

Memorandum

April 26, 2012

The Center for Democracy and Technology (CDT) and Consumers Union (CU) understand that the three agencies are interested in receiving recommendations on how to proceed and what standards to use when/if a breach of security occurs through the California Healthcare Eligibility, Enrollment, and Retention System (CalHEERS). California's security breach notification laws governing a breach of security are some of the strongest in the nation. Unlike HIPAA¹ and other security rules, the California security breach notification law applies to all types of unencrypted², personal information³ stored electronically, not just medical or health information. Additionally, California's security breach notification laws apply to all parties, government agencies, businesses, and people conducting business in California, not just HIPAA-covered entities.

Under California Civil Code sections 1798.82 and 1798.29,⁴ CalHEERS and any of its vendors⁵ are required to disclose a breach of any unencrypted personally identifiable information stored electronically. The disclosure must be made in "the most expedient time possible, without unreasonable delay,"⁶ the highest standard that exists under federal or state law. In situations where the personal information that is breached is not owned by the agency or business, the standard for notification is "immediately following discovery."⁷

Under California law, CalHEERS and any of its vendors will be required to issue a security breach notification,⁸ either on paper or electronically,⁹ that meets the following requirements:

¹ HIPAA's Security Rule, 45 C.F.R. 164, applies to covered entities. Whether or not the Exchange will be a covered entity will depend on the functions it carries out.

² The security breach notification law does not include a definition of encrypted or unencrypted data nor does it set any standard for encrypting data. While HIPAA does not specifically use the word unencrypted, CU and CDT recommend that CalHEERS adopt HIPAA's definition of 'data not secured by a technology' that renders it "unusable, unreadable or indecipherable to unauthorized individuals" in order to set a standard for unencrypted data.

³ Under the security breach notification law "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. Cal. Civ. Code 1798.29(g) and 1798.82(i).

⁴ Cal. Civ. Code 1798.29(a) and 1798.82(a).

⁵ If the vendor is considered a business associate under HIPAA, the vendor has the option to follow HITECH's breach notification requirements set out in Section 13402(f) of the Act. Cal. Civ. Code and 1798.82(e).

⁶ Cal. Civ. Code 1798.29(a) and 1798.82(a).

⁷ Cal Civ. Code 1798.29(b) and 1798.82(b).

⁸ If CalHEERS demonstrates that the cost of providing notice would exceed \$250,000, or the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information, the law provides for substitute notice. Cal. Civ. Code 1798.29(i) and 1798.82(j).

⁹ Further, under the circumstances where CalHEERS is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system, CalHEERS or any vendors will also have to electronically submit a single sample copy of that security breach notification,

1. The security breach notification must be written in plain language; and
2. The security breach notification must include, at a minimum, the following information:
 - The name and contact information of the agency, in this case CalHEERS;
 - A list of the types of personal information that were or are reasonably believed to have been the subject of the breach;
 - The date of the notice and, if the information is possible to determine at the time the notice is provided, then any of the following:
 - The date of the breach,
 - The estimated date of the breach, or
 - The date range within which the breach occurred;
 - Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;
 - A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
 - The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.

The statute also provides agencies discretion to include additional information in a notification. CDT and CU recommend that CalHEERS make these provisions mandatory for breaches of information held by CalHEERS and its vendors in order to build trust in the new online system. Therefore the security breach notification should also include information about what CalHEERS has done to protect individuals whose information has been breached and advice on steps that the person whose information has been breached may take to protect himself or herself.

The security breach notification laws permit delayed notification only when "a law enforcement agency determines that it would impede a criminal investigation."¹⁰ The laws also require any entity that licenses such information to notify the owner or licensee of the information of any breach in the security of the data.¹¹

Finally, CDT and CU, in line with the structure of the California security breach notification laws, believe that no notice needs to be given, either to individuals or authorities, if the data is properly encrypted because it will be inaccessible.

For more information contact:

Kate Black, Center for Democracy and Technology, kate@cdt.org (415) 882-1714

Julie Silas, Consumers Union, jsilas@consumer.org (415) 431-6747 ext. 106

excluding any personally identifiable information, to the state Attorney General. Cal. Civ. Code 1798.29(e) and 1798.82(f).

¹⁰ Cal. Civ. Code 1798.29(c) and 1798.82(c).

¹¹ Cal. Civ. Code 1798.29(b) and 1798.82(b).