APPENDIX PR 12-A

Federal and State Breach Notification Laws for California

	BREACH OF COMPUTERIZED DATA	***BREACH IN A LICENSED HEALTH FACILITY***	***HIPAA BREACH REQUIREMENT***
LEGAL CITATION	California Civil Code Section 1798.82	California Health and Safety (H&S) Code Section 1280.15	42 U.S.C. Section 17932; 45 C.F.R. Section 164.400 *et seq.*
EFFECTIVE DATE	Jan. 1, 2003	Breaches that occur on or after Jan. 1, 2009.	Breaches that occur on or after Sept. 23, 2009.
WHO MUST COMPLY	Any person or business that conducts business in California.	Health facilities licensed by the California Department of Public Health (CDPH) under H&S 1250 (hospitals, skilled nursing facilities, psychiatric health facilities, etc.), clinics licensed under H&S 1204, home health agencies licensed under H&S 1725, and hospices licensed under H&S 1745.	Covered entities (includes hospitals, physicians, clinics, other health care professionals) that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use or disclose **"unsecured"** protected health information (PHI), their business associates and subcontractors of the business associates. **"Unsecured"** PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the U.S. Department of Health and Human Services (DHHS) in guidance. The guidance can be found at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

	BREACH OF COMPUTERIZED DATA	***BREACH IN A LICENSED HEALTH FACILITY***	***HIPAA BREACH REQUIREMENT***
INFORMATION COVERED	Data containing: 1. An individual's first name or first initial and last name in combination with one or more of the following if either the name or data element is not encrypted: ▪ Social Security number; ▪ Driver's license number or California identification card number; ▪ Tax identification number; ▪ Passport number; ▪ Military identification number; ▪ 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 (defined in the column to the right); or ▪ Health insurance information: policy or subscriber number, or any information in an individual's application and claims history, including any appeals records. ▪ 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. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes;	A patient's **"medical information"** — any individually-identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. A court decision has interpreted the definition of "medical information" to exclude demographic information, such as the patient's name, medical record number, age, date of birth, and the last four digits of his or her Social Security number. (However, if the provider is not a general hospital, but a provider connected to a certain disease or condition (such as a psychiatrist, oncologist, AIDS clinic, etc.) where revealing the fact that a patient is connected to that provider also reveals something about the patient's medical condition, then disclosure of a patient's name alone could possibly constitute the disclosure of "medical information.") **"Individually-identifiable"** means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, e-mail address, telephone number, or Social Security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.	PHI — individually-identifiable health information that is transmitted or maintained in electronic media or any other form or media. Individually-identifiable health information is health information (including demographic information) that identifies or can be used to identify the individual. **"Health information"** includes any information, oral or recorded in any form or medium, relating to the physical or mental health or condition of an individual, the health care provided, or payment for health care provided.

	BREACH OF COMPUTERIZED DATA	***BREACH IN A LICENSED HEALTH FACILITY***	***HIPAA BREACH REQUIREMENT***
INFORMATION COVERED (CONT.)	▪ Information collected by an automated license plate recognition system. ▪ Genetic data. **"Genetic data"** means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom. 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.		

	BREACH OF COMPUTERIZED DATA	***BREACH IN A LICENSED HEALTH FACILITY***	***HIPAA BREACH REQUIREMENT***
BREACH DEFINITION	An unauthorized acquisition by an unauthorized person of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.	An unlawful or unauthorized access to, or use or disclosure of, a specific patient's medical information. **"Unauthorized"** means the inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment or other lawful use under any state or federal law. A breach "reasonably believed to have occurred" must also be reported.	The acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of the PHI. Notification obligations apply if the incident involves "unsecured" PHI, which is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the U.S. Department of Health and Human Services (DHHS) in guidance. The guidance can be found at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

