



California Department of Public Health Security Breach Notices

The California Department of Public Health (CDPH) is required to notify individuals when, regardless of the medium type (e.g., paper, electronic), certain "notice-triggering" personal information data elements were, or are reasonably believed to have been acquired by an unauthorized person. (NOTE: While Civil Code section 1798.29 focuses on unencrypted computerized data elements, the current state policy requires notification when a breach of an individual's personal information involves these same "notice-triggering" data elements or otherwise exposes individuals to substantial risk of harm, regardless of the data medium, and where such notification may allow those individuals to take steps to mitigate the risk of identity theft and/or other information-related crimes.

A copy of the applicable Security Breach Notice regarding each information security breach that involved personal information held by CDPH may be accessed below, by clicking on the link to the particular notice. The Security Breach Notices are organized by the particular CDPH program, office or unit involved in the breach and the date of the security breach.

The Program contact information is listed at the bottom of each Security Breach Notice. General information regarding CDPH Security Breach Notices can be found in [CDPH Frequently Asked Questions](#).

Security Breach Notices by the CDPH Program Name, Office or Unit

[CDPH, California Reportable Disease Information Exchange \(CalREDIE\), January 15, 2014](#)

Security Breach Notices by the Date of the Security Breach

[January 15, 2014, CDPH, California Reportable Disease Information Exchange \(CalREDIE\)](#)