- **Briefing Paper** -

CalHEERS: Protecting Consumer Data by Developing and Implementing Strong Physical, Technical and Administrative Security Safeguards

The California Public Interest Research Group (CALPIRG) Education Fund

Spring 2013

Executive Summary

With the passage of the federal *Patient Protection and Affordable Care Act* (ACA), Californians will soon enjoy unprecedented access to affordable health insurance. Once fully implemented in 2014, 92 percent of non-Medicare eligible Californians will enjoy health care coverage provided either by their employer, the new *Covered California* run health insurance exchange market, or public benefit programs such as Medi-Cal. [1]

Last year Covered California established the *California Health care Eligibility, Enrollment and Retention System* ("CalHEERS") to provide Californians with easy access to the health care solutions.[2] The California Public Interest Research Group (CALPIRG) Education Fund is pleased to be able to provide recommendations on best practices and standards for the development and implementation of strong physical, technical and administrative security safeguards for the CalHEERS data ecosystem.

Key to the success of CalHEERS is the element of trust. Simply put, Californians must have confidence that their personal information will be safe, accurate, and used responsibly within CalHEERS. For its part, CalHEERS must be able to rely on the authentication of the individual with which they are engaging and the data they provide in order to offer accurate health care coverage solutions.

This report sets to highlight and address relevant data security and integrity concerns relevant to CalHEERS, and provide a framework for both protecting consumers and supporting the success of Covered California. CALPIRG Education Fund recognizes that Covered California has already addressed several data security and integrity concerns involving CalHEERS.[3] Yet the fact that 30% of data breaches in the U.S. targeted government and health care service providers during 2012 adds urgency to identifying threats and implementing robust policies that secure user data. This report lays out proactive measures that Covered California should take to protect and secure sensitive consumer data within the CalHEERS data ecosystem.[4]

Building on strong security protections found in the Health Information Portability and Accountability Act (HIPAA) Security Rule,[5] and the Fair Information Practice Principles (FIPs)[6], this report provides guidance for protecting against, assessing and addressing risks to data security and integrity, while encouraging a robust cyber-security culture.

---

[1] *Most non-elderly Californians covered under ACA*, UCLA Center for Health Policy Research, June 2012. Accessed online at http://www.universityofcalifornia.edu/news/article/27857

[2] California Healthcare Eligibility, Enrollment & Retention System (CalHEERS) Questions and Answers about the Intent to Award May 31, 2012, California Health Benefit Exchange. Accessed online at: http://www.healthexchange.ca.gov/Documents/CHBE-CalHEERS_Intent_Q-A_05_31_12.pdf

[3] In particular, CALPIRG Education Fund notes the *CalHEERS Development and Operations Services - Solicitation # Technical Requirements* & *Solicitation HBEX4 – Request for CalHEERS Development and Operations Services* (January 26, 2012) which acknowledge some of the issues raised in this report.

[4] The Open Security Foundation, DataLossDB, accessed online January 2013at: http://datalossdb.org/statistics?utf8=%E2%9C%93&timeframe=last_year

[5] Specifically, the HIPAA Security Rule, 45 CFR Section 164.300–164.318.

[6] A 1973 U.S. Federal Trade Commission's report established the *Fair Information Practices* - a.k.a "FIPs" or "Principles"- which deal with the accuracy, transparency and uses of information. Use of personal information, no matter the medium or purpose for which it is collected, should be guided by the FIP principles.

Guiding Principles

As the design and implementation of CalHEERS moves forward, we have the opportunity to build in data security mechanisms and procedures, rather than bolting them on later to an existing design or realized system. Various technical solutions exist to address specific issues outlined in this report. We do not in this report recommend a specific technology or mechanism. Instead, the report seeks to provide technology neutral guidelines and key principles Covered California should take into consideration as they move forward with CalHEERS development.

These include, but are not limited to, the following guiding principles:

1. **Trust:**
   Californian consumers should be able to trust that their personal information will be safe, secure, used responsibly, exposed only to those specifically authorized to access the data, and stored and retrievable under strong security mechanisms. Policies and procedures, as detailed below, should be put in place so that consumers have the confidence and trust in CalHEERS necessary to ensure its success.

