California Dental Association
1201 K Street, Sacramento, CA 95814
800.232.7645 cda.org

Data Breach Notification Requirements

There are both state and federal laws for notification of patients, the public and government agencies when patient information is lost, stolen or used or disclosed without authorization. There are differences in the laws. All California health care providers must comply with state law but not all health care providers are HIPAA covered entities who must also comply with the HIPAA Breach Notification Rule.

Under state law, businesses and government agencies are required to notify individuals whose unencrypted, electronically stored personal information is breached. (Federal law applies to all hard copy as well as electronic forms of protected health information.) California businesses have been required since 2003 to provide data breach notifications. The law changed in 2008 with the passage of AB 1298, when medical and health insurance information was added to the list of specified personal information that, if reasonably believed to have been acquired by an unauthorized person, trigger a mandatory notification. SB 24, signed in August 2011, also enhanced the law, requiring that a notification letter contain specific information about the breach including a description of what happened, the type of information breached, and advice on how affected individuals can protect themselves from identity theft. It also requires, in the event 500 or more California residents are affected, sending a copy of the letter to the state Attorney General's office. This law became effective Jan. 1, 2012. Starting Jan. 1, 2014, the definition of "personal information" expanded to include information that could be used to access a consumer's online accounts. An amendment to the law effective Jan. 1, 2015, required that if a company is responsible for a data breach and decides to offer credit monitoring services to affected individuals, the company must provide the services at their own expense and for no less than 12 months. The amendment does not require companies to offer credit monitoring. It simply states that if a company decides to offer it, the company must provide the service free of charge and for one year. Another amendment became effective Jan. 1, 2016 that defined "encrypted" as "rendered unusable, unreadable or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security. This amendment also required that certain headers are used in breach notification letters (described in detail in the checklist below). The latest amendment, effective Jan. 1, 2017, clarifies that along with unencrypted information, encrypted information that is breached along with its decryption key also triggers breach notification. In other words, if the decryption key is compromised along with the encrypted information, the information is considered unencrypted and affected individuals must be notified.

State law requires notification related to types of unencrypted, computerized "personal information" including a person's first name or first initial and last name in combination with any of the following:

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

If any of the above-referenced computerized personal information is breached, you are required to notify any California resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Notification (Sample Breach Notification Notice) should be provided immediately following discovery of the breach and can be provided by written or electronic notice. In the case of a breach of a username or email address in combination with a password or security question answer, electronic notification shall not be sent to an email address that was subject to the breach, but rather an alternative method of notification prescribed by law.

The federal Health Insurance Portability and Accountability Act (HIPAA) was amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) and a Breach Notification Rule was added. As of Sept. 23, 2009, HIPAA covered entities must notify patients any time their unsecured personal health information (PHI) may have been compromised through unauthorized acquisition, access, use or disclosure. HIPAA/HITECH's security breach notification requirements also require that a business associate notify a covered entity of a breach of any unsecured PHI that it holds on the covered entity's behalf.

It is important to remember that HIPAA/HITECH does not change the fact that state laws such as California's, which are more protective of patient information, are not pre-empted by HIPAA. Covered entities must comply with all applicable state and federal privacy laws and follow the more stringent requirement. SB 24, effective Jan. 1, 2012, specifies that a covered entity under HIPAA will be deemed to have complied with California's notice requirements if it has complied completely with the breach notification requirements of the HITECH Act. It is not necessary to send separate notices under both state and federal law.

HIPAA Breach Assessment

Any impermissible use or disclosure of unsecured patient information, whether on paper, film or electronic format, is presumed to be a breach requiring notification. Notification is not required if the covered entity determines that the incident is one of the following:

1. The unintentional acquisition, access, use or disclosure of PHI by a staff member or a business associate acting in good faith and with the scope of his or her job responsibility, as long as the breach does not result in further impermissible use or disclosure.
2. The inadvertent disclosure of PHI to another person who is authorized to access PHI at the same business.
3. The covered entity determines that the unauthorized individual who received the PHI is unable to retain it.
4. Low probability that the PHI in question was compromised.

