

Date of Hearing: April 9, 2024

ASSEMBLY COMMITTEE ON HUMAN SERVICES

Alex Lee, Chair

AB 2241 (Alvarez) – As Introduced February 8, 2024

**SUBJECT:** Public social services: reporting and verification

**SUMMARY:** Requires state and county agencies to accept information from public social services applicants and recipients in any form no later than January 1, 2026. Specifically, **this bill:**

- 1) Requires, no later than January 1, 2026, state and county agencies to accept reporting by an applicant or recipient of public social services of any lawfully required information changes, and verification required by law that affect eligibility and benefit amounts, by any means available to the applicant or recipient, including, but not limited to, in person, by telephone, through facsimile, by email, or by any other electronic means.
- 2) Requires a county agency to accept reporting as stated in 1) above to January 1, 2026, if the county agency uses software designed to do both of the following:
  - a) Prevent, detect, search and remove viruses and other types of malware from computers and networks; and,
  - b) Send and receive emails securely.
- 3) Requires the California Department of Social Services (CDSS) and the Department of Health Care Services to implement this act through all-county letters, provider bulletins or notices, policy letters, or similar instructions from the director of each department issued no later than July 1, 2025.
- 4) Prohibits appropriation pursuant to Welfare and Institutions Code (WIC) § 15200 to implement this bill.
- 5) Provides, to the extent that this bill has an overall effect of increasing certain costs already borne by a local agency for programs or levels of services mandated by the 2011 Realignment Legislation within the meaning of Section 36 of Article XIII of the California Constitution, it shall apply to local agencies only to the extent that the state provides annual funding for the cost increase. Any new program or higher level of service provided by a local agency pursuant to this act above the level for which funding has been provided shall not require a subvention of funds by the state or otherwise be subject to Section 6 of Article XIII B of the California Constitution. Further provides that, if the Commission on State Mandates determines that this act contains other costs mandated by the state, reimbursement to local agencies and school districts for those costs shall be made.

**EXISTING LAW:**

State law:

- 1) Declares that the administration of public social services is a county function and responsibility; requires each county to establish a department or agency to administer and promote public understanding of the public services. (WIC § 10800)
- 2) Requires all applications or records concerning any individual made or kept by a public officer or agency in connection with the administration of this code relating to any form of public social services, including protective services provided through public social services agencies, for which grants-in-aid are received by the state to be confidential, and not be open to examination for any purpose not directly connected with the administration of that program, or any investigation, prosecution, or criminal or civil proceeding conducted in connection with the administration of that program. (WIC § 10850(a))
- 3) Requires every person administering aid under any public assistance program to conduct themselves with courtesy, consideration, and respect toward applicants for, and recipients of, aid under that program, and to endeavor at all times to perform their duties in such manner as to secure for every person the amount of aid to which they are entitled, without attempting to elicit any information not necessary to carry out the provisions of law applicable to the program, and without comment or criticism of any fact concerning applicants or recipients not directly related to the administration of the program. (WIC § 10500)
- 4) Requires, pursuant to the data breach notification law, that a person, business, or agency in California that owns or licenses computerized data that includes personal information to notify any California resident whose unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person by a breach of the security of the system or data. The notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified. (Civil Code Sections §§ 1798.29(a), (c); 1798.82(a), (c))
- 5) Requires CDSS to establish verification policies and procedures for CalFresh applicants and beneficiaries in the event that necessary verification is not provided by the applicant or beneficiary to accompany the application at the time of submission. Further requires counties to check all available electronic sources or self-attestation before requesting documentary evidence from the applicant or beneficiary to complete required verification or pursuing secondary evidence to verify the necessary information (WIC § 18901)
- 6) Defines “electronically collected personal information” as any information that is maintained by an agency that identifies or describes an individual user, including, but not limited to, the user’s name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history, password, electronic mail address, and information that reveals any network location or identity, but excludes any information manually submitted to a state agency by a user, whether electronically or in written form, and information on or relating to individuals who are users serving in a business capacity, including, but not limited to, business owners, officers, or principals of that business. (Government Code § 11015.5(d)(1))

