ConsumersUnion
POLICY & ACTION FROM CONSUMER REPORTS

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE
CENTER FOR DEMOCRACY & TECHNOLOGY

Preserving Integrity in California's Healthcare Eligibility, Enrollment and Retention System (CalHEERS): Policy Recommendations

April 2012

One of the primary values of the California Health Benefit Exchange (the Exchange) is integrity, defined as: "earn[ing] the public's trust through its commitment to accountability, responsiveness, transparency, speed, agility, reliability, and cooperation."[1] Consistent with this core value, the Exchange, the Department of Health Care Services (DHCS) and the Managed Risk Medical Insurance Board (MRMIB) have the opportunity to develop workable privacy and security policies for the California Healthcare Eligibility, Enrollment and Retention System (CalHEERS) that build confidence and enhance integrity so that consumers, health plans, and others interacting with CalHEERS trust that personal information collected, accessed and disclosed is handled responsibly. Such policies will need to balance the information needs of the agencies with the rights of individuals to have personal information protected by reasonable privacy and security safeguards.

New federal regulations,[2] specifically governing the privacy and confidentiality required for information obtained and transmitted in the Exchange, will help foster that balance by requiring that the Exchange adopt specific policies that implement fair information practice principles. The regulations provide a roadmap for ensuring that the Exchange, DHCS and MRMIB create privacy and security policies that implement the fair information practice principles and that CalHEERS collects, maintains, and discloses only the minimum necessary personally identifiable information, while supporting state activities that promote and encourage eligibility, enrollment and retention of millions of eligible individuals in health coverage programs.

Effective implementation of the federal regulations will help ensure that on the first day CalHEERS opens its doors for business, consumers trust that the Exchange, DHCS, and MRMIB offer "a consumer-friendly experience that is accessible to all Californians, recognizing the diverse cultural, language, economic, educational and health status needs of those [it serves];"[3] a system that will "[expand] coverage and access, [improve] health care quality, [promote] better health and health equity, and [lower] costs for all Californians."[4] Undertaking these initial and basic steps to protect privacy at the outset will help the Exchange, DHCS, MRMIB and their partners ensure CalHEERS operates effectively and with the trust and confidence of the public.

[1] Accessed online at http://www.healthexchange.ca.gov/Pages/HBEXVisionMissionValues.aspx
[2] 45 C.F.R. §155.260.
[3] California Health Benefit Exchange "Vision, Mission, Values." http://www.healthexchange.ca.gov/Pages/HBEXVisionMissionValues.aspx
[4] California Health Benefit Exchange "Vision, Mission, Values."

Adopting Policies to Implement Federal Exchange Regulations

Federal regulations require health insurance exchanges to adopt policies that implement the fair information practice principles set forth in the "Nationwide Privacy and Security Framework for the Electronic Exchange of Individually Identifiable Health Information," initially developed by the U.S. Health and Human Services Office of the National Coordinator of Health Information Technology.[5] In brief, this Nationwide Framework implements a model of strong data stewardship, where entities that access, use, disclose or retain personally identifiable information are subject to a set of obligations (imposed through applicable law and the adoption of responsible business practices) regarding when they are permitted to collect, use, disclose and/or retain such information and the types of security safeguards that must be employed to support data use policies and practices.

The Nationwide Framework was initially developed to apply to personal health information, but the new federal exchange regulations require that the Nationwide Framework be applied to any personal information collected, accessed, used, disclosed or retained by an exchange.[6] Specifically, federal regulations require exchanges to develop and implement policies that address all of the following fair information practices:[7]

- **INDIVIDUAL ACCESS** Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.

- **CORRECTION** Individuals should be also provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.

- **OPENNESS AND TRANSPARENCY** There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.

- **INDIVIDUAL CHOICE** Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.

- **COLLECTION, USE, AND DISCLOSURE LIMITATION** Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.

