Policy Type: Administrative

Category: Administrative Practices

Policy Name: Notification of Security Breach of Personal Information

Policy Owner: County Executive

Policy Purpose

The purpose of this policy is to ensure that departments comply with the provisions of state law requiring government agencies to notify individuals whose personal identifying information has been compromised due to a security breach of computerized data.

Policy Summary

Section 1798.29 of the California Civil Code requires the County to notify individuals when their personal information has been compromised due to a security breach. Because each department collects different types of personal information on County residents and customers, each individual department shall be responsible for developing its own processes and procedures in compliance with this policy and its related procedures. Each department shall also be responsible for identifying any security breach affecting the personal information that the department maintains, uses, transfers, owns, or leases.

The personal information covered by this policy is either or both of the following:

1) An individual's first and last names, or an individual's first initial and last name, in combination with any one or more of the following, where either the name or the information is not encrypted:

   1a) Social security number;

1b) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;

1c) 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;

   1d) Medical information *(see definitions section below);*

1e) Health insurance information *(see definitions section below);*

1f) Biometric information (see *definitions section below*);

1g) Information or data collected through the use or operation of an automated license plate recognition system (*see definitions section below*); and/or

2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

   This policy also covers certain breaches of personal information that is encrypted, as discussed below.

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

When Notice of Data Breach is Required

A "security breach" is defined by state law as "the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information." A security breach can affect any number of individuals; even situations where only a single individual's personal information has been compromised can constitute a security breach. Examples of breaches include, but are not limited to:

- Sending an individual's personal information to the wrong person through an incorrect email address;
- An employee acquiring the personal information of an individual for any purpose other than for legitimate County business;
- Losing a laptop computer, mobile device, flash drive, or other device that contains personal information; or
- A malicious actor from outside the organization acquiring personal information from a County database.

When the County owns or licenses computerized data that includes personal information, the County must provide notification to individuals whose personal information has been or is reasonably believed to have been acquired by an unauthorized person. When the personal information is encrypted, the County must provide notification to individuals when both the encrypted personal information and the encryption key or security credential have been or are reasonably believed to have been acquired by

an unauthorized person, if the County has a reasonable belief that the encryption key or security credential could render the encrypted personal information readable or useable.

The notification must be provided without unreasonable delay following the discovery of the security breach. The department may delay sending notification at the direction of law enforcement, as described below.

When the County maintains computerized data that includes personal information owned by another entity, such as another public agency or a non-profit organization, the County must provide notification to the owner or licensee of the information when the personal information has been or is reasonably believed to have been acquired by an unauthorized person. This notification must be provided immediately following the discovery of the breach.

When a County employee or contractor knows or suspects a breach has occurred, they must immediately contact an executive in their department as well as County Counsel, Information Security Office, and the Privacy Office. In the event of a security breach affecting personal information of a Santa Clara Valley Heath and Hospital (SCVHHS) patient/client/member, the breach must be reported immediately to the SCVHHS Ethics, Compliance & Privacy Office. Reporting and notification of security and privacy breaches of SCVHHS patient/client/member information will be governed by applicable SCVHHS department policies in conjunction with this policy.

Delayed Notice of Data Breach to Affected Parties for Law Enforcement Investigations

For any breach that is being investigated by law enforcement, the department must work with County Counsel to determine whether notification to affected parties should be delayed in light of the ongoing

investigation. If a law enforcement agency determines that immediate notification of a security breach to the affected parties would impede a criminal investigation, the County may delay notification. The County must provide notification to affected individuals upon law enforcement determining that doing so will no longer compromise the investigation.

Using the Notice of Data Breach Template

The law requires that the Notice of Data Breach sent to those affected by the breach have specified headings and information. Departments must comply with the requirements of the law and this policy by either using the attached Notice of Data Breach template, or using a comparable letter approved by the Office of the County Counsel. A comparable letter may be necessary to comply with other breach reporting laws. The department must print the letter on its own letterhead and fill in or otherwise edit the highlighted sections of the form as applicable, leaving all headings as listed. All breach notices must be reviewed by County Counsel and the Chief Privacy Officer or designee prior to distribution.