2. **Accuracy & Reliability of Data:**
   CalHEERS should take reasonable steps to assure data integrity by implementing policies and procedures that protect information from improper alteration or destruction. Preventing those who do not have access to sensitive data from accessing it, limiting the degree of access to sensitive data for those who do require it, and monitoring user behavior to identify and prevent inappropriate access or modification of sensitive data are all key to maintaining data security and integrity.

3. **Restrictive:**
   The collection of data should be minimal in scope, servicing only the direct needs for which data is collected. Access to collected information must also be minimal, following the principal of "need to know". Both elements are important to avoid the misuse or abuse of sensitive personal information.

4. **Accountability:**
   Whether intentionally or not, system users can put the information held by CalHEERS at risk.[7] Data managers should be able to conduct audits to accurately detail who accesses information, what actions they are taking, from which locations the system is accessed, and at what times. This is crucial to preventing, minimizing, and addressing potential data breaches.

[7] While much of an organization's focus is put on external threats, research has found that up to 26% of breaches and data loss incidents were a result of internal losses. See Open Security Foundation, DataLossDB, accessed online January 2013at: http://datalossdb.org/statistics?utf8=%E2%9C%93&timeframe=last_year

Key Policy Recommendations

Our report makes the following policy recommendations:

1. **Data incident plans:** CalHEERS should put into place data incident plans, to ensure a rapid and effective response in the event a data breach or other data incident does occur. Such a plan will include a check list of required actions staff can immediately take in order to prevent further damage to the system, contain threats, and preserve existing forensic evidence**.**

2. **Protecting data security and integrity**: We recommend two key policies for the CalHEERS ecosystem. First is *Role Based Access* – i.e. preventing those who do not require access to sensitive data from getting it while limiting the degree of access to sensitive data for those who do require it. Second, we recommend monitoring user behavior to identify and prevent inappropriate access or modification of sensitive data.

3. **CalHEERS ID number:** In order to prevent social security numbers from being used as CalHEERS identifiers, we recommend creating a unique CalHEERS identifier (ID number) assigned to each individual consumer after an initial sign-up process. This new CalHEERS ID number will be linked to each individual's profile, but will not display any of their personal identifiable information. The number could migrate from CalHEERS to relevant insurance provider, and could then be used to track and monitor each consumer's history throughout the CalHEERS system without putting at risk sensitive user information.

4. **Two-stage authentication:** When users first register onto the online CalHEERS system, consumers should be authenticated through a two-stage authentication system. This means that in addition to their login ID and password, users will be asked to provide an additional verification code, sent via SMS or email to a device that only they can access.

5. **Staff oversight:** To ensure that all staff and assister activity is monitored and controlled for consumer protection:
    a. Assisters and CalHEERS staff must be assigned unique individual credentials with specific and limited roll-based permissions that can be audited to monitor actions throughout the system.
    b. Detailed logs regarding Assisters and other CalHEERS staff activity must be created and retained. Auditors must be able to recognize when an assister has acted on behalf of a consumer, and what actions the *Assister* has taken.
    c. Exiting staff profiles must be deleted from the system to prevent unauthorized access.
    d. Two-stage verification must be required for Assister and staff sign-in.
    e. Instruction on security and data protection policies must be included in the training of Assisters and other CalHEERS staff.

Introduction

Covered California was established as California's health care market exchange as part of statewide efforts to implement the *Patient Protection and Affordable Care Act* (ACA). Covered California's mission is to increase the number of Californians with health insurance, improve the quality of health care, reduce health care coverage costs and make sure California's diverse population has fair and equal access to quality health care.

Last year Covered California established the *California Health care Eligibility, Enrollment and Retention System* ("CalHEERS") to provide Californians with easy access to the health coverage opportunities that will be available under the ACA. T he system will include an internet portal where individuals and small employers can sign up for health coverage for themselves or their employees, and see what subsidies are available to help defray the costs of coverage. The system will allow enrollees to shop for and compare plans based on price, benefits, out - of - pocket costs, and plan quality measures. The portal will also make it easier to enroll in Medi-Cal and Healthy Families programs through a single application process.[8]

Covered California recognizes the critical role earning the public's trust will play in ensuring its success. Covered California has made a commitment to accountability, responsiveness, transparency, speed, agility, reliability, and cooperation as part of its efforts to ensure the ultimate success of CalHEERS.[9]

This report outlines relevant security and integrity concerns throughout the data lifecycle within the CalHEERS (acquisition, storage, and disposal). Our report provides a framework for action that will both protect consumers and support the success of Covered California. We provide the background for protecting against, assessing and addressing risks to data security and integrity, while encouraging a robust cyber-security culture. The sections below lay out technology-neutral guidelines and key principles Covered California should take into consideration as they move forward with CalHEERS development.