- **DATA QUALITY AND INTEGRITY** Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-

[5] Office of the National Coordinator for Health Information Technology, The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information, accessed at http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy___security_framework/1173
[6] 45 C.F.R. §155.260(a)(3) and the preamble found in the Federal Register (FR) /Vol. 77, No. 59, page 18339 (March 27, 2012).
[7] 45 C.F.R. §155.260(a)(3)(i)-(viii) and Federal Registry, page 18450.

date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.

- **SAFEGUARDS** Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.[8]

- **ACCOUNTABILITY** These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non- adherence and breaches.

Policy Recommendations for Implementing the Nationwide Framework

Consumers Union (CU) and The Center for Democracy and Technology (CDT) provide the following initial recommendations for policies that the Exchange, DHCS, and MRMIB should adopt as they develop the CalHEERS system. Because the policies should reference and support the information flows needed to operate CalHEERS, they will need to be developed in the process of finalizing decisions about CalHEERS information flows. Thus, what follows is an initial set of recommendations; CU and CDT intend to make subsequent policy recommendations as CalHEERS operations are further developed.

The recommendations are organized first by general policy considerations that should guide the agencies in considering how to implement the Nationwide Framework,[9] followed by specific policy recommendations, where appropriate.

INDIVIDUAL ACCESS

Under the Individual Access principle, individuals, both applicants and non-applicants applying on behalf of applicants, should be provided with a simple and timely means to access and obtain their individually identifiable information in a readable form and format. Generally, the Exchange, DHCS, and MRMIB need to consider how this principle best applies to information collected, accessed or shared in CalHEERS. To that end, CalHEERS should be designed to:

- Provide individuals with a reasonable and accessible means of access to their own individually identifiable information collected or accessed by CalHEERS;
- Enable individuals to obtain their own personal information easily, consistent with security needs for authentication and the functional impairments of the individual;
- Provide prompt access to such information so as to be useful; and
- Present such information in a readable form and format, including in electronic format.

[8] While proper security safeguards are also crucial, CU and CDT will provide specific recommendations for implementing security measures in a subsequent paper.

[9] Office of the National Coordinator for Health Information Technology, The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information, accessed at http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy___security_framework/1173 .

CORRECTION

The Correction principle provides individuals, both applicants and non-applicants, with a timely means to dispute the accuracy or integrity of their individually identifiable health information and to have erroneous information corrected or to have a dispute documented if their requests are denied. Generally, the Exchange, DHCS, and MRMIB should adopt policies applicable to CalHEERS to ensure that:

- Individuals have practical, efficient, and timely means for disputing the accuracy or integrity of their individually identifiable health information; and
- Individuals can easily correct information or dispute a document when their requests are denied.

OPENNESS AND TRANSPARENCY

According to the Openness and Transparency principle, the public should be informed about policies and processes that directly affect individuals, both applicants and non-applicants, and/or their individually identifiable information. Generally, the Exchange, DHCS, and MRMIB should adopt policies that enable CalHEERS to ensure that:

- Individuals are able to understand what individually identifiable information is collected or accessed by CalHEERS; how that information is used and disclosed; for how long it is retained; and whether and how they can exercise choice over such collection, use, and disclosure;
- A notice of policies and operations -- including the parameters of information collection, use and disclosure - is made in a timely way and, wherever possible, in advance of the collection, use, and/or disclosure of individually identifiable information; and
- Policies and procedures are communicated in a manner that is appropriate and understandable to all individuals who may interact with CalHEERS.

