INFORMATION SECURITY-BREACH NOTIFICATION

1. Purpose and Scope

The purpose of this Administrative Regulation is to determine the need for notification of a system data breach and outline the required formatting of a breach notice pursuant to California Civil law codes, sections civ:1798.29 and hsc:1280.15. California Civil Law only applies to California residents per section 1798.29 (a), however this administrative regulation may be used for non-California residents as well. For specific information regarding incident response for a suspected system data breach please refer to Admin Regulation ITS-AR-1506. Throughout this document "agency" refers to the Yosemite Community College District.

2. Timing of Breach Notifications

Per civ:1798.29: The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

subdivision (c): The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

Per hsc:1280.15 (b) (1): A clinic, health facility, home health agency, or hospice to which subdivision (a) applies shall report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information to the department no later than 15 business days after the unlawful or unauthorized access, use, or disclosure has been detected by the clinic, health facility, home health agency, or hospice.

(c) (1): A clinic, health facility, home health agency, or hospice shall delay the reporting, as required pursuant to paragraph (2) of subdivision (b), of any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information beyond 15 business days if a law enforcement agency or official provides the clinic, health facility, home health agency, or hospice with a written or oral statement that compliance with the reporting requirements of paragraph (2) of subdivision (b) would likely impede the law enforcement agency's investigation that relates to the unlawful or unauthorized access to, and use or disclosure of, a patient's medical information and specifies a date upon which the delay shall end, not to exceed 60 days after a written request is made, or 30 days after an oral request is made. A law enforcement agency or official may request an extension of a delay based upon a written declaration that there

exists a bona fide, ongoing, significant criminal investigation of serious wrongdoing relating to the unlawful or unauthorized access to, and use or disclosure of, a patient's medical information, that notification of patients will undermine the law enforcement agency's investigation, and that specifies a date upon which the delay shall end, not to exceed 60 days after the end of the original delay period.

(2) If the statement of the law enforcement agency or official is made orally, then the clinic, health facility, home health agency, or hospice shall do both of the following:

(A) Document the oral statement, including, but not limited to, the identity of the law enforcement agency or official making the oral statement and the date upon which the oral statement was made.

(B) Limit the delay in reporting the unlawful or unauthorized access to, or use or disclosure of, the patient's medical information to the date specified in the oral statement, not to exceed 30 calendar days from the date that the oral statement is made, unless a written statement that complies with the requirements of this subdivision is received during that time.

(3) A clinic, health facility, home health agency, or hospice shall submit a report that is delayed pursuant to this subdivision not later than 15 business days after the date designated as the end of the delay.

3. Determination of the need for Breach Notification

The need for breach notification is determined by utilizing the breach notification flowchart in appendix A. By following the flow chart all of the relevant questions per California civil code are asked for determination of the need for breach notification.

To use the flow chart, start from top to bottom, ask yourself each of the questions and follow the appropriate decision path.

4. Breach Notification Format

California civil code civ:1798.29 requires a specific formatting for breach notifications in order to comply with the law. The notification shall be written in plain English and shall be titled "Notice of Data Breach" then notice shall contain the following headings:

- "What Happened"
- "What Information Was involved"
- "What We Are Doing"
- "What You Can Do"
- "For More Information"

Additional information may be provided as a supplement to the notice.

5. Breach Notification Required Information

The breach notification shall include at a minimum the following information (civ:1798.29 (e))

- The name and contact information of the reporting agency (YCCD)
- A list of the types of personal information that were or are reasonably believed to have been the subject of the breach.
- If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.
- Whether the notice 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.
- 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.

At the discretion of the agency, the security breach notification may also include any of the following:

- Information about what the agency has done to protect individuals whose information has been breached.
- Advice on steps that the person whose information has been breached may take to protect himself or herself.

6. Notifying external agencies of a Security Breach

California State Attorney Generals Office

Any agency that 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 shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General.

California Department of Public Health

A clinic, health facility, home health agency, or hospice licensed pursuant to Section 1204, 1250, 1725, or 1745 shall report any unlawful or unauthorized access to, or use or disclosure of, a patient’s medical information to the department no later than 15

business days after the unlawful or unauthorized access, use, or disclosure has been detected by the clinic, health facility, home health agency, or hospice.

7. Determining if Personal Information was Involved

"Personal information" means either of the following: An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social security number
- Driver's license number or California identification card number
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
- Medical information
- Health insurance information
- Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5
- A user name or email address, in combination with a password or security question and answer that would permit access to an online account

If any of the preceding data elements in combination or in whole were part of a data breach and the data was accessed or potentially accessed in an unencrypted form for the purposes of this document personal information was involved.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

8. Delivery of Breach Notifications

Breach Notification may be provided by one of the following methods:

- Written notice
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code
- Substitute notice

8.1. Providing Breach Notification by Substitute Notice

If the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds ($500,000), or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

- Email notice when the agency has an email address for the subject persons
- Conspicuous posting, for a minimum of 30 days, of the notice on the agency's Internet Web site page, if the agency maintains one. Conspicuous posting on the agency's Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.
- Notification to major statewide media and the Office of Information Security within the CA Department of Technology
- In the case of a breach of the security of the system involving personal information for an online account, and no other personal information the agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the agency and all other online accounts for which the person uses the same user name or email address and password or security question or answer.
- In the case of a breach of the security of the system involving personal information for login credentials of an email account furnished by the agency, the agency shall not comply by providing the security breach notification to that email address, but may, instead, comply by providing notice by another method or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the agency knows the resident customarily accesses the account.