Federal law:

- 7) Requires households to file Supplemental Nutrition Assistance Program (SNAP) applications by submitting the forms to the SNAP office either in person, through an authorized representative, by mail, by completing an online electronic application, or, if available, by fax, telephone, or other electronic transmission. (7 Code of Federal Regulations 273.2(c)(1)(i))

**FISCAL EFFECT:** Unknown, this bill has not been analyzed by a fiscal committee.

**COMMENTS:**

**Background:** *Public Social Services.* California administers a number of public assistance programs to uplift those in poverty. Many of those programs are housed within CDSS and then administered by each county. When counties are determining eligibility to administer the public assistance, a county representative must communicate with the applicant or recipient, which likely includes a telephone call. If there is a question of eligibility, an applicant must provide the requested information or risk being denied eligibility. Information commonly collected across public social services programs include name, income, citizenship status, social security numbers, residency, identity, disability, and household composition, among other things.

At the county level, California administers three federally funded safety net or public assistance programs: CalFresh (federally known as SNAP), California Work Opportunity and Responsibility to Kids (CalWORKs) (federally known as the Temporary Assistance for Needy Families or TANF), and Medi-Cal (federally known as Medicaid). Each county works to determine eligibility set forth by federal and state standards and then helps disburse the aid to recipients.

*CalFresh* uses federal funds to provide food assistance to low-income individuals and families. The United States Department of Agriculture (USDA) is responsible for setting specific eligibility requirements for programs like CalFresh including a gross and net income test, work requirements, and other documentation requirements. The maximum allowable gross income is 200% of the federal poverty level (FPL). Households with elderly or disabled members are not subject to gross income criteria but must have a net monthly income at or below 100% of the FPL. Individuals can complete the CalFresh application online, over the phone, in-person at their county CalFresh office, or through the mail.

Once approved, CalFresh recipients cannot access CalFresh funds through withdrawal at point-of-sale terminals or at ATMs. Instead, CalFresh benefits are distributed monthly through an electronic benefits transfer (EBT) card to purchase food items to be prepared and consumed at home, as well as seeds and plants that can be grown at home and produce food. The USDA reports that only 70% of eligible Californians are enrolled in CalFresh benefits, compared to the national average of 82% of eligible persons in the country that are enrolled. The LAO reports that in 2022-23, about 5.1 million Californians received a total of \$14.5 billion in CalFresh benefits, for an average monthly benefit of about \$185.

*CalWORKs* is also administered at the local level through counties. CalWORKs is funded in part by the federal TANF block grant and aims to help children and families meet basic needs and break the cycle of poverty. Families receive cash assistance and have access to a variety of services aimed at addressing mental health needs, substance use disorders, instances of domestic

violence, and learning disabilities, among other issues. Parents are required to develop and participate in a welfare-to-work plan unless otherwise exempted. CDSS' 2023 annual summary reports that 347,868 families received monthly CalWORKs benefits in 2022-23, or 0.8% of the total population in California. While grant amounts are adjusted based on family size, income level, and region, in 2022-23, the average monthly cash grant was \$962 across all family sizes and income levels, according to the LAO.

*Information Verification and Storage Processes.* The California Statewide Automated Welfare System (CalSAWs) aims to streamline public assistance programs like CalWORKs, CalFresh, Medi-Cal, and others across all 58 counties. By December 31, 2023, all counties were required to transition to CalSAWs from their existing welfare systems to ensure efficient and consistent delivery of services. CalSAWs handles functions like eligibility determination, benefit computation, benefit delivery, case management, and information management. Applicants or recipients of social services programs utilize BenefitsCal, which has the ability for secure document upload. Counties do not require in-person document or information drop-off, but it remains an option. Alternatively, documents can also be mailed or dropped off in a secure dropbox.