Policy Recommendations to Enhance Integrity

1. Prioritizing Data Security

Consumers will be wary of participating in CalHEERS if they do not have confidence that their sensitive personal and medical data is protected. To alleviate these concerns CalHEERS must adopt and develop a robust security culture, wherein the safety and integrity of sensitive user data is given high importance and is an integral part of every employee's duties. To this end, CalHEERS should take the following actions:

- Establish a *Chief Data Security Officer* position whose responsibility will be to develop and implement clear administrative and physical system-wide data security stewardship (see elaboration below). This person will be responsible for internalizing a robust security

[8] California Healthcare Eligibility, Enrollment & Retention System (CalHEERS) Questions and Answers about the Intent to Award May 31, 2012, California Health Benefit Exchange. Accessed online at: http://www.healthexchange.ca.gov/Documents/CHBE-CalHEERS_Intent_Q-A_05_31_12.pdf

[9] Accessed online at http://www.healthexchange.ca.gov/Pages/HBEXVisionMissionValues.aspx

culture throughout CalHEERS so that data security becomes a core element in the daily activity of every employee.[10]

- Designate data security and integrity security staff across the CalHEERS system. Staffing should be sufficient to complete system-wide security audits that monitor for unauthorized or unlawful access or activity which are critical to maintain the integrity of the CalHEERS. Under the direction of the Chief Data Security Officer, data managers should have the authority and technical ability to conduct audits that accurately detail who accesses information, what actions they are taking, from which location is the system being accessed, and at what times.
- Develop and implement policies, workflows, incident management plans, and trainings that ensure the security and integrity of the CalHEERS ecosystem. Data security policies and training should include all staff, vendors, contractors and others operating within the CalHEERS ecosystem. Such policies should include: [11]
    1. Development and use of data security check lists;
    2. Identification of potential data security risks to the system (e.g. physical loss or damage to devices, passwords are compromised, external attacks on servers, etc.);
    3. Development of action plans that address identified risks to CalHEERS;
    4. Design and implementation of data backup and recovery protocols;
    5. Training of staff in data protection policies and promote compliance;
    6. Performance of routine data security audits;
    7. Provision of data security assurances across multiple devices platforms (mobile, tablet, PC) and operating systems (e.g., Apple iOS, Microsoft Windows).
    8. Develop and maintain data security documentation, including:
        - Completed checklists,
        - Risk management action plans,
        - Data incident plans,
        - Up to date data security and integrity policies and procedures,
        - Regular security risk analysis reports,
        - Documentation of regular backups and software updates,
        - Documentation of completed data security trainings for staff,
        - Documentation of regular security audit reports,
    9. Monitor policy implementation, and update as needed over time.

Policy Recommendation: Data incident plans

CalHEERS should put into place data incident plans, to ensure a rapid and effective response in the event a data breach or other data incident does occur. Such a plan will include a check list of required actions staff can immediately take in order to prevent further damage to the system, contain threats, and preserve existing forensic evidence**.**

[10] See Thomas Schlienger & Stephanie Teufel, *Information Security Culture: From Analysis to Change*, Proceedings of ISSA 2003, Johannesburg, South Africa, 9-11 July 2003.

[11] While Covered California has addressed some of the data security and integrity issues in their technical requirements, there is still more to be done. We highlight these points to provide a complete picture of a robust security culture.

2. Safe Data Storage Policies

Physical, technological and managerial precautions are crucial to maintain the security and integrity of any large database. This is particularly true of databases that hold sensitive personal and health related information such as CalHEERs. Increasingly, we see sophisticated criminal organizations identifying and specifically targeting large systems that hold large quantities of sensitive personal information. Given the breadth and complexity of the CalHEERS system, a multi-pronged approach is necessary. To prevent theft or loss of sensitive data, policies should be put in place that limit access to such information, secure physical devices at work stations and in locked rooms, manage the use of physical keys, and restrict the ability to remove devices from a secure area.