9. Definitions

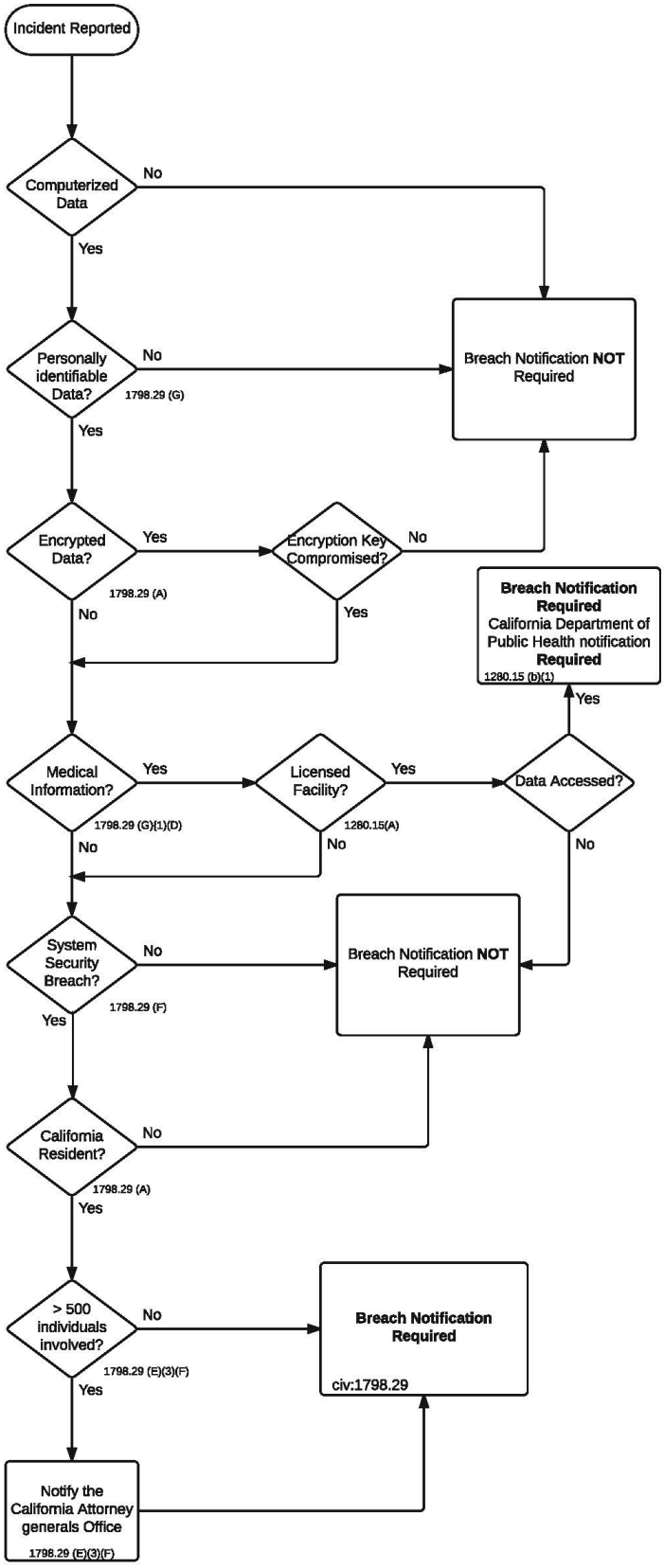
Breach of the security of the system
means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

Medical Information
means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

Health Insurance Information
means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

Encrypted
means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

Appendix A


Incident Reported
Computerized Data
No
Yes
Personally identifiable Data?
No
1798.29 (G)
Yes
Breach Notification NOT Required
Encrypted Data?
Yes
1798.29 (A)
No
Encryption Key Compromised?
No
Yes
Breach Notification Required
California Department of Public Health notification Required
1280.15 (b)(1)
Yes
Medical Information?
Yes
1798.29 (G)(1)(D)
No
Licensed Facility?
Yes
1280.15(A)
No
Data Accessed?
No
System Security Breach?
No
1798.29 (F)
Yes
Breach Notification NOT Required
California Resident?
No
1798.29 (A)
Yes
> 500 individuals involved?
No
1798.29 (E)(3)(F)
Yes
Breach Notification Required
civ:1798.29
Notify the California Attorney generals Office
1798.29 (E)(3)(F)