At the federal level, regulations allow SNAP applications (or CalFresh) to submit forms to a CalFresh office either in person, through an authorized representative, by mail, by completing an on-line electronic application, or if available, by fax, telephone, or other electronic transmission. "Other electronic transmission" is not further defined, but also does not explicitly exclude email submissions. Furthermore, state law defines "electronically collected personal information" as any data that an agency maintains and that identifies or describes an individual user, but excludes information manually submitted to a state agency by a user, regardless of whether it was submitted electronically or in written form. This means that any data provided directly by the user to the agency, without the involvement of electronic systems or processes is not considered "electronically collected personal information." In the case of when an applicant or beneficiary is missing information at the time of submitting an application, existing state law requires counties to check all available electronic sources or self-attestation before requesting documentary evidence from the applicant or beneficiary to complete required verification or pursuing secondary evidence to verify the necessary information.

*Technology Privacy and Security Agreement.* CDSS and CalSAWs Joint Powers Authority entered into a Privacy and Security Agreement (Agreement) in order to ensure the privacy and security of electronic sources, including, but not limited to, the Applicant and Recipient Income and Eligibility Verification System (IEVS), the Social Security Administration (SSA) information and Medi-Cal Eligibility Data System (MEDS) information, as well as electronic and physically stored Personally Identifiable Information (PII). PII is defined as any information that can be used to search for or identify individuals, or can be used to access their files, including, place and date of birth, driver's license number, or mother's maiden name, and may also include other information such as medical, educational, financial, and employment information. The Agreement further defines PII as electronic, paper, verbal, or recorded and includes statements made by, or attributed to, the individual.

The Agreement outlines various technical security controls when it comes to storing and processing PII, including requiring all workstations, laptops, and other systems to install and actively use antivirus software solutions with automatic updates and be encrypted. The Agreement further states that all data transmission of PII outside of a secure internal network be

encrypted, and that this requirement pertains to any PII in motion such as website access, file transfer, and email. Despite these protections outlined in the Agreement, CDSS has cited counties for encouraging any type of email verifications/documents from applicants because of the privacy risk associated with emailing personal, private documents, particularly because counties are liable for any breach of privacy. When breaches do occur, California has strict requirements for informing those impacted which takes time and resources from counties.

*Data Breaches in Government.* Government officials worldwide are regularly subjected to data breaches. Most government agencies require strict training to warn and make employees aware of the danger of data breaches. Among many other training points, trainings teach employees to handle sensitive information with caution to avoid data breaches that would cause detriment. A December 21, 2022, New York Times article entitled “*How Hackers Used One Software Flaw to Take Down a County Computer System,*” detailed how Suffolk County was subject to a cyberattack that forced 10,000 county employees' emails to be disabled and private sensitive data was stolen.

According to the Attorney General’s Data Security Breach report, since 2013, 42 different county departments in California have reported a security breach to the Attorney General with almost half reporting a breach more than one time. The following are examples in the report:

- In Sacramento County’s Child, Family, and Adult Services Department, on June 22, 2021, Sacramento County was the target of a malicious phishing campaign in which an unknown threat actor obtained access to several employees’ credentials and began using those credentials to access the users’ Webmail. An internal investigation has determined that the exposed emails contained PII.
- Contra Costa County reported that, “on March 11, 2022, we completed an investigation regarding an incident of unauthorized access to certain County employee email accounts. Upon first learning of the activity, we immediately took steps to secure the email accounts and began the investigation with the assistance of a cybersecurity firm. The investigation determined that an unauthorized person accessed the accounts at various times between June 24, 2021, and August 12, 2021. The investigation was not able to determine whether any emails or attachments in the accounts were accessed or downloaded by the unauthorized individual; however, we were not able to rule out that possibility.”

*California’s Data Breach Notification Law (DBNL).* Effective 2003, California became the first state in the nation to require businesses and government agencies to notify residents of security breaches if private information was, or was reasonably believed to have been, stolen. California has very specific guidelines on breach notification, and the notification must include, at a minimum, the following:

- The name and contact information of the reporting person or business;
- A list of the types of private information that were or are reasonably believed to have been the subject of a breach;
- Whether notification was delayed as a result of law enforcement investigation;
- A description of the breach incident;

- Toll-free phone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number, driver's license or California identification card number; and,
- If the person or business making the notification was the source of the breach, then it must offer to provide identity theft prevention services at no cost for at least 12 months.