Incidents reported to Health & Human Service's Office for Civil Rights show that more than half of all these data loss cases consist of missing devices, including portable storage media (e.g., thumb or flash drives, CD or DVD disks), laptops, handheld devices, desktop computers, hard drives taken out of machines, lost and stolen backup tapes, and even entire network servers.[12] To prevent loss, all computers should be locked down at work stations, and servers stored behind locked doors. Physical work stations, offices where sensitive health care data is stored or may be accessed, and data storage units must be secured and supervised to prevent un-authorized access. If offsite cloud-based data storage is used within the CalHEERS ecosystem, the Chief Data Security Officer should insure that that they meet CalHEERS data security and integrity standards and procedures.

Where possible, systems with sensitive personal information should be separated from non-sensitive systems required for day to day use. Sensitive consumer data should be stored and locked separately from other office material. This will prevent loss or exposure of sensitive data through unprotected systems.

Sensitive consumer data provided to CalHEERS should not be readily available for download and/or copying for all but a small group of authorized staff. To this end, the use of CD burners, thumb drives, and other portable data devices should be restricted within the CalHEERS ecosystem.[13]

Data destruction and device disposal protocols must be set and implemented to ensure that sensitive data is not lost or exposed during the disposal, reuse, or back-up of all hardware, electronic media, and digital devices used within the CAlHEERS ecosystem.

3. Managerial protections:

In addition to physical safeguards, policies must be put into place to protect sensitive data. At a technical level, such policies would include the use of Secure Socket Layer (SSL) or HTTPS transmission encryption, and encryption-at-rest for the storage of sensitive consumer information controlled by CalHEERS. In addition, these procedures must ensure that all antivirus, firewall, and operating software are updated regularly.

---

[12] For more on the protection of data and systems see *Internet:10 Best Practices For The Small Healthcare Environment*, Health and Human Services, V 1.0 November 2010, p. 14.

[13] To the extent possible, sensitive consumer data should never be place on laptops, external hard drives, flash drives, tablets or other mobile device that can be lost or stolen. If they must be, strong disk-based encryption or encrypted disk images must be used so that even in the event of a loss, no sensitive information would be compromised.

Policy Recommendations to Preserve Data Reliability

The existences of accurate, secure and up-to-date data backups are key to maintaining data integrity across CalHEERS following any significant data security event. Critical files should be systematically copied onto backup media. These can (and should) be in secure off site locations. In addition, meticulous data recovery plans should be put into place in order to be able to restore critical CalHEER data in case of loss.

Emergency recovery preparation should include plans to access to backup data and restore system wide functionality. Relevant staff should train and practice emergency data recovery procedures since this requires knowledge about where the backups are stored, how they were prepared, and what types of equipment are needed to read them. Combined, these procedures will ensure that localized data loss due to a virus infection, cyber attack, theft, or natural disaster will not have devastating effects on the CalHEERS system.

1. Role-based Controlled Access

Given the complexity on the CalHEERS ecosystem, it is not possible nor is it reasonable to craft a "one size fits all" approach to designating access. We recommend recognizing the different users in this ecosystem, identify their needs, and addressing the unique challenges each group places on the entire CalHEERS ecosystem in regards to data security and integrity.

Specifically, there are (at least) three user types in the CalHEERS ecosystem, as follows:

User Type	Characteristics	Unique Needs	Unique Challenges
Consumers	• Consumers looking to gain access to affordable health coverage. • Users will provide some level of sensitive personal identifiable information (PII), and must be sufficiently authenticated in the system. • Users will require specialized authentication procedures.	1) Easy access. 2) Infrequent access once enrolled. 3) Authentication of user identity. 4) Access from different locations and devices. 5) Varying technical skill levels. 6) Possible reliance on "Assisters".	1) Access to system from unsecured environments. 2) Exposure to web-based threats. 3) Ability to access the system numerous times while saving partial information until form is completed.
CalHEERS Staff	• Assisters, health care exchange personnel, county officials, and health plan providers who need to access to user data. • Each employee accessing data systems must be	1) Daily access must be easy. 2) Potential access to large amounts of sensitive consumer data must be restrictive. 3) Legitimate work purposes may	1) Unique access levels are required for each user ID. 2) User ID activity must be tracked and recorded for audit purposes.

	provided with a unique identifier which will grant customized access levels. • Staff will be accessing the system on regular basis from controlled environments, providing administrators a higher level of control and verification.	require sharing and accessing data.	
3rd Parties	• A collection of employees, vendors, consultants, and other staff providing different services and input into the system.	1. Legitimate work purposes may require sharing and accessing data. 2. Access must be easy. 3. Assisters must be able to act on behalf of consumers. 4. Unique access levels are required for each user ID. 5. User ID activity must be tracked and recorded for audit purposes.	1) Location and technology may vary among different users. 2) Potential access to large amounts of sensitive data. 3) Unique access levels are required for each user ID. 4) User ID activity must be tracked and recorded for audit purposes.