Notice of Data Breach Requirements

The department may provide notification to affected individuals or to the owner of non-County-owned information in any one or more of the following ways:

1) Written notice;

2) Electronic notice, if County Counsel has determined that the notice is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code; and/or

3) Substitute notice, if approved by County Counsel and if the County can demonstrate that the cost of providing notice would exceed $250,000, or that that the affected class of subject persons to be notified exceeds 500,000, or the County does not have sufficient contact information. Substitute notice shall consist of all of the following:

3a) Email notice when the department or agency has an email address for the subject persons;

3b) Conspicuous posting, for a minimum of 30 days, of the notice on the County's website, with a link to the notice from the home page; and

3c) Notification to major statewide media and the Office of Information Security within the California Department of Technology.

As set forth in the Notice of Data Breach Template, each of the above-mentioned forms of notice must be written in plain language, titled "Notice of Data Breach", include the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information," and must include, at a minimum, the following information:

1) The name and contact information of the County department or agency;

2) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

3) The date that the notification is being provided;

4) Any of the following, if available at the time of providing the notification:

4a) The date of the breach;

4b) The estimated date of the breach; and/or

4c) A date range within which the breach occurred.

5) An indication of whether the notification was delayed due to a law enforcement investigation, if available at the time of providing the notification;

6) A general description of the breach incident, if available at the time of providing the notification; and

7) The toll-free numbers and addresses of the major credit reporting agencies, if the breach involved a social security number, or a driver's license number, or a California identification card number.

When any department or agency sends a notification to more than 500 California residents, County Counsel will also electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the California Attorney General.

Optional Information that Departments May Include in a Notice of Data Breach

In addition to the above-mentioned requirements, the department or agency may also include any of the following information at the department's or agency's discretion:

1) Information about what the department or agency has done to protect individuals whose information has been breached; and/or

2) Advice on steps that the person whose information has been breached may take to protect himself or herself.

Additionally, the department may also provide notification under this policy in multiple languages as the department determines is necessary or as required by state or federal law on the advice of County Counsel.

Special Actions for Breaches Involving Only User Names and Passwords

If a security breach involves only login information for an account – usually consisting of a user name or email address and a password or security question answer – then the department may comply with the notification portions of this policy by providing the security breach notification in electronic or other form that directs the affected individuals to change their password and/or security question answer, or take other appropriate steps to prevent unauthorized access to their account. The department should also inform the affected individuals to change the passwords and/or security question answers for other accounts that use the same or similar login information.

If a security breach involves only login information for an email account that was provided by the department rather than created by the user, the department may either provide full notification using the attached Notice of Data Breach Template or similar letter, or the department can comply with the notification portions of this policy through a clear and conspicuous notice displayed to the person whose information was breached when that person connects to his or her account online. The department may not, however, email the Notice of Data Breach to the compromised email address.

Internal Notification to Specified County Officials

In addition to the procedures identified above, whenever a single incident potentially breaches the personal information of 10 or more individuals, possibly involves criminal conduct, or, at the determination of County Counsel, otherwise poses a significant risk to the County, the department must work with the Office of the County Counsel to prepare and provide an Incident Notification of the breach to the County Counsel pursuant to the Notification of Major or Sensitive Incidents (Incident Notification) Policy. The County Counsel will then ensure the County officials as listed in the procedures below are notified via an attorney-client privileged communication and with the Office of the County Executive determine whether notification of additional County Officials is required. The Incident Notification to County Counsel must include, at minimum, a brief description of the incident or event that resulted in the possible breach of personal information and the actions taken by the department to resolve the situation.

Procedures

Notification of Security Breach

1) Upon suspicion that a security breach has occurred, the **department** immediately informs the Office of the County Counsel, the Information Security Office (via o365-iso-team@sccconnect.onmicrosoft.com), and the Privacy Office (via PrivacyOffice@ceo.sccgov.org) of the breach, and works with those offices to determine the scope of the breach, and if necessary, implement emergency security practices to contain the breach and/or avoid the compromise of any additional information. All written communications regarding a potential breach (e.g. emails) must include the Office of the County Counsel.

