INITIAL STATEMENT OF REASONS

Summary of the Proposed Regulations

The California Department of Public Health (Department) proposes to adopt Chapter 13 (sections 79900-79905) of Division 5, Title 22 of the California Code of Regulations to establish standards for assessing breaches of a patient's medical information, and administrative penalties related to such breaches.

In 2008, Health and Safety Code section 1280.15 (Code) was enacted. The Code requires clinics, health facilities, home health agencies, and hospices (collectively, the health care facilities) to prevent the unlawful or unauthorized access to, and use or disclosure of, patient medical information (breaches). The Code authorizes the Department to assess administrative penalties against these health care facilities.

Policy Statement Overview

***Problem Statement**:* The Department, in its efforts to assess administrative penalties for breaches of patient medical information pursuant to the Code, requires regulations to establish a framework by which administrative penalties will be assessed in a fair and consistent manner, as well as to clarify reporting requirements for the health care facilities.

***Objectives (Goals)**:* Broad objectives of this proposed regulatory action are:

- Fewer breaches of patient medical information.
- Increased vigilance by health care facilities to protect patient medical information.
- Closer alignment of state and federal law relating to patient medical information breaches.
- Improved patient experiences for the people of California.

Benefits:

- Increased security of patient medical information.
- Health care facilities will be more protective of patient medical information.
- Health care facilities will be more efficient in their internal data protection processes due to federal and state alignment.
- Health care facilities will be more efficient in responding to breaches due to federal and state alignment.
- Increased consumer confidence in the security of medical information.
- Increased transparency and consistency in calculation of assessed penalties.

Evaluation as to Whether the Proposed Regulations are Inconsistent or Incompatible with Existing State and Federal Regulations

The Department has determined that the proposed regulations are compatible and consistent with existing state and federal laws. Under the Health Insurance Portability and Accountability Act (HIPAA), the federal government has established provisions relating to medical information breaches. In drafting these proposed regulations, the Department has extensively used the HIPAA regulations as a model for developing its own. However, in some cases the HIPAA provisions differ from the final regulations proposed herein. These differences are often the result of variation between existing state and federal law as they relate to privacy and medical information (i.e. differences between underlying statutorily defined terms). In other cases, the Department has modeled its regulations after HIPAA regulations, but constructed them differently when the Department finds such changes are in the best interest of the people of California. HIPAA's provisions are meant to be a "floor" for patient protection standards and a state may enact its own laws and regulations under certain circumstances, including, but not limited to, when the state's law provides greater protection. (45 C.F.R. §§ 160.201-205 (2013).) Therefore, the Department concludes that the proposed regulations are consistent with existing state and federal laws.

Background

The Department has regulatory oversight for more than 30 types of health care facilities and providers and approximately 10,000 facilities. The proposed regulations relate to the Department's assessment of administrative penalties for breaches of patient medical information by these health care facilities. Breaches of patient medical information are a serious national problem. One study found that 94% of hospitals experienced data breaches between the years 2010 and 2012. [1] In California alone, the Department received an estimated 8,400 reported breaches between January 1, 2016 and December 31, 2017. These proposed regulations clarify how the Department will enforce the Code.

Authority and Reference

The Department may promulgate the proposed regulation sections under the Department's regulatory authority provided by Health and Safety Code sections 131000, 131050, 131051, 131052 and 131200. The proposed regulation sections implement, interpret, and make specific Health and Safety Code section 1280.15.

Detailed Discussion of Each Regulation

The Department proposes to adopt the following sections to implement the regulations needed to address patient medical information breaches:

[1] Ponemon Institute LLC, Third Annual Benchmark Study on Patient Privacy & Data Security, December 2012

Section 79900. Applicability.

Adopt subdivision (a) that describes the applicability of Article 1 as it pertains to the assessment of administrative penalties. The subdivision explicitly states that the assessment of administrative penalties applies to violations of the Code, excluding other penalties that the Department is authorized to assess or relate to patient medical information breaches.

Adopt subdivision (b) that indicates the regulations apply only to breaches of patient medical information occurring on or after the effective date of this regulation. However, the proposed language makes clear that these administrative penalties will take into account the compliance history of the health care facilities three years prior to a breach, including compliance history three years preceding the effective date of this regulation, as required under section 79904(a).

Section 79901. Definitions.

Adopt subdivision (a)-(q) that defines terms used in the Code and Article 1. Each of the definitions is discussed below.

