

No impact to this section.

2.3 Special Investigation Detail

2.3.1 Overview

The 'View Images' button is located at the top right of the Special Investigation Detail page. Clicking this button will open a new EDMS window which contains the documents associated to the case with an investigation linked.

2.3.2 Description of Changes

1. Call the new web service when the user clicks on the 'View Images' button to obtain the one-time login authentication token.
 - a. The new EDMS web service will call the 'getLoginToken' endpoint of the EDMS service to obtain the one-time login authentication token.
 - b. After obtaining the token, a new window will open and send a subsequent request to EDMS with the token appended to the base64 encoded URL.
2. Update the EDMS URL that gets generated to contain the authentication token obtained from the new webservice and use the 'https' protocol.
 - a. When the user copies the updated link to a new browser window, the EDMS page will display an error message. Refer to the below scenario table for the EDMS messages that will display:

Scenario	EDMS Error Message
The new EDMS web service is down or has failed while the EDMS server is up	The default HTTP 404 will be displayed.

The new EDMS web service is down or has failed while the EDMS server is down	Error: Failed to connect to EDMS
The username sent by the new EDMS web service is invalid	Error: Invalid user (username)
The token appended to the EDMS URL is invalid	Error: Authentication failed. The token is invalid.
The one-time login token has already been used	Error: Authentication failed. The token is invalid.

Technical Note: The existing URL will be appended with a new request attribute, DM_TICKET, followed by an equal sign and then the encrypted authentication token. The default value of DM_TICKET is null until it gets populated by the new EDMS web service. If the new web service is down, the default value will remain as null.

2.3.3 Page Location

Global: Special Units, Special Investigations

Local: Special Investigation Search

Task:

2.3.4 Security Updates

Security Rights

Security Right	Right Description	Right to Group Mapping

Security Groups

Security Group	Group Description	Group to Role Mapping

2.3.5 Page Mapping

No impact to this section.

2.3.6 Page Usage/Data Volume Impacts

No impact to this section.

2.4 Task Detail

2.4.1 Overview

The 'View Images' button is located at the top right of the Task Detail page. Clicking this button will open a new EDMS window which contains the documents associated to the case.

2.4.2 Description of Changes

1. Call the new web service when the user clicks on the 'View Images' button to obtain the one-time login authentication token.
 - a. The new EDMS web service will call the 'getLoginToken' endpoint of the EDMS service to obtain the one-time login authentication token.
 - b. After obtaining the token, a new window will open and send a subsequent request to EDMS with the token appended to the base64 encoded URL.
2. Update the EDMS URL that gets generated to contain the authentication token obtained from the new webservice and use the 'https' protocol.
 - a. When the user copies the updated link to a new browser window, the EDMS page will display an error message. Refer to the below scenario table for the EDMS messages that will display:

Scenario	EDMS Error Message
The new EDMS web service is down or has failed while the EDMS server is up	The default HTTP 404 will be displayed.
The new EDMS web service is down or has failed while the EDMS server is down	Error: Failed to connect to EDMS
The username sent by the new EDMS web service is invalid	Error: Invalid user (username)
The token appended to the EDMS URL is invalid	Error: Authentication failed. The token is invalid.
The one-time login token has already been used	Error: Authentication failed. The token is invalid.

Technical Note: The existing URL will be appended with a new request attribute, DM_TICKET, followed by an equal sign and then the encrypted authentication token. The default value of DM_TICKET is null until it gets populated by the new EDMS web service. If the new web service is down, the default value will remain as null.

2.4.3 Page Location

Global: Case Info, Tasks

Local: Worklist

Task:

Note: For tasks assigned to the case worker, a hyperlink on the task will display. Otherwise, the worker will need to click on the 'Edit' button for the related task to view the Task Detail page.

2.4.4 Security Updates

Security Rights

Security Right	Right Description	Right to Group Mapping

Security Groups

Security Group	Group Description	Group to Role Mapping

2.4.5 Page Mapping

No impact to this section.

2.4.6 Page Usage/Data Volume Impacts

No impact to this section.

2.5 Point of Service Image List

2.5.1 Overview

The Point of Service Image List contains a list of documents linked to the case. Clicking one of the document links under the 'Document Type' column will open a new EDMS window containing the image of the said document.

