ConsumersUnion®

POLICY & ACTION FROM CONSUMER REPORTS

January 14, 2013

Model Overarching Privacy Policies for Covered California[1]•

We at Covered California are committed to ensuring that all personally identifiable information is kept private and secure.

Personally identifiable information that is available, stored, or disclosed through Covered California is subject to these principles and policies:[2]

- Individual Access: Covered California shall provide individuals with a simple and timely means to access and obtain their personally identifiable health information in a readable form and format;

- Correction: Covered California shall provide individuals with a timely means to dispute the accuracy or integrity of their personally identifiable health information and to have erroneous information corrected or to have a dispute documented if their requests are denied;

- Openness and Transparency: Covered California is committed to openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable health information;

- Individual Choice: Covered California shall provide individuals a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their personally identifiable health information;

- Collection, use and disclosure limitations. Covered California shall create, collect, use and/or disclose personally identifiable health information only to the extent necessary to accomplish the specified purposes of Covered California and never to discriminate inappropriately. Specifically, Covered California is committed to:

  > Only collecting, maintaining, and disclosing the information strictly necessary to authenticate identity, determine eligibility, and determine the amount of the credit or reduction,[3]

---

[1] These overarching policies are intended to be an initial set of commitments by Covered California to individuals utilizing its services. More specific implementations of these policies should be developed as CalHEERS makes decisions on the data flows necessary to support Covered California's operations.

[2] According to 45 CFR § 155.260(a)(3), the Exchange is required to implement policies according to Office of the National Coordinator for Health Information Technology's Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy___security_framework/1173). These policies are an iteration of that Framework.

Social Security Numbers (SSNs) will not be required from individuals who are applying on behalf of other family members and not seeking health insurance benefits for themselves; SSNs will not be collected from individuals simply exploring Covered California or comparing plans;[4]

- Data quality and integrity: Covered California shall take reasonable steps to ensure that personally identifiable health 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;

- Safeguards: Covered California shall protect personally identifiable health information with reasonable operational, administrative, technical and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure;[5] and

- Accountability: Covered California shall implement these principles and assure adherence to them through appropriate monitoring and other means and methods put in place to report and mitigate non-adherence and breaches.

---

[3] This is a specific requirement of the Affordable Care Act. See Pub. L. 111-148, § 1411(g)(1)

[4] The restriction on the collection of Social Security Numbers is also one imposed by the Affordable Care Act. See Pub. L. 111-148 at § § 435.907(e)(1) and 155.305(f)(6).

[5] CalHEERs has already begun to establish these safeguards in the Enterprise Security Framework and in the business requirements. We applaud these initial efforts and will continue to provide feedback as additional details are released.