1a) If the breach affects personal information of a SCVHHS patient/client/member, the **department** should instead immediately notify the SCVHHS Ethics, Compliance & Privacy Office of the breach in conformity with SCVHHS department policies. Reporting and notification of breaches will be governed by applicable SCVHHS department policies in conjunction with this policy.

1b) Reporting and notification of breaches will be governed by applicable SCVHHS department policies in conjunction with this policy.

2) The **department** works with the Chief Information Security Officer or designee, the Chief Privacy Officer or designee, and the Office of the County Counsel to determine the following:

2a) How many individuals were affected;

2b) The names and contact information for the individuals whose information was compromised;

2c) Whether the breach involved a criminal act;

2d) Whether notification should be delayed due to an ongoing law enforcement investigation;

2e) The types of information that were possibly breached; and

2f) If the breach poses a significant risk to the County.

3) If the security breach potentially affected the personal information of 10 or more individuals, or if the breach involved a potentially criminal act, or if, at the determination of the County Counsel, the breach otherwise poses a significant risk to the County, the **department** must work with its

representative in the Office of the County Counsel to prepare and send only to County Counsel (via an email to incident@cco.sccgov.org) an internal notification of the breach in a timely manner, in compliance with the Notification of Major or Sensitive Incidents (Incident Notification) Policy.

3a) At minimum, the **department** must include in the Incident Notification a brief description of the incident or event that resulted in the possible breach of personal information and the actions taken by the County to resolve the situation.

3b) **County Counsel** must provide the internal notification of the breach to the County Executive, the Chief Operating Officer, the pertinent Deputy County Executive, the Chief Information Security Officer or designee, the Chief Privacy Officer or designee, the Director of Risk Management, and the Chief Information Officer via an attorney-client privileged communication..

3c) The **Office of the County Counsel and the Office of the County Executive** will determine whether notification to additional County Officials is required.

4) If the security breach only affected login information, the **department** consults with County Counsel to determine the best method for providing notification to the individuals affected as follows:

4a) If the security breach only affected login credentials for an email account provided by the department, the **department** may comply with this policy by providing a clear and conspicuous notice the next time the affected individuals log in to their accounts from an Internet Protocol address or online location from which the department knows the individual customarily accesses the account. The department shall not send the notice to the email account.

4b) If the security breach only affected login information created by the user, the **department** may comply with this policy by providing the Notice of Data Breach in electronic or other form directing the affected individuals to change their password and/or security question and answer.

5) If the security breach affected any other type of personal information, the **department** consults with County Counsel to determine the appropriate method as follows:

   5a) Written notice;

   5b) Electronic notice; or

   5c) Substitute notice.

6) The **department** submits a draft Notice of Data Breach to the Office of the County Counsel for approval.

7) Upon receiving approval from the Office of the County Counsel, the **department** provides notification to all affected individuals using the Notice of Data Breach form.

8) If the security breach affected more than 500 California residents, **County Counsel** provides an electronic copy of the notification to the California Attorney General, excluding any personal information.

9) Following any security breach, the **department** shall consult with the Information Security Office and the Office of the County Counsel as appropriate to implement additional security features in order to avoid future security breaches.

Definitions

1) "**Automated License Plate Recognition System**" means a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data.

2) "**Biometric Information**" means unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Biometric information does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

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

4) "**Encryption key**" and "**security credential**" mean the confidential key or process designed to render the data useable, readable, and decipherable.

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

6) "**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.

7) "**Personal Information**" means either or both of the following:

7a) An individual's first and last names, or an individual's first initial and last name, in combination with any one or more of the following, where either the name or the information is not encrypted:

- Social security number;
- Driver's license number or California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;
- 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; or
- Information or data collected through the use or operation of an automated license plate recognition system.