Policy Recommendation: data security and integrity

To protect data security and integrity, we recommend two key policies for the CalHEERS data ecosystem. First is *Role Based Access* – i.e. preventing those who do not require access to sensitive data from getting it while limiting the degree of access to sensitive data for those who do require it. Second, we recommend monitoring user behavior to identify and prevent inappropriate access or modification of sensitive data.

To preserve data security and integrity, guidelines must be drafted to define each user type, and to provide individual users with the appropriate level of access required by their role while addressing the unique challenges each group places on the entire system. Guidelines should include the following elements:

- Policies for terminating clearance and access when a consumer or staff member no longer requires access to the CalHEERS ecosystem.
- Procedures to review and modify an individual's degree of access to the CalHEERS ecosystem.
- Protocols to track and record user activity for audit purposes.

Remote Identity Authentication

As noted, each of the different user types will require a unique solution. However, the methodology to address this problem of remote authentication is essentially the same for all. The guiding framework for this endeavor was laid out by the *Office of Management and Budget* (OMB) Memorandum. M-04-04 was followed by the technical guidance developed by the *National Institute of Standards and Technology* (NIST) for government agencies to use for identifying the appropriate authentication technologies that provide secure electronic services that protect individual privacy.

Identity authentication - How do we know you are who you say you are?
OMB recommends a five-step process in determining the appropriate assurance level required for each user type:

i. Conduct a risk assessment for remote authentication measuring the severity of potential harm and the likelihood of adverse impacts to the system if there is an error in identity authentication.[14]
ii. Map identified risks to the applicable assurance level.
iii. Select appropriate technology solutions to address the identified risks.
iv. Verify that the implemented technology solutions achieve the required assurance level.
v. Continue to reassess the system to determine technology continues to meet existing requirements.

The required level of authentication assurance should be determined based on the potential damage caused by an authentication error on:

i. Inconvenience, distress, or damage to standing or reputation;
ii. Financial loss or agency liability;
iii. Harm to agency programs or public interests;
iv. Unauthorized release of sensitive information;
v. Personal safety; and/or
vi. Civil or criminal violations.

OMB defines four levels of electronic authentication assurance and identifies the criteria for determining the level of authentication assurance. Level 1 is the lowest assurance, and Level 4 is the highest. The levels are based on the degree of confidence needed in the process used to establish identity and in the proper use of the established credentials. As the consequences of an authentication error and misuse of credentials become more serious, the required level of assurance increases.

Four levels of electronic authentication assurance:
Level 1 - Little or no confidence in the asserted identity's validity.
Level 2 - Some confidence in the asserted identity's validity.
Level 3 - High confidence in the asserted identity's validity.
Level 4 - Very high confidence in the asserted identity's validity.

Following is a summary of the technical requirements specified in NIST SP 800-63-1 for the four levels of assurance defined by OMB:

Level 1 requires little or no confidence in the asserted identity. No identity proofing is required at this level, but the authentication mechanism should provide some assurance that the same individual is accessing the protected transaction or data. To be authenticated, the claimant must prove control of the token through a secure authentication protocol.

[14] Guidance for conducting a risk analysis is available in OBM Circular A-130 and in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

Level 2 requires confidence that the asserted identity is accurate. Level 2 provides for single-factor remote network authentication, including identity-proofing requirements. Successful authentication requires that the claimant prove through a secure authentication protocol that the claimant controls the token. Assertions issued as a result of a successful authentication are either cryptographically authenticated by relying parties (using approved methods) or are obtained directly from a trusted party via a secure authentication protocol.

Level 3 is appropriate for transactions that need high confidence in the accuracy of the asserted identity. Level 3 provides multifactor remote network authentication. At this level, identity-proofing procedures require verification of identifying materials and information. Authentication is based on proof of possession of a key or password through a cryptographic protocol. Cryptographic strength mechanisms should protect the primary authentication token (a cryptographic key) against compromise by the protocol threats, including eavesdropper, replay, online guessing, verifier impersonation, and man-in-the-middle attacks. A minimum of two authentication factors is required. Authentication requires that the claimant prove control of the token through a secure authentication protocol. The token must be unlocked with a password or biometric representation, or a password must be used in a secure authentication protocol, to establish two-factor authentication. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using approved methods) or are obtained directly from a trusted party via a secure authentication protocol.