Notification also is not required if the covered entity or business associate can demonstrate low probability that patient information has been compromised based on a risk assessment of at least:

1. Nature and extent of patient information involved.
2. Who received/accessed the information.
3. Potential that patient information was actually acquired or viewed.
4. Extent to which risk to the data has been mitigated.

Following are examples of impermissible uses or disclosures for which a dental practice may choose to do a documented risk assessment (a sample breach assessment form is available in the ADA HIPAA Compliance Kit and online–see link below):

- A fax with patient information is sent from Practice A to Practice B, but the fax was not intended for Practice B.
- A practice forwards a copy of a patient's financial agreement to its collection agency and inadvertently includes the treatment plan.
- A patient receives mail from the practice that contains another patient's information.

A covered entity or business associate must document its rationale if it determines breach notification is not necessary. If a dental practice decides to proceed with notifying affected individuals of a breach, a breach risk assessment is not required.

Breach Notification Requirements

The notification requirements are detailed in the accompanying checklist. In summary:

- A dental practice that is not a HIPAA covered entity must notify individuals if a breach of unencrypted electronic personal information occurs. The non-HIPAA CE also must notify law enforcement if illegal activity occurred and, if the number of affected individuals is 500 or more, the state Attorney General's office. The practice must provide notification without unreasonable delay.
- A dental practice that is a HIPAA covered entity must notify individuals of a breach of information in any format. The practice must notify law enforcement if illegal activity occurred. If a breach affects 500 or more individuals, the dental practice also must notify the U.S. Department of Health and Human Services (HHS) and prominent media outlets. Notification must occur no later than 60 days after discovery of the breach. For smaller breaches, a covered entity must keep a log or other documentation of all such breaches that involve 499 or fewer individuals. A sample breach log is available in the ADA HIPAA Compliance Kit and online (see link below). The log must be submitted annually to HHS no later than 60 days after the end of each calendar year.

Breach Notification Policy and Procedures

HITECH requires a covered entity to have written Breach Notification Policy and Procedures. The American Dental Association has a sample breach notification policy and procedures document in the ADA HIPAA Compliance Kit and online (see link below). Also, the California Office of Information Security and Privacy Protection offers "Recommended Practices on Notice of Security Breach Involving Personal Information" on its website (see link below). "A California Business Privacy Handbook" also is available on the site. The handbook provides information on breach prevention. You may want to consider adding items from the California publications to your breach notification policy and procedures. A California dental practice that is a covered entity should have written policy and procedures that addresses both HIPAA and California law. The checklist below may be incorporated in the practice's written procedures.

Other Considerations

Check with your business property insurance carrier on the availability of a data breach policy. You may also want to consider offering to pay for credit monitoring if your patient's information is breached.

Resources

- California Office of Information Security and Privacy Protection
  Recommended Practices on Notice of Security Breach Involving Personal Information
- American Dental Association
  HIPAA/HITECH Breach Notification Rule
- U.S. Department of Health and Human Services, Breach Notification Rule

Checklist: State and Federal Breach Notification Requirements

	State	Federal HITECH
Who Must Comply	California business and state and local government agencies.	"Covered entities" as defined by HIPAA. The covered entity is responsible for providing notification even if the breach was discovered or caused by an independent contractor or business associate.
Type of Information Covered by Law	Unencrypted, computerized information, or encrypted information along with the decryption key, that has a person's first name or first initial and last name in combination with any of the following: • Social Security number • Driver's license number of California identification card number • Account number, credit/debit card number, in combination with any required security code, access code, or password that would allow access to the person's financial account • Medical information, defined as "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, defined as "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" • A username or email address in combination with a password or security question and answer that would permit access to an online account • Information or data collected through the use or operation of an automated license plate recognition system	Person's name in combination with personal health information (PHI) that is not encrypted or not secured. PHI on paper, film, or other non-computer medium is considered unsecured.