2.5.2 Description of Changes

1. Call the new web service when the user clicks on the document link to obtain the one-time login authentication token.
 - a. The new EDMS web service will call the 'getLoginToken' endpoint of the EDMS service to obtain the one-time login authentication token.
 - b. After obtaining the token, a new window will open and send a subsequent request to EDMS with the token appended to the base64 encoded URL.
2. Update the EDMS URL that gets generated to contain the authentication token obtained from the new webservice and use the 'https' protocol.
 - a. When the user copies the updated link to a new browser window, the EDMS page will display an error message. Refer to the below scenario table for the EDMS messages that will display:

Scenario	EDMS Error Message
The new EDMS web service is down or has failed while the EDMS server is up	The default HTTP 404 will be displayed.
The new EDMS web service is down or has failed while the EDMS server is down	Error: Failed to connect to EDMS
The username sent by the new EDMS web service is invalid	Error: Invalid user (username)
The token appended to the EDMS URL is invalid	Error: Authentication failed. The token is invalid.
The one-time login token has already been used	Error: Authentication failed. The token is invalid.

Technical Note: The existing URL will be appended with a new request attribute, DM_TICKET, followed by an equal sign and then the encrypted authentication token. The default value of DM_TICKET is null until it gets populated by the new EDMS web service. If the new web service is down, the default value will remain as null.

2.5.3 Page Location

Global: Case Info, Case Summary

Local: Point of Service

Task:

2.5.4 Security Updates

Security Rights

Security Right	Right Description	Right to Group Mapping

Security Groups

Security Group	Group Description	Group to Role Mapping

2.5.5 Page Mapping

No impact to this section.

2.5.6 Page Usage/Data Volume Impacts

No impact to this section.

2.6 VLP Step 3 Initiate Third Verification Request Detail

2.6.1 Overview

The VLP Step 3 Initiate Third Verification Request Detail contains an image attachment selected from the 'Select VLP Step 3 Image' page. Clicking the image attachment hyperlink will open a new EDMS window containing the image of the said document.

2.6.2 Description of Changes

1. Call the new web service when the user clicks on the image attachment hyperlink to obtain the one-time login authentication token.

- a. The new EDMS web service will call the 'getLoginToken' endpoint of the EDMS service to obtain the one-time login authentication token.
 - b. After obtaining the token, a new window will open and send a subsequent request to EDMS with the token appended to the base64 encoded URL and the username of the staff accessing this page. The staff's information is used for auditing purposes on EDMS.
2. Update the EDMS URL that gets generated to contain the authentication token obtained from the new webservice and use the 'https' protocol.
- b. When the user copies the updated link to a new browser window, the EDMS page will display an error message. Refer to the below scenario table for the EDMS messages that will display:

Scenario	EDMS Error Message
The new EDMS web service is down or has failed while the EDMS server is up	The default HTTP 404 will be displayed.
The new EDMS web service is down or has failed while the EDMS server is down	Error: Failed to connect to EDMS
The username sent by the new EDMS web service is invalid	Error: Invalid user (username)
The token appended to the EDMS URL is invalid	Error: Authentication failed. The token is invalid.
The one-time login token has already been used	Error: Authentication failed. The token is invalid.

Technical Note: The existing URL will be appended with a new request attribute, DM_TICKET, followed by an equal sign and then the encrypted authentication token. The default value of DM_TICKET is null until it gets populated by the new EDMS web service. If the new web service is down, the default value will remain as null.

2.6.3 Page Location

Global:

Local: Verification of Lawful Presence Detail

Task:

2.6.4 Security Updates

Security Rights

Security Right	Right Description	Right to Group Mapping

Security Groups

Security Group	Group Description	Group to Role Mapping

2.6.5 Page Mapping

No impact to this section.

2.6.6 Page Usage/Data Volume Impacts

No impact to this section.

2.7 Select VLP Step 3 Image

2.7.1 Overview

The Select VLP Step 3 Image contains a list of immigration documents linked to the case. Clicking one of the document links through the corresponding 'View Image' button will open a new EDMS window containing the image of the said document.