This is the recommended requirement for consumers, Assisters, and other low-level staff.

Level 4 is for transactions that need very high confidence in the accuracy of the asserted identity. Level 4 provides the highest practical assurance of remote network authentication. Authentication is based on proof of possession of a key through a cryptographic protocol. This level is similar to Level 3 except that only "hard" cryptographic tokens are allowed, cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key that is bound to the authentication process. Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through a secure authentication protocol that the claimant controls the token. Eavesdropper, replay, online guessing, verifier impersonation, and man-in-the-middle attacks are prevented.

This is the recommended requirement for vendors, consultants, and CalHEERS staff.

Implementing Remote Identity Authentication

NIST's Special Publication (SP) 800-63-2, *Electronic Authentication Guideline*, provides technical guidance on existing and widely implemented methods for remote authentication.[15] The basic concept behind the methods described in the guidelines is based on the authentication of information known only by the individuals that are later used to create identity credentials. M-04-04 defines four levels of authentication, which NIST SP 800-63-1 later expands on the minimum technical requirements for remotely authenticating the identity of users for each level.[16]

1. Authentication Factors

To ensure that sensitive data remains accurate and protected at all times, CalHEERS must be able to successfully authenticate the individual user as they approach the CalHEERS ecosystem. To this end, we recommend Covered California develop an authentication system that incorporates the following principles:

i. Authentication procedures must differ for different user types. Consumers should be provided with simpler and user-friendly solutions while staff may be provided with more robust access solutions (for example, a rotating token key fob).
ii. Covered California should establish a unique CalHEERS identifier, to prevent sensitive social security numbers being used to track an individual across the system (see box below).
iii. Covered California should establish two-factor authentication systems for all users, inclusive of information only the user knows (such as user ID and a password) and information of which only the user has possession - for example a secondary access code.

Policy Recommendation: CalHEERS ID number

How an individual record is entered, identified, and tracked throughout the CalHEERS system is a problem that must be addressed. In order to prevent social security numbers from being used as CalHEERS identifiers, we recommend creating a unique CalHEERS identifier (ID number) assigned to each individual consumer after an initial sign-up process. This new CalHEERS ID number will be linked to each individual's profile, but will not display any of their personal identifiable information. The number could migrate from CalHEERS to relevant insurance provider, and could then be used to track and monitor each consumer's history throughout the CalHEERS system without putting at risk sensitive user information.

2. Password Authentication

As CalHEERS is a public facing system intended for easy use by the general public, determining the password criteria is a thorny task. For security purposes, the system should require a long and complex password comprising of letters, numbers and special characters. Yet for the normal users, it often proves difficult to remember such complex passwords. Taking these two factors into consideration, the CalHEERS should insist on a long password, at minimum 12 digits.[17] The combination of a lengthy password and challenge questions should provide consumers with reasonable protection against un-authorized access to their sensitive data.[18]

---

[15] The summary below is based on the following publication: Shirley Radack (Editor), Electronic Authentication: Guidance for Selecting Secure Techniques, Information Technology Laboratory, National Institute of Standards and Technology. Accessed online September 2012 at: http://www.itl.nist.gov/lab/bulletns/bltnaug04.htm

[16] Topics covered in NIST SP 800-63-1 include discussion of the e-authentication process, the use of tokens, identity proofing, authentication protocols, and assertion mechanisms. Definitions of technical terms, references to general and NIST publications, and specific information about the use of passwords are also included in the publication.

[17] Research indicates that given the strength of today's computing systems the use of special characters are not effective in slowing down brute-force attack on passwords as are lengthy passwords.

[18] Some consumers may lack the technical ability (such as access to a mobile phone) or the skill to access an online system with two-stage verification. However, the "Assisters" program is designed to provide help to precisely those types of consumers.

Policy Recommendations for Identity Authentication

Consumers should be encouraged to access and engage with CalHEERS. To this end, it is important to simplify and streamline the user experience as much as possible. That said, convenience should not come at the cost of robust data security.