	BREACH OF COMPUTERIZED DATA	***BREACH IN A LICENSED HEALTH FACILITY***	***HIPAA BREACH REQUIREMENT***
EXCEPTIONS	Good faith acquisition of personal information by an employee or agent for business purposes is not a breach if no further unauthorized use/disclosure.	1. A paper record, electronic mail, or facsimile transmission inadvertently accessed, used, or disclosed within the same health care facility or health care system where the information is not further accessed, used, or disclosed unless permitted or required by law. 2. An internal paper record, electronic mail or facsimile transmission outside the same health care facility or health care system sent to a HIPAA covered entity that has been inadvertently misdirected within the course of coordinating care or delivering services. 3. A disclosure of medical information in which a health care facility or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such medical information. 4. Any access to, use, or disclosure of medical information permitted or required by state or federal law. 5. Lost or stolen encrypted electronic data containing a patient's medical information that is in any way created, kept, or maintained by a health care facility where the encrypted electronic data has not been accessed, used, or disclosed in an unlawful or unauthorized manner. Lost or stolen electronic data containing a patient's medical information that is in any way created, kept, or maintained by a health care facility that is not encrypted is presumed to be a breach unless it is excluded after completing a four-factor risk assessment that determined there was a low probability that medical information was compromised.	Breach does not include: 1. Unintentional acquisition, access, or use of PHI by authorized person if made in good faith within scope of authority and no further use/disclosure in a manner not permitted by Privacy Rule. 2. Inadvertent disclosure by authorized person to another authorized person at same covered entity (CE) or business associate (BA) or organized health care arrangement, and no further use/disclosure in a manner not permitted by Privacy Rule. 3. Disclosure where CE or BA has good faith belief that the recipient would not reasonably have been able to retain the information. An acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule is a reportable breach, *unless* the covered entity demonstrates a low probability that the PHI has been compromised based on a risk assessment of the following four factors, plus any other relevant factors: 1. The nature/extent of the PHI involved, including types of identifiers and the likelihood of re-identification. 2. The unauthorized person who used the PHI or to whom the disclosure was made. 3. Whether the PHI was actually acquired or viewed. 4. The extent to which the risk to the PHI was mitigated.

	BREACH OF COMPUTERIZED DATA	***BREACH IN A LICENSED HEALTH FACILITY***	***HIPAA BREACH REQUIREMENT***
EXCEPTIONS (CONT.)		6. A disclosure for which a health care facility or business associate, as applicable, determines that there is a low probability that medical information has been compromised based on a risk assessment of at least the following factors: ▪ The nature and extent of the medical information involved, including the types of identifiers and the likelihood of re-identification; ▪ The unauthorized person who used the medical information or to whom the disclosure was made; ▪ Whether the medical information was actually acquired or viewed; and ▪ The extent to which the risk of access to the medical information has been mitigated.	

	BREACH OF COMPUTERIZED DATA	***BREACH IN A LICENSED HEALTH FACILITY***	***HIPAA BREACH REQUIREMENT***
WHO MUST BE NOTIFIED	• California residents (individuals who live in California). • State Attorney General (AG) must be sent a sample notice if more than 500 California residents were required to be notified as a result of a single breach. (Redact personally-identifiable information in sample notice sent to AG.) *See oag.ca.gov/ecrime/databreach/report-a-breach.*	• Patient (or legal representative) • CDPH	• Patient (or legal representative) • DHHS Office for Civil Rights • Media must also be notified if more than 500 residents of a state or jurisdiction are affected. For breaches by a business associate or a subcontractor of a business associate, the subcontractor must notify the business associate, and the business associate must notify the covered entity of any breach. Once the covered entity is aware of the breach, it must report the breach as explained above. The covered entity is permitted, however, to coordinate with its business associate as to who will make the notification to patients. As a result, the business associate may make the patient notification, as agreed upon by the covered entity.
TIME FRAME FOR NOTIFICATION	Notification must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notification may be delayed if a law enforcement agency determines it will impede a criminal investigation. Notify when agency dedtermines it will not compromise the investigation.	No later than 15 business days after detection. However, must delay reporting upon law enforcement request.	To the patient: Without unreasonable delay and in no case later than 60 calendar days after discovery. To DHHS: Notify at the same time patients are notified, if more than 500 patients affected. Smaller breaches must be submitted via annual log each March 1 (Feb. 29 in leap years). To media: Without unreasonable delay and in no case later than 60 calendar days after discovery. Must delay notification upon law enforcement request.

	BREACH OF COMPUTERIZED DATA	***BREACH IN A LICENSED HEALTH FACILITY***	***HIPAA BREACH REQUIREMENT***
METHOD OF NOTICE	Notice may be provided by: 1. Written notice (on paper); 2. Electronic notice in conformity with the federal E-SIGN Act; or 3. Substitute notice if the costs of providing notice will exceed $250,000 or if more than 500,000 consumers are affected, or if the business does not have sufficient contact information. Substitute notice consists of: ▪ E-mail notice when the business has an e-mail address; ▪ Conspicuous posting, for at least 30 days, on the website; and ▪ Notification to major statewide news media. For a breach regarding a user name or email address, in combination with a password or security question/answer that would permit access to an online account (and no other personal information defined above), notice may be provided in some cases in electronic form. *(See "E. Method of Notice to Patient" on page 12.4.)* However, may use another notification procedure in accordance with hospital policy.	▪ To the patient by U.S. mail to the last known address or by email. ▪ To CDPH: By phone, fax, email, or U.S. mail to the hospital's district office or through the online California Healthcare Event and Reporting Tool (CalHEART). Facilities may also use a hybrid approach, using CalHEART to make the initial report and submitting additional documentation to the local district office, referring the CalHEART confirmation number.	To the patient: Written notice or substitute notice. May notify by phone if urgent, but also need written notice. Substitute notice applies only where there is insufficient or out-of-date contact information for affected patient(s). If fewer than 10 patients in this category, use alternative form of written notice, phone, email, or other means. If more than 10, website notice for 90 days or media notice. Must include toll-free phone number for 90 days. To DHHS Office for Civil Rights: Via website www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html. To media: Press release to prominent media outlets serving the state or jurisdiction where affected patients reside.