	State	Federal HITECH
Risk Assessment	Not required	Upon discovery or notice of a possible breach, the covered entity may provide immediate notification to affected individual(s) OR conduct a risk assessment to determine if there is a low probability that patient information was compromised. The risk assessment must be documented. A sample risk assessment worksheet is available from the ADA. The risk assessment must analyze the following factors: • The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification. • The unauthorized person who used the protected health information or to whom the disclosure was made. • Whether the protected health information was actually acquired or viewed. • The extent to which the risk to the protected health information has been mitigated. A sample breach notification risk assessment worksheet is available to ADA members on ada.org.
Trigger Requiring Notification	Discovery or notification of a breach in the security of the data, or a reasonable belief that an unauthorized person has acquired the data.	Upon discovery or notification of a breach or impermissible use or disclosure or after a documented breach risk assessment determines that the patient information was compromised.

	State	Federal HITECH
Exceptions to Notification Requirement	None	The unintentional acquisition, access, use, or disclosure of PHI by a staff member or a business associate acting in good faith and with the scope of his or her job responsibility, as long as the breach does not result in further impermissible use or disclosure. The inadvertent disclosure of PHI to another person who is authorized to access PHI at the same business. The covered entity determines that the unauthorized individual who received the PHI is unable to retain it. Low probability that the PHI in question was compromised following risk assessment.
Who Must Be Notified	Report theft of data storage unit/device to local law enforcement. Also report to local law enforcement other unauthorized access to personal information that you believe resulted from illegal activity.	
	California residents whose electronic information was accessed in the breach. If 500 or more individuals are affected, a copy of the letter must be sent to the state Attorney General's office, oag.ca.gov/ecrime/databreach/reporting. Certain licensed health facilities are required to report breaches to the California Department of Public Health (Health and Safety Code 1280.1, 1280.3 and 1280.15). Private dental practices are not included in the definition of licensed health facilities.	Affected individuals. If affected individuals are deceased, next of kin must be notified. U.S. Department of Health and Human Services via submittal of an annual log.* If breach involves PHI of more than 500 individuals, the department should be notified without unreasonable delay and in no case longer than 60 days. Prominent media outlets if the breach involves 500 or more residents of a state or jurisdiction.
Notification Time	Must be done "in the most expedient time possible and without unreasonable delay." Time may be allowed for legitimate law enforcement needs or for taking necessary measure to determine the scope of the breach and restore reasonable integrity to the system.	Must be sent no later than 60 calendar days after discovery of the breach "without unreasonable delay."