"Access" is defined in the proposed regulations to provide clarity. Here, the Department borrows the definition of the term from HIPAA[2] in an effort to promote uniformity between state and federal law and to simplify compliance for the regulated community.

"Breach" is defined to clarify what constitutes the "unlawful or unauthorized access to, use or disclosure of, patients' medical information," as provided by the Code. The definition of breach that the Department proposes is modeled largely on the definition of breach found in HIPAA.[3] The Department chose to use this definition of breach because facilities prefer as much uniformity between state and federal law as possible.

The definition of breach used in the proposed regulations captures the Code's language that refers to each individual unlawful or unauthorized access to, use, or disclosure of a specific patient's medical information. This language is similar to the HIPAA definition, which provides that a breach means "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."[4] The Department considered as an alternative using this exact definition, but decided against it as doing so would not account for state patient medical information breach exceptions discussed in more detail below.

[2] 45 C.F.R. § 164.304 (2013)
[3] 45 C.F.R. § 164.402 (2013)
[4] 45 C.F.R. § 164.402 (2013)

The breach definition in the proposed regulations further emulates federal law in the breach exclusion provisions found in section 79901(b)(1). Under the proposed definition, the Department provides for six exceptions to a breach of patient medical information, while HIPAA lists three such exceptions.

The first exception at section 79901, subdivision (b)(1)(A) addresses the inadvertent misdirection of internal paper records, emails, or faxes. The proposed regulatory language incorporates the statutory limits of what constitutes a breach in the Code. This first exception also somewhat mirrors the first and second HIPAA exceptions. However, the state requirement is stricter as it is limited to internal paper records, emails, and faxes. The intent of this section is to exclude from the definition of a breach inadvertent access, use, or disclosures of medical information made within a health care facility (including any business associates of the health care facility). This exception is intended to capture clinically integrated care settings in which patients typically receive health care from more than one provider. The Department understands that in the course of providing care, it is ultimately unavoidable to have inadvertent access to patient information under these circumstances, and the Department has determined that such access, use, or disclosure should not constitute a breach of patient medical information under state law. In its proposed regulation, the Department included language relating to the "access or use" of the "medical information," for consistency with the Code.

The second exception at section 79901, subdivision (b)(1)(B) provides that "any internal paper records, electronic mail or facsimile transmission *outside* [emphasis added] the same health care facility or health care system sent to a covered entity (45 C.F.R. § 160.103 (2014)) that has been inadvertently misdirected within the course of coordinating care or delivering services" is not considered a breach. The Department has determined that inadvertently misdirecting a record, email or fax to an entity that is a "covered entity" under HIPAA should not constitute a breach under state law and does not require reporting or the assessment of penalties. Under federal law, covered entities must comply with HIPAA privacy rules for safeguarding the privacy of patient medical information. Thus, these entities have established policies and procedures in place to appropriately handle medical information that has been inadvertently misdirected. The Department does not consider inadvertently misdirected medical information sent to a covered entity a greater threat than if medical information was inadvertently misdirected within a health care system.

The third exception at section 79901, subdivision (b)(1)(C) is similar to the third breach exception in HIPAA. The Department creates an exception in instances where there is a good faith belief on the part of a health care facility or its business associates that patient medical information in a disclosure is not reasonably likely to be retained. The Department's proposed language is modelled after federal law, with the exception of certain defined terms. In addressing the relevant section of federal law in the Federal Register, the United States Department of Health and Human Services (HHS) provided examples of how this section would be applied, and the Department finds the reasoning of HHS applicable for these regulations as well. HHS suggests that, for example, if a

covered entity sends a number of explanation of benefits (EOBs) to the wrong individuals and a few of the EOBs are returned, the covered entity can conclude that the improper addressees could not reasonably have retained the information. (78 Fed.Reg. 5640 (Jan. 25, 2013).) The Department adopts this rationale as it applies to breaches under these regulations.

The fourth exception at section 79901, subdivision (b)(1)(D) provides that access, use, or disclosure of patient medical information is not a breach if it is permitted or required by state or federal law. In creating this exemption, the Department wanted to capture permitted and required disclosures provided for under Civil Code section 56 *et seq*. and other state and federal provisions relating to permitted and required disclosures of medical information.