INDIVIDUAL CHOICE

Under this principle, individuals, both applicants and non-applicants, should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable information. Generally, the Exchange, DHCS, and MRMIB should adopt policies that ensure that CalHEERS provides:

- Individuals with reasonable opportunities to exercise some choice with respect to collection, use and disclosure of their individually identifiable information. What choices should be provided depends on the context for information sharing[10] – for example, information flows that are required for CalHEERS operations may be treated differently than those that would not be reasonably expected by an individual seeking services through CalHEERS;
- Individuals the ability to designate someone else, such as a family member, care-giver, or legal guardian, to make decisions on their behalf;

[10] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*, March 2012, available at http://www.ftc.gov/opa/2012/03/privacyframework.shtm

- Individuals the ability to make their own decisions that are communicated through the use of chosen translators, legally recognized translation systems, or language facilitators; and
- A fair and not unduly burdensome decision making process.

Federal regulations require California to adopt policies that address the principle of individual choice and it is important that the Exchange, DHCS, and MRMIB consider what choices individuals will have with respect to information collected, used, or disclosed for purposes of CalHEERS. However, overreliance on consent – and failing to comprehensively address the other fair information practices in the Nationwide Framework – will result in weak privacy protection in practice. In the case of CalHEERS, individuals will be required to submit certain information (or to authorize the submission of information) necessary to secure coverage or determine eligibility for subsidies. Consequently, if individuals want to use CalHEERS to avoid penalties under the Affordable Care Act, they will have to provide information (or authorize the provision of information) necessary to facilitate CalHEERS operations.

Consequently, CU and CDT recommend the following specific CalHEERS policies regarding individual choice:

- Individuals who might be eligible for CalHEERS services should be specifically asked for consent before an actual application is initiated. A specific example of this might be CalFresh families, who have not applied for health coverage, but who could affirmatively indicate that the information transferred from CalFresh to CalHEERS could be considered for purposes of applying for and determining the family's eligibility for health coverage.
- Consumers have the right to refuse consent for the sharing of specific information. For example, some individuals and families applying for health coverage may prefer NOT to be considered for insurance affordability benefits, which require disclosure of discreet financial information. The federal regulations allow applicants to opt out of consideration for insurance affordability programs.[11] The CalHEERS system and health coverage application process needs to provide the capacity for an applicant to explicitly decline to share financial information needed for determining insurance affordability programs by phone, in-person, website, and mail applications.
- During some specific interactions with CalHEERS, it will be vital to provide "just-in-time" consent before applicants are able to move forward in the application process.[12] For example, applicants must be able to understand the implications of the reconciliation process before they apply for advance payments of the premium tax credit. During the online application process, an applicant should not be able to apply for advance payments without some type of real-time warning or pop-up box that provides information about the repercussions of the reconciliation process and a consent box that ensures the applicant has read and acknowledged it before proceeding. For non-electronic applications, the insurance affordability programs should include practices that require sharing of just-in-time information and a check box indicating consent for the assister (via telephone or in-person) or on a paper

[11] 45 C.F.R. §155.310(b).
[12] This recommendation is consistent with recent privacy guidance issued by the Obama Administration. See Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers,* March 2012, available at http://www.ftc.gov/opa/2012/03/privacyframework.shtm, The White House, *Consumer Bill of Rights,* February 2012, available at www.whitehouse.gov/sites/default/files/**privacy**-final.pdf.

application (mailed in). Another situation where "just-in-time" consent should apply is for the release of sensitive information, which may include disclosure of immigration status, incarceration status, and/or health and disability status.

- Consent language should be written in a clear and concise manner, enabling individuals to understand to what exactly they are consenting. Consent language should be comprehensible to individuals of all cultural, language, economic, educational and health status needs.

COLLECTION, USE, AND DISCLOSURE LIMITATION

According to this principle, personally identifiable information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.

