

### **Security and Business Rules:**

1. A new security role of Social Security Number (SSN) Administrator has been created. This security role grants the user access to the SSN of persons associated to their agency as defines below.
2. Any user can add, create, delete and save the 9-digit SSN (the assumption is that if user is adding/creating then user is aware of the actual SSN) per current functionality.
  - a. The SSN cannot be deleted if the person has a current, valid, open Medicaid span. However, the SSN can be changed to a new valid SSN.
  - b. The SSN cannot be deleted if the person has a current benefit account set up under the social security number (SSN).
3. Any user can search using the 9-digit SSN (the assumption is that if user is searching with the 9-digit SSN, then user is aware of the actual SSN). However, the search results will display the 9-digit SSN as masked as xxx-xx-xxxx if a SSN has been recorded for the person.
4. Any user can search for a person without using the SSN. However, the search results will display the 9-digit SSN as masked as xxx-xx-xxxx if a SSN has been recorded for the person. If no SSN has been recorded for the person, the SSN field will remain blank.
5. There are five types of Assignments "Provider", "Case", "Adopted Child", "AA/SAMS Subsidy Children", and "State Employee". Once a worker assignment ends, their ability to view the person's SSN ends as well. Based on assignment, a user can view a persons SSN if they meet the following criteria:
  - a. Provider Assignment: The provider worker is assigned to the provider record and is also an employee of the recommending agency for any provider type. This worker can view the SSN while the Provider record is open (open is provider type has an effective date but no end date). Once the Provider record is no longer showing as "open" under that recommending agency, the provider worker is no longer able to view the provider member's SSN.
  - b. Intake/Case Assignment: An Intake Screener and Screening Decision Maker (SDM) and/or all workers assigned to an open case (regardless of case category) can view any intake/case participants members SSN. This only pertains to active Case Members (not associated persons or inactive members). Once the case is closed, the worker is no longer assigned, thus they are no longer able to view the case member's SSN.
    - i. When the SDM screens out an intake then the worker no longer has SSN view ability.
    - ii. If the SDM links the intake to a case, the intake screener no longer has SSN view capability. However, if the SDM is assigned to the newly created/linked case, then the worker can view the SSN based on assignment.
    - iii. If the SDM links the intake to an ongoing case in which they are not assigned, then the worker no longer has rights to view the SSN.
  - c. Adopted Child Assignment: A SSN Administrator who works for the Agency who sealed/ secured the child's adoption record can view the child's pre-adoptive and post-adoptive person IDs SSN.
    - i. For converted closed adoption cases, ownership belongs to the agency whose converted data processed the sealed adoption record.

## Social Security Number (SSN) Masking Initiative.

November 6, 2009

- ii. If the finalized child is an active permanent child household member of a provider record, the provider assignment rules apply.
  - d. AA/SAMS Subsidy Children Assignment: Workers assigned to children on the financial workload can view both the child's pre-adoptive and post-adoptive person ID's SSN.
  - e. State Employee Assignment: State employees with the assignment to the user Group "Merge Administrator" or "Closed/Sealed Adoption Reviewer" can view a person's SSN.
6. Merge Administrator Function: Users with security of Merge Administrator and SSN Administrator can complete the (Person) merge function regardless of agency.
- a. If one or both SSN number fields are blank and the user only has the (Person) Merge Administrator security and not the SSN Admin role, then user can complete the (person) merge function. However, if a SSN exists for both person records and the SSNs are masked, then the user would be prevented from merging the records.
- | Example:    | SSN View (retain) | SSN View (remove) | Allow Merge: |
|-------------|-------------------|-------------------|--------------|
| Merge Admin | xxx-xx-xxxx       | xxx-xx-xxxx       | No           |
| SSN Admin   | 123-45-6789       | 123-45-6789       | Yes          |
| SSN Admin   | Blank             | Blank             | Yes          |
| Merge Admin | Blank             | xxx-xx-xxxx       | Yes          |
7. Alleged Perpetrator (AP) Search function: The SSN will display in the AP search results for users with security roles of AP Search and SSN Administrator. If the user only possess the AP Search user group, then the SSN for the person in the results list will be masked as xxx-xx-xxxx.

### Screen Modifications:

1. Person – Profile – Basic Tab: The social security number field will remain on this screen.
  - a. Regardless of the assignments or security of the user that is viewing this screen, the SSN will always display as masked xxx-xx-xxxx if a SSN exists for the person. (The SSN field will display as blank if a SSN has not been recorded for this person).
  - b. Two new radio buttons will be added next to the SSN field. One radio button for "Retain" and the second radio button for "Add/Edit". When the user selects to "Add/Edit" the SSN field with no value for the SSN, the user will receive a confirmation message prior to saving/canceling the action.
2. Person – Profile – Confidential Information Tab – This is a new tab that would display next to "Safety Hazard" tab. At this time it is a view or display only screen for SSNs. Access to this tab is based on the two criteria referenced above: assignment or SSN Administrator role. Thus, while one can enter/edit SSN on the person – profile – basic tab, once the information is saved, the data can only be viewed from this new Confidential Information tab.