7b) A user name or email address, in combination with a password or security question and answer that would permit access to an online account

"Personal information" covered under this policy does not include publicly available information that is lawfully made available to the general public

from federal, state, or local government records. This policy also covers personal information that is encrypted if there has been a security breach.

8) "**Security Breach**" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the County. This definition shall include any incident or situation where an unauthorized individual has obtained or is reasonably believed to have obtained an individual's personal information, including through accidental disclosure or theft. This definition also includes any incident or situation where an unauthorized person has obtained or is reasonably believed to have obtained both encrypted personal information and the encryption key or security credential if the County has a reasonable belief that the encryption key or security credential could render the encrypted personal information readable or useable.

Frequently Asked Questions

1) **I accidentally sent someone's personal information to the wrong email address. Can I just re-send it to the correct email address without providing notification?**

No. This type of accidental disclosure may constitute a security breach and may require your department to provide notification under this policy to the individual whose personal information was disclosed. Your department may need to provide the individual with the Notice of Data Breach or other similar letter that conforms to this policy and your department's practices, regardless of whether you re-send the information to the correct email address.

2) **Some information maintained by my department was acquired by an unauthorized individual, but I am not sure whether the information is covered by this policy. Do I have to send notifications to the affected individuals?**

Possibly. All departments must consult with the Information Security Office, Privacy Office, and County Counsel as soon as possible after discovering a possible breach to determine the appropriate steps. Since this policy and state law require departments to send notifications promptly if they are required, you must contact County Counsel as soon as possible in order to ensure that your department does not unnecessarily delay notification if County Counsel determines that notification is required.

3) **Some personal information maintained by my department in an encrypted format was acquired by an unauthorized individual, but I am not sure whether the encryption key or security credential was also compromised. Do I have to send notifications to the affected individuals?**

Possibly. All departments must consult with the Information Security Office, Privacy Office, and County Counsel as soon as possible after discovering a possible breach to determine the appropriate steps. A determination of whether notification is required depending on the circumstances of the particular instance will be made in consultation with the Chief Information Security Officer or designee, Chief Privacy Officer or designee, and County Counsel, which will include an analysis of the security of the information, including any encryption.

4) **The personal information that my department collects is also covered by other notification laws, such as the Health Insurance Portability and Accountability Act (HIPAA). Do I still have to comply with this policy?**

Yes. State law requires all counties – including all of their departments or agencies – to provide the notification described in this policy. Your department must comply with all applicable laws, including all applicable notification laws. However, if the breach affects the personal information of a SCVHHS patient/client/member, the SCVHHS Ethics, Compliance & Privacy Office will ensure proper notification is provided to individuals, in accordance with SCVHHS department policy, HIPAA, and any other applicable laws, in consultation with the Office of the County Counsel. Contact County Counsel if your department has questions regarding complying with multiple notification laws.

Related Policies

- Board Policy 3.25 – Policy Relating to Confidentiality of Documents - https://saecommon.sccgov.org/countypolicy/Board-Policy-3.25-Policy-Relating-to-Confidentiality-of-Documents.pdf

- Board Policy 3.40 – General Policy Relating to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) - https://saecommon.sccgov.org/countypolicy/Board-Policy-3.40-General-Policy-Relating-to-HIPAA.pdf

- Notification of Major or Sensitive Incidents (Incident Notification) https://saecommon.sccgov.org/countypolicy/Incident-Notification.pdf

- Information Security Policies - https://saecommon.sccgov.org/countypolicy/Information-Technology-Security-Policies.pdf

- Legal Services Policy - https://saecommon.sccgov.org/countypolicy/Legal-Services-Policy.pdf

- SCVHHS Department Policies - [url]/Pages/policies-home.pdf

Related Forms and Information

- Notice of Data Breach Template - [url]/sites/policies/FormsrelatedtoPolicies/Notice-of-Data-Breach-Template.docx

History

Date	Changes Made
1/12/2021	Policy Updated.
5/2/2016	Policy Uploaded. (Kyle Larson)
5/2/2016	Policy Adopted.