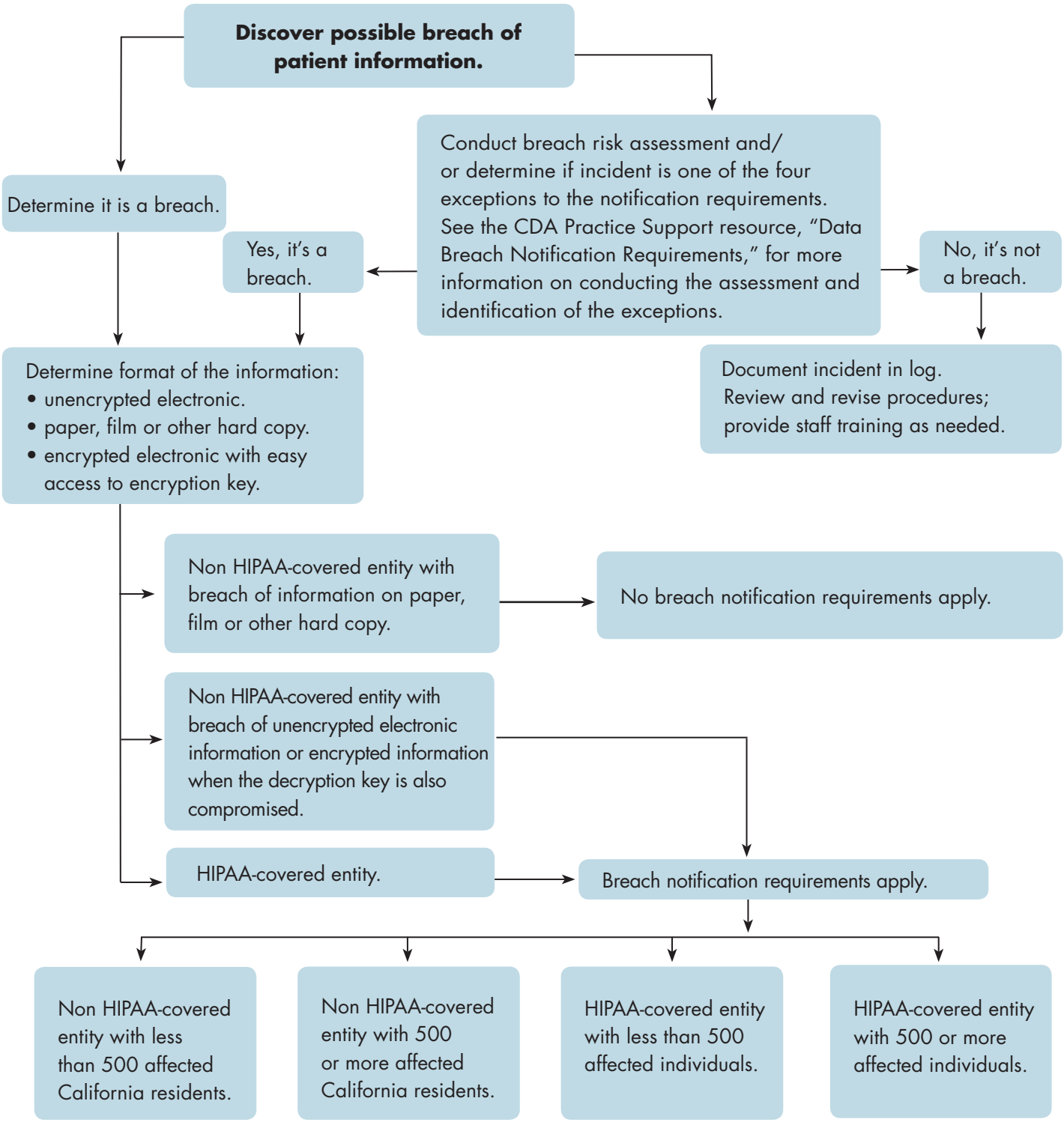
	State	Federal HITECH
Notice Contents	A *Sample Breach Notification Notice* is available on cda.org/practicesupport. The sample letter meets both state and federal requirements.	
	Notifications should be titled "Notice of a Data Breach "and can be in no smaller than 10-point font. Notifications should contain the following information under headers that state: • What Happened? • What Information Was Involved? • What Are We Doing? • What You Can Do? and • For More Information o General description of what happened, including, if available, the date of the breach, the estimated date of the breach, or the date range within which the breach occurred. The notification should also include the date of the notice. o The specific type of personal information that was involved. — In breaches of financial related information, specify whether Social Security number, driver's license or California ID number, or financial account number was involved. — In breaches of medical or health insurance information, be as specific as possible about the nature of the information involved. Specify that Social Security numbers, driver's license or California ID numbers and financial account numbers were not involved, when that is the case.	Notifications must contain the following information: • Description of what happened • Description of information involved • Steps the individual should take to protect themselves from potential harm resulting from the breach • Description of investigation and mitigation steps • Contact information

	State	Federal HITECH
Notice Contents *(continued...)*	o What you have done to protect the individual's personal information from further unauthorized acquisition. o What your organization will do to assist individuals, including providing your toll-free contact telephone and assistance. o Information on what individuals can do to protect themselves from identity theft, as appropriate for the specific type of personal information involved. o Contact information for the website of the state Attorney General's Office (oag.ca.gov/privacy) for additional information for California residents on protection against identity theft. o If an offer for credit monitoring is extended to affected individuals, the offer must be free of charge to the affected individuals and for a duration of no less than 12 months.	
Method of Notification	The written notice must be sent via first-class mail or by email, as long as the individual has consented to receive communications via email. Substitute notice can be used if certain criteria are met.	
	In the case of a breach of a username or email address in combination with a password or security question answer, electronic notification shall not be sent to an email address that was subject to the breach, but rather an alternative method of notification prescribed by law.	Telephone notice may be given in addition to written notice.