**Author's Statement:** According to the Author, "It is important that we modernize the functions of our government that are intended to serve Californians, especially those who are in need to access food to ensure their families don't go hungry. We know that Cal[Fresh] and CalWORK[s] are two programs that heavily impact low-income families. This bill is necessary to prevent program participants from missing out on these benefits."

**Equity Implications:** Access to public social services is key to eradicating poverty. The individuals in need of services come from home lives that may not allow for in-person information verification due to transportation, office hours, or limited physical ability. Electronic submission, which is secure, can provide an alternative way to ensure wider access and create equitable opportunities to receive aid.

Applicants and recipients of public social services are already experiencing a hardship that is causing a need for assistance. This population is important to protect when possible, including their information.

**Policy Considerations:** Public social service applicants are required to disclose sensitive information including, but not limited to, name, address, phone number, and Social Security number. Information that is improperly collected can be used for scams, identity theft, and/or financial theft. California is not immune to privacy breaches, the state has had 24.5 million breached records.

The Cybersecurity and Infrastructure Security Agency (CISA) lists suggestions to protect sensitive and personal information. Among many, the CISA suggests encrypting sensitive information. Last year, a similar bill was introduced, AB 991 (Alvarez), which aimed to accomplish the same goals of this bill, but did not include any protections to the language that ensured consumer information is safe, regardless of the modality the applicant chooses to utilize. While this bill aims to increase the number of ways a recipient or applicant can submit information to verify eligibility of public social services, the bill still includes email as an alternative method, which is highly susceptible to data breaches.

**Proposed Amendments:** In order to address the above policy considerations, the Committee proposes the author take the following amendments:

On page 2, in line 3, strike out "(1) No later than January 1, 2026, notwithstanding" and insert "Notwithstanding"

On page 2, in line 8, strike out "any", strike out line 9, on page 3, strike out lines 1 and 2 and insert: "the following means: (1) In-person reporting. (2) By telephone. (3) By facsimile. (4) By electronic means if submitted through a secure and encrypted method that permits the state or county agency, or client, access to the information changes, or verification after submission."

On page 3, strike out lines 3 to 10, inclusive, and insert: “(b) If a state or county agency receives information in an unsecure manner, the state or county agency shall immediately, upon receipt, inform the applicant or recipient of the privacy concern and provide a reasonable alternative method for resubmitting the information.”

**RELATED AND PRIOR LEGISLATION:**

**AB 991 (Alvarez) of 2023**, would have required state and county agencies to accept information from public social service applicants and recipients in any form. *AB 991 was held on the Assembly Appropriations Committee suspense file.*

**SB 46 (Corbett), Chapter 396, Statutes of 2013**, revised certain data elements included within the definition of personal information under the DBNL, by adding certain information that would permit access to an online account and imposed additional requirements on the disclosure of a breach of the security of the system or data in situations where the breach involves personal information that would permit access to an online or email account.

**SB 1386 (Peace), Chapter 915, Statutes of 2002**, required businesses and government agencies to notify residents of security breaches if private information was, or was reasonably believed to have been, stolen.

**REGISTERED SUPPORT / OPPOSITION:**

**Support**

Coalition of California Welfare Rights Organizations (Co-Sponsor)  
Western Center on Law & Poverty (Co-Sponsor)  
California Association of Food Banks  
California Council of The Blind  
Family Violence Appellate Project  
Grace Institute - End Child Poverty in Ca  
Legal Aid Society of San Diego  
San Diego Hunger Coalition  
Second Harvest Food Bank of Orange County

**Opposition**

County Welfare Directors Association of California

**Analysis Prepared by:** Bri-Ann Hernández / HUM. S. / (916) 319-2089