The fifth exception at section 79901, subdivision (b)(1)(E) relates to lost or stolen electronic data containing patient medical information. Under the proposed regulation, in the event a health care facility loses or has stolen electronic patient medical records or other similar data, it would not be considered a breach provided that the electronic data has been encrypted, and there is no evidence of subsequent access, use, or disclosure of the data. It is not uncommon for potential breaches to be reported in the form of misplaced electronic data, such as a stolen laptop. The Department has determined that adequate encryption, as provided in the definition, sufficiently eliminates the potential for a breach, absent evidence that there has been unauthorized access, use, or disclosure of the patient medical information. However, a stolen or lost laptop that was not encrypted has a high enough probability of being a breach that it shall be presumed a breach. This will further create an incentive for health care facilities to encrypt electronic data.

The sixth exception at section 79901, subdivision (b)(1)(F) is based on similar breach provisions within the HIPAA definition found at 45 C.F.R. § 164.402(2). Under this provision, the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of HIPAA is presumed to be a breach. However, a covered entity or business associate can overcome this presumption with a showing that there is a low probability that protected health information has been compromised. The Department has included similar language in its definition, making minor changes to capture California specific definitions. In both the proposed language and the federal law, in determining whether the data has been compromised, health facilities must complete a "risk assessment." The proposed risk assessment will bring state and federal law into alignment and allow health care facilities to employ the same process for reviewing a breach and reporting it pursuant to both state and federal law. In providing the rationale for the risk assessment that it promulgated, HHS noted that "there are several situations in which [a breach] is so inconsequential that it does not warrant notification." (78 Fed.Reg. 5642 (Jan. 25, 2013).) HHS discusses the rationale for these four factors at length in the Federal Register (*ibid*.) The Department concurs with and adopts this rationale and includes it in the Documents Relied Upon.

In determining the definition of "Breach," the Department also considered the first sentence of the Code, which provides that the health care facility shall "prevent unlawful or unauthorized access to, and use or disclosure of, patients' medical information, as defined in section 56.05 of the Civil Code and consistent with section 1280.18" of the Health and Safety Code. Section 1280.18 provides, in part, that "every provider of health care shall establish and implement appropriate administrative, technical and physical safeguards to protect the privacy of a patient's medical information. Every provider of health care shall reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use, or disclosure." The Department interprets that the proposed regulations are consistent with section 1280.18.

"Business associate" is defined to clarify the relationship between a health care facility and any associates, agents, contractors, or other such entities in which the health care facility, in general terms, shares patient medical information as part of a contractual obligation. The definition is intended to limit who may be classified as a business associate. Under the proposed regulations, a business associate may be a person or entity (including any agents or subcontractors) that has entered into a contractual agreement with a health care facility or a larger health care system. The nature of the contractual agreement must pertain to those activities provided for under subparagraph (1), relating specifically to the creating, receiving, maintaining or transmitting of medical information. The regulation requires that these uses must be for a function or activity regulated by Subchapter C of Subtitle A of Title 45 of the Code of Federal Regulations. This subchapter, "Administrative Data Standards and Related Requirements," covers HIPAA standards for the use of patient medical information. By referring to HIPAA, the Department has determined that the regulation will capture all uses permitted under federal law and therefore will not exclude any business associate activities or functions that should be included in the regulation. Furthermore, subparagraph (1) mirrors part of the definition of business associate found in HIPAA. (45 C.F.R. § 160.103 (2014).) This federal definition provides, in part, that a business associate is one that "creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. § 3.20, billing, benefit management, practice management, and repricing." Thus, the Department's definition essentially captures the same functions and activities. Similarly, subparagraph (2) is created to capture the types of functions and activities permitted under a business associate contractual relationship. The Department's proposed language includes legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services when the provision of services involves medical information disclosure. The language drafted in this subparagraph is similar to the HIPAA definition of business associate. Subparagraph (3) clarifies that workforce members of health care facilities, their affiliated health care systems, and health care providers are not business associates.

"Business day" is defined to avoid any confusion in calculating business days for the purposes of the reporting requirements. The Department's definition is based on the definition found in Civil Code section 1689.5(e). The Department, however, adds Saturday as a non-business day and deletes Columbus Day as a holiday from the Civil Code definition.

"Department" is defined in the regulations as it is in this Initial Statement of Reasons, for the purpose of making the regulation text more readable.