	State	Federal HITECH
Substitute Notice	Substitute notice is allowed under state law if the cost of providing individual notice is more than $250,000, more than 500,000 people would have to be notified, or the organization does not have sufficient contact information for those affected. A substitute notice is comprised of (1) email when email address is available AND (2) conspicuous posting on company website AND (3) notification of major statewide media and the state Attorney General's Office (oag.ca.gov/privacy).	If fewer than 10 individuals are affected by the breach and insufficient contact information for them is available, providing substitute notice by telephone is acceptable. Provide limited information (for example, only call-back information) when leaving a message on an answering machine or with the affected individual's family member or roommate. If there is insufficient contact information for 10 or more individuals affected by the breach, substitute notice can be provided in one of two ways: post a conspicuous notice or hyperlink to the notice for a 90-day period on the home page of the covered entity's website or place a conspicuous posting in major print or broadcast media in geographical areas where the individual affected by the breach likely resides. The substitute notice must include a toll-free telephone number that is active for a 90-day period. The return of 10 or more mailed notices to the covered entity indicates insufficient contact information and substitute notice must be provided.

	State	Federal HITECH
Recordkeeping	Recommended, not required	A covered entity must keep a log or other documentation of all breaches of PHI that occur on or after Sept. 23, 2009. Submit the information annually to the U.S. Department of Health and Human Services* not later than 60 days after the end of each calendar year as specified by the agency. Documentation such as risk assessments, copies of notices and a breach notification log must be kept for six years.

* hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html


Discover possible breach of patient information.
Conduct breach risk assessment and/ or determine if incident is one of the four exceptions to the notification requirements. See the CDA Practice Support resource, "Data Breach Notification Requirements," for more information on conducting the assessment and identification of the exceptions.
Determine it is a breach.
Yes, it's a breach.
No, it's not a breach.
Document incident in log. Review and revise procedures; provide staff training as needed.
Determine format of the information:
• unencrypted electronic.
• paper, film or other hard copy.
• encrypted electronic with easy access to encryption key.
Non HIPAA-covered entity with breach of information on paper, film or other hard copy.
No breach notification requirements apply.
Non HIPAA-covered entity with breach of unencrypted electronic information or encrypted information when the decryption key is also compromised.
HIPAA-covered entity.
Breach notification requirements apply.
Non HIPAA-covered entity with less than 500 affected California residents.
Non HIPAA-covered entity with 500 or more affected California residents.
HIPAA-covered entity with less than 500 affected individuals.
HIPAA-covered entity with 500 or more affected individuals.

TABLE

Breach Notification Requirements Apply

Non HIPAA-CE >500 CA residents	Non HIPAA-CE <500 CA residents	HIPAA-CE <500 individuals	HIPAA-CE >500 CA individuals
Notify law enforcement of suspected illegal activity, such as theft of computers, boxes of charts, etc., as soon as possible.			
Notify affected residents "in the most expedient time possible and without unreasonable delay." The written notice must have specific content and be sent via first-class mail or by email, as long as the individual has consented to receive communications via email.		Notify affected individuals, or next of kin if individual is deceased, within 60 calendar days after discovery of the breach and without unreasonable delay. The written notice must have specific content and be sent via first-class mail or by email, as long as the individual has consented to receive communications via email. Substitute notice (website or print or broadcast posting) with toll-free telephone number active for 90 days must be used if contact information for 10 or more individuals is insufficient.	
Substitute notice is allowed under state law if the cost of providing individual notice is more than $250,000, more than 500,000 people would have to be notified or the organization does not have sufficient contact information for those affected.		Substitute notice allowed if less than 10 individuals are affected.	
Upon notifying affected residents, upload a copy of the notification to the state attorney general's website.[i]		No later than 60 days after the end of the year in which the breach or breaches occurred, file a breach report or breach log on the Office for Civil Rights website.[ii]	Within 60 calendar days after discovery of the breach, file a report on the Office for Civil Rights website.[iii]
			Within 60 calendar days after discovery of the breach, notify prominent media outlets of the breach.

i. oag.ca.gov/ecrime/databreach/report-a-breach
ii. ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true
iii. ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true