2.7.2 Description of Changes

1. Call the new web service when the user clicks on the 'View Image' button to obtain the one-time login authentication token.
 - a. The new EDMS web service will call the 'getLoginToken' endpoint of the EDMS service to obtain the one-time login authentication token.
 - b. After obtaining the token, a new window will open and send a subsequent request to EDMS with the token appended to the base64 encoded URL and the username of the staff accessing this page. The staff's information is used for auditing purposes on EDMS.
2. Update the EDMS URL that gets generated to contain the authentication token obtained from the new webservice and use the 'https' protocol.
 - c. When the user copies the updated link to a new browser window, the EDMS page will display an error message. Refer to the below scenario table for the EDMS messages that will display:

Scenario	EDMS Error Message
----------	--------------------

The new EDMS web service is down or has failed while the EDMS server is up	The default HTTP 404 will be displayed.
The new EDMS web service is down or has failed while the EDMS server is down	Error: Failed to connect to EDMS
The username sent by the new EDMS web service is invalid	Error: Invalid user (username)
The token appended to the EDMS URL is invalid	Error: Authentication failed. The token is invalid.
The one-time login token has already been used	Error: Authentication failed. The token is invalid.

Technical Note: The existing URL will be appended with a new request attribute, DM_TICKET, followed by an equal sign and then the encrypted authentication token. The default value of DM_TICKET is null until it gets populated by the new EDMS web service. If the new web service is down, the default value will remain as null.

2.7.3 Page Location

Global:

Local: VLP Step 3 Initiate Third Verification Request Detail

Task:

2.7.4 Security Updates

Security Rights

Security Right	Right Description	Right to Group Mapping

Security Groups

Security Group	Group Description	Group to Role Mapping

2.7.5 Page Mapping

No impact to this section.

2.7.6 Page Usage/Data Volume Impacts

No impact to this section.

DRAFT

2.8 Set up a new Web Service Operation on the EDMS web service.

2.8.1 Overview

The new web service operation will be added to the existing EDMS web service. The web service operation will be used to get a one-time login token for authentication.

2.8.2 Description of Change

Set up the new web service operation ('getLoginToken') that will be used to get a one-time login token for authentication.

Web Service details:

1. Operation name: 'getLoginToken'.
2. Request parameter:

getLoginToken – REQUEST			
FIELD NAME	TYPE	COMMENTS	REQUIRED
userName	String	Login username. userName constant is "leader_reader"	Y

3. Response parameter:

getLoginToken – RESPONSE			
FIELD NAME	TYPE	COMMENTS	REQUIRED
loginToken	String	Single use token string.	Y

Please refer to more details in the XSD file in the supporting document. Exception while retrieving authentication token will not be handled by the Interface. The exception will be handled by the web service caller.

Note: ITD will create an operation within current webservice to pass one-time token to construct URL.

2.8.3 Execution Frequency

Real time.

2.8.4 Key Scheduling Dependencies

N/A.

2.8.5 Counties Impacted

Los Angeles county only.

2.8.6 Data Volume/Performance

N/A.


2.8.7 Interface Partner

ITD.

2.8.8 Failure Procedure/Operational Instructions

Batch Support Operations staff will evaluate transmission errors and failures and determine the appropriate resolution (i.e., manually retrieving the file from the directory and contacting the external partner if there is an account or password issue, etc...)

3 SUPPORTING DOCUMENTS

Number	Functional Area	Description	Attachment
1	Imaging	EDMS updated XSD file.	 EdmsWebserviceService_schema.xsd

DRAFT

4 REQUIREMENTS

The SCR will update the web service that CalACES communicates with external partner - EDMS.

4.1 Project Requirements

REQ #	REQUIREMENT TEXT	How Requirement Met
2.20.1.19	The LRS shall have the ability to receive data from external sources (e.g., State's SACWIS system and COUNTY-approved agencies/partners) for the purposes of establishing and maintaining a case.	The SCR will update the web service that CalACES communicates with external partner - EDMS.

4.2 Migration Requirements

DDID #	REQUIREMENT TEXT	How Requirement Met

5 MIGRATION IMPACTS

SCR Number	Functional Area	Description	Impact	Priority	Address Prior to Migration?

DRAFT