As a threshold matter, federal regulations prohibit exchanges from using or disclosing identifiable information about any individual collected in order to perform the core functions of an exchange required by the Affordable Care Act for any other purpose.[13] Such core functions include:

- Eligibility determinations for exchange participation and insurance affordability programs;[14]
- Enrollment in qualified health plans;[15]
- Small business health options program (SHOP);[16]
- Certification of qualified health plans;[17] and
- Certification of exemptions, oversight and financial integrity, and quality activities.[18]

This federal policy, by default, creates some limitations on how CalHEERS can use identifiable information; for example, explanatory material provided with the federal regulations (the preamble) indicates that information collected for exchange core functions cannot be used for marketing.[19] However, California is still required to establish its own policies to specifically address this principle. In addition, to the extent that CalHEERS takes on functions other than the core functions required by the Affordable Care Act, specific policies that set limitations on collection, use and disclosure of information will be needed in order to support and build public trust in those additional data flows.

Because CalHEERS is still in the planning stages, creating a final set of appropriate data use, disclosure and retention policies will not be possible until the data flows and operations of

[13] 45 C.F.R. §155.260(a).
[14] Subpart D governing exchange functions in the individual market. Federal registry at page 18451.
[15] Subpart E governing exchange functions in the individual market. Federal registry at page 18462.
[16] Subpart H governing exchange functions: the SHOP. Federal registry at page 18464.
[17] Subpart K governing exchange functions: certification of qualified health plans. Federal registry at page 18467.
[18] 45 C.F.R. §155.200.
[19] Patient Protection and Affordable Care Act; Establishment of Exchanges and Qualified Health Plans; Exchange Standards for Employers, 77 Fed. Reg. 18310, 18341 (Mar 27, 2012) (Amending 45 CFR § 155, 156, and 157). Accessed at http://www.gpo.gov/fdsys/pkg/FR-2012-03-27/html/2012-6125.htm. The preamble alludes to barring marketing by third parties—not the Exchange itself. We will provide recommendations on language in a later paper.

CalHEERS are determined with more certainty. The following recommendations should serve as a baseline approach for developing further policies:

Data Collection

- CalHEERS should provide consumers with the ability to *anonymously* explore or search the CalHEERS website to learn more about the health coverage programs and plans available to them, including insurance affordability programs. Browsers should be able to explore the website without first being required to consent to any sharing of information. Further, no information regarding such browsers or explorers (including her/his internet provider address) should be collected or saved (a.k.a. "cached") without the person affirmatively consenting to begin the application process. The technical design of the site should support this policy.
- Consistent with federal regulations, when an individual begins the application process, CalHEERS should collect only the minimum personally identifiable information necessary to complete the application.[20]
- When data about an individual exists in another database, agencies should consider whether it is necessary for a copy of that data to also be collected and stored in the CalHEERS system. For example, if it is possible for personally identifiable information stored in the federal "Data Services Hub" to be accessed for an eligibility determination then forwarded to CalHEERS, it is unlikely that the individual's personally identifiable information will need to be stored in the CalHEERS system. Matching against the Data Services Hub rather than saving the information locally allows an individual to be connected with appropriate coverage while minimizing the collection of additional information and storage of the data needed to make the eligibility determination in more than one place.

Data Disclosure

The federal regulations place responsibility on the Exchange to create privacy and security standards and apply the same or "more stringent" standards to all vendors, contractors, sub-contractors, issuers, health plans, agents, navigators, and other relevant entities as a condition of contract or agreement.[21] To adhere to the federal requirements, DHCS, the Exchange and MRMIB should ensure the following:

- Contract language includes common terms and standards that cannot be modified. The federal prohibition regarding use and disclosure of exchange information for non-exchange purposes must be included in contracts with all other relevant parties. Other CalHEERS data limitation policies enacted to implement this principle must also be included in such contracts.

CU and CDT anticipate that information collected by CalHEERS will also need to be used for important secondary purposes. As just one example, we hope that the state will use information that is part of CalHEERS to evaluate enrollment patterns and gaps in order to assess how well it is serving residents of the state. We urge the State to be transparent about such secondary uses and to seek input from stakeholders about potentially valuable uses of CalHEERS data.