	BREACH OF COMPUTERIZED DATA	***BREACH IN A LICENSED HEALTH FACILITY***	***HIPAA BREACH REQUIREMENT***
CONTENT OF NOTICE	Must be written in plain language and include: 1. Hospital's name and contact information. 2. The types of information breached. 3. If known: the date, estimated date, or date range of the breach. 4. The date of the notice. 5. Whether notification was delayed as a result of a law enforcement investigation, if that information. 6. A general description of the breach incident, if known. 7. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a SSN or driver's license or California ID number. 8. Information regarding identity theft prevention services, if offered *(see "G. Mitigation" on page 12.4, for further information)*. However, a covered entity is deemed to have complied with these content requirements if it complies with the HIPAA content requirements *(see far right column)*. A state-developed format may be used as described in Civil Code Section 1798.82(d).	To CDPH: ▪ Name and address of the health care facility where the breach occurred; ▪ Date and time that each breach occurred; ▪ Date and time that each breach was detected; ▪ Name of patient(s) affected; ▪ Description of the medical information that was breached, including the nature and extent of the medical information involved, including the types of individually identifiable information, and the likelihood of re-identification; ▪ Description of the events surrounding the breach; ▪ Name(s) and contact information of the individual(s) who performed the breach, any witness(es) to the breach, and any unauthorized person(s) who used the medical information or to whom the disclosure was made, to the extent known; ▪ Date that patient or patient's representative was notified, was attempted to be notified, or will be notified of breach; ▪ The contact information of a health care facility representative whom CDPH may contact for additional information; ▪ Description of any corrective or mitigating action taken by the health care facility; ▪ Any other instances of a reported event that includes a breach of that patient's medical information by the health care facility in the previous six years.	To patient/media: 1. Brief description of what happened, including the date of breach and date of discovery of breach, if known. 2. Description of types of unsecured PHI involved (such as whether full name, SSN, date of birth, home address, account number, diagnosis, disability code, etc.). 3. Steps patients should take to protect themselves from potential harm. 4. Brief description of what CE is doing to investigate, mitigate, and protect against further breaches. 5. Contact information for patients to obtain further information, including toll-free phone number, e-mail address, website address, or street address. 6. Use plain language — translate as required under other applicable laws. To DHHS Office for Civil Rights: *See OCR's website at* www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

	BREACH OF COMPUTERIZED DATA	BREACH IN A LICENSED HEALTH FACILITY	HIPAA BREACH REQUIREMENT
CONTENT OF NOTICE (CONT.)		To CDPH (cont.): ▪ A copy of the notification sent to the patient or patient's representative and any additional information provided to the patient or patient's representative relating to the breach. ▪ Any audit reports, witness statements, or other documents that the health care facility relied upon in determining that a breach occurred. To patient: ▪ A brief description of what happened, health care facility name and address, date of the breach, and the date of the discovery of the breach, if known. ▪ The types of medical information involved (e.g., full name, Social Security number, date of birth, home address, account number, diagnosis, or other types of information). ▪ Any steps the patient should take to protect himself or herself from potential harm resulting from the breach. ▪ What the health care facility is doing to investigate the breach, mitigate harm to individuals, and protect against any further breaches. ▪ Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an e-mail address, internet website address, or postal address.	

	BREACH OF COMPUTERIZED DATA	***BREACH IN A LICENSED HEALTH FACILITY***	***HIPAA BREACH REQUIREMENT***
OTHER			The HIPAA Privacy Rule permits an **"incidental disclosure,"** defined as: a use/disclosure "incident to" an otherwise permissible use/disclosure that occurs despite reasonable safeguards and proper minimum necessary procedures. *(See 45 C.F.R. Section 164.502(a)(1)(iii).)*