CalHEERS must trust the identity of the individual who is engaging with the system and the data he or she provides in order to provide accurate options for their health care coverage needs. According to recently published documents[19], a system for consumer verification is already in place. To verify each consumer's identity, the online CalHEERS application will administer an identification proofing process that will generate three to five challenge questions based on the information the consumer initially provides. The tool will randomly generate questions based on information from external databases, such as a previous address where an individual lived, that the consumer must verify prior to continuing.

The CALPIRG Education Fund recommends that CalHEERS consider integrating a two-stage verification system for when consumers initially sign up, to be followed by challenge questions during subsequent sign-in sessions. A two-stage verification system for consumers would consist of information only the user knows (such as user ID and a password) and information only the user possesses - for example a secondary access sent to the user's mobile phone or email.[20]

Policy Recommendation: Two-stage authentication

When users first register onto the online CalHEERS system, consumers should be authenticated through a two-stage authentication system. This means that in addition to their login ID and password, users will be asked to provide an additional verification code, sent via SMS or email to a device that only they can access, each time they attempt to login.

Policy Recommendations Supporting Data Security Implementation

1. Audit controls and reports

As noted earlier, data security audits must be built into system-wide work protocols. Audits must be supported by the design and implementation of the underlying technology and appropriate procedures must exist to ensure audits are triggered at the right times, professionally performed, analyzed and acted upon.

This is in order to ensure that sensitive personal information does not leak through abuse or neglect, is not altered without authorization, or is not accidently destroyed. To facilitate successful auditing of data security, automatic logs should be created each time a user logs into CalHEERS recording time, location, IP address, and activity during login.

Assisters will play a key role in the success of the CalHEERS system by providing guidance and help to consumers as they navigate this new system. For it to succeed, Assisters must be able to add and

[19] See *Supporting Statement for Data Collection to Support Eligibility Determinations for Insurance Affordability Programs and Enrollment through Affordable Insurance Exchanges, Medicaid and Children's Health Insurance Program Agencies*.

[20] The Assisters program will be able to provide support for those consumers who may not have sufficient levels of access to the technical skills or resources needed for two-stage verification.

modify information as well as act on the behalf of consumers. Yet to earn the trust of consumers, Assisters' actions throughout CalHEERS must be monitored, audited, and held accountable for any possible misuse of personal data.

Policy Recommendation: Staff oversight

In order to implement a high level of control and oversight over Assisters and other staff, CalHEERS should implement the following policies:

1. Assisters and CalHEERS staff must be assigned unique individual credentials with specific and limited roll-based permissions that can be audited to monitor actions throughout the system.
2. Exiting staff profiles must be deleted from the system to prevent unauthorized access.
3. Passwords must be at least 12 digits and automatically set to change periodically.
4. Two-stage verification must be required for Assister and staff sign-in.
5. Detailed logs regarding Assisters and other CalHEERS staff activity must be created and retained. Auditors must be able to recognize when an assister has acted on behalf of a consumer, and what actions the Assister has taken.
6. Instruction on security and data protection policies must be included in the training of Assisters and other CalHEERS staff.

Documented audits should take place on a regular basis and encompass all user types. In addition to random spot checks, criteria should be developed by the Chief Data Security Officer to trigger in-depth audits. Criteria could include simultaneous log-ins from different devices, unusual login locations, erratic login behavior, and attempts to access data outside of permissions. Audit reports should be documented and stored for future reference.

The Chief Data Security Officer should oversee the periodic technical and non-technical system wide evaluation to ensure that they meet data security requirements and policies. This is especially critical when there are system or environmental changes (such as setting up new data servers or expanding offices).

2. Implementation Policy Assurances

The CalHEERS ecosystem will undoubtedly be vast, with many different users accessing it. In addition to establishing and monitoring their own data security culture, Covered California must also validate that external vendors, consultants, and Assisters all abide by data security and integrity policies. Contract terms and policies should be put into place to ensure that all such vendors, consultants, and Assisters are sufficiently trained on system data security measures, and audited appropriately to ensure compliance with said data security and integrity policies.

3. Sanction Policy

Data security and integrity policies should be stated up-front and made clear to all external vendors, consultants, and Assisters. Clear, actionable, and appropriate sanctions for failure to comply with these policies and procedures must also be explained to external vendors, consultants, and Assisters prior to engaging their services. The key role external vendors will play in setting up and maintaining CalHEERS warrant particularly severe penalties for failure to comply with data security and integrity policies and standards set by CalHEERS.