[20] PPACA, Pub. L. 111-148, §1411(g)(1), 5 CFR §155.260(a)(1), Cal. Assembly Bill No. 1602 (2010). See also California Welfare and Institutions Code, Section 10500.
[21] 45 C.F.R. §155.260(b).

As an initial recommendation, and consistent with the Nationwide Framework's focus on collecting, using and disclosing only the minimum amount of information needed to accomplish a given purpose, we urge the Exchange, DHCS, and MRMIB to:

- Require the use of "de-identified" data for such purposes whenever possible. "De-identified" data is personally identifiable information that has been so stripped of common identifiers that there is no "reasonable basis" to believe it can be traced back to the subject.
- At a minimum, adopt HIPAA's de-identification standard and methodologies; and
- Strictly prohibit re-identification of any disclosed de-identified data in binding contracts and all policies.

Data Retention

- Under circumstances where personally identifiable information is being retained in another location, for example the federal Data Services Hub, the CalHEERS system should not retain duplicate information; and
- The agencies will also need to establish data retention policies for those circumstances when data is collected by the CalHEERS system. Retention policies should incorporate legitimate agency needs for the data but should not be longer than is reasonably necessary. For example, the retention period for information collected from persons deemed to be ineligible for certain programs should be different from the period for successful applicants who may want to rely on previously gathered information to facilitate more rapid recertification.

CDT and CU look forward to working with the Exchange, DHCS and MRMIB to continue developing recommendations on use, disclosure, and retention policies as CalHEERS is built.

DATA QUALITY AND INTEGRITY

Per the Data Quality and Integrity principle, the Exchange, DHCS, and MRMIB should take reasonable steps to ensure that individually identifiable information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner. Generally, the Exchange, DHCS, and MRMIB should adopt policies that enable the following:

- The Exchange, DHCS, and MRMIB should ensure that CalHEERS updates or corrects individually identifiable information when appropriate, and provides timely notice of these changes to individuals and to others with whom the underlying information has been shared;
- The agencies develop processes and deploy technical capabilities to ensure that CalHEERS can detect, prevent, and mitigate any unauthorized changes to, or deletions of, individually identifiable information; and
- The agencies develop methods to ensure individual accounts are not shared. Assisters, navigators, brokers and agents should access the CalHEERS system through a unique login, rather than using the login of the individual whom they are assisting. The source of all changes to an individual's personally identifiable information should be tracked in order to properly identify the source of any mistakes or misinformation.

SAFEGUARDS

Individually identifiable information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure. The federal regulations require exchanges to adopt security safeguards. The state must ensure the confidentiality, integrity, and availability of personally identifiable information created, collected, used or disclosed by the exchange. As stated above, CDT and CU will provide more specific security recommendations in a paper to follow.

ACCOUNTABILITY

The fair information practice principles should be implemented, and adherence assured, through appropriate monitoring, and other means should be in place to report and mitigate non-adherence and privacy or security breaches. Generally, the Exchange, DHCS, and MRMIB should adopt policies that apply to CalHEERS that ensure that:

- There is sufficient monitoring by CalHEERS for internal compliance including authentication and authorizations for access to or disclosure of individually identifiable health information;
- The three agencies have the ability to receive and act on complaints by individuals, including taking corrective measures; and
- The agencies develop reasonable mitigation measures, including notice to individuals and appropriate authorities of privacy violations or security breaches.

Conclusion

The Exchange, DHCS, and MRMIB are in a strong position to integrate into development of the CalHEERS system, as well as into each of their own policies and procedures, strong privacy and security protections to promote integrity and establish public confidence in this historic initiative. By adopting policies to implement fair information practice principles as required by the new federal exchange regulations, the Exchange, DHCS, and MRMIB will help foster and promote the values and goals of health reform.

Funded in part by The California Endowment

For more information contact:
Julie Silas, Consumers Union, jsilas@consumer.org (415) 431-6747 ext. 106 or
Kate Black, Center for Democracy and Technology, kate@cdt.org (415) 882-1714