"Detect" is defined to bring clarity to when the reporting requirements of the health care facility are to become active. The definition provides that the detection of a breach includes not only the discovery of a breach, but also the reasonable belief of a breach. In considering how to define this term, the Department relied on part 164.404(a)(2) of Title 45 of the Code of Federal Regulations. The Department has determined that health care facilities must report breaches not only when there is certainty of a breach, but also when the health care facility is reasonably certain that a breach may have occurred. Detection of a breach occurs when known by a health care facility or business associate, or when a health care facility or business associate would have known through reasonable diligence. The Department's rationale for including business associates is that the parties have entered into a contractual relationship when a health care facility has entrusted sensitive patient medical information to the business associate with appropriate contractual protections and requirements in place. The medical information has been entrusted to the health care facility by the patient. The care of the medical information is ultimately the responsibility of the health care facility, and as such any breach detection by a business associate is imputed to the health facility.

"Disclosure" is based on the definition of the term from HIPAA (45 C.F.R. § 160.103 (2014)) in an effort to promote uniformity between state and federal law and to simplify compliance for the regulated community.

"Encrypted" is based on the HIPAA definition of "encryption" (45 C.F.R. § 164.304 (2013)) in an effort to promote uniformity between state and federal law and to simplify compliance for the regulated community. The Department found that it is necessary to clarify in the definition that the "confidential process or key" has not been compromised, which would defeat the purpose of encryption.

"Factors outside the control of the health care facility" is defined to clarify under what circumstances the Department will consider those factors outside a health care facility's control when determining what administrative penalties to assess for a breach. Pursuant to the Code, the Department is to consider, among other things, "factors outside its control that restricted the facility's ability to comply with this section." The Legislature, however, did not define what constitutes a factor outside of a health care facility's control. The Department's definition has addressed this omission by adding "factors outside the control of the health care facility" which it has determined covers factors

outside of a health care facility's control in a way that is consistent with the original intent of the statute. The Department's definition is intended to capture events that are truly outside the control of a health care facility. These include natural disasters and severe weather as well as other factors outside the control of the health care facility such as war and civil unrest. The elements of the definition of "factors outside the control of the health care facility" are based upon basic *force majeure* provisions found commonly in contract law. Health facilities, under the doctrine of non-delegable duties, are responsible for the actions of their workforce and their business associates. Interpreting the statute to include workforce member actions is consistent with legislative intent and aligns with relevant case law, including *California Assn. of Health Facilities v. Department of Health Services* (1997) 16 Cal.4th 284 [65 Cal.Rptr.2d 872], where the Supreme Court of California held that unreasonable actions of employees are imputed to long-term health care facility licensees.

"Health care facility" is defined to provide clarity and serve as a more readable reference to all of the types of health care facilities licensed under their respective statutes. The Department also includes in its definition of health care facility a provision that states "[f]or purposes of this chapter, a "health care facility" as it relates to a breach of a patient's medical information shall include workforce members, medical staff, and business associates at the time of the breach and the detection of the breach." This provision is included to clarify that, for the purposes of committing a breach of a patient's medical information, the actions of the workforce of a health care facility, or the medical staff, or its business associates are imputed to the health care facility. The workforce, medical staff, and business associates are folded into the definition of health care facility primarily for the ease of the reader when reviewing the specific regulation text and to avoid the repetition of these terms throughout. From a policy perspective, the Department finds it is appropriate to include the actions of the workforce, medical staff, and business associates for which the health care facility is to be responsible. This is consistent with the doctrine of non-delegable duties in which a health care facility is responsible for the acts or omissions of its employees or contractors. Furthermore, this provision is consistent with federal law. (45 C.F.R. § 160.402 (2013).)

"Health care system" is defined to provide clarity as to the meaning of the term as used in the Code. Subsection (a) of the Code references a health care system; however, "health care system" is not defined under the Code. The Department considered basing the term on the HIPAA definition of "organized health care arrangement" found at 45 C.F.R. § 160.103, though this term appeared to be too broad, as defined. Ultimately, the Department solicited input from the California Hospital Association (CHA). The CHA proposed an option that served as the basis for the Department's definition. In doing so, the CHA indicated that it "tried to develop a definition that includes all 'systems' that share a responsibility for managing/coordinating the health care of a patient, that deliver services to the same patients, that refer patients to each other, and that share health care information about their patients with each other." This definition covers, generally: health care facilities and their medical staffs under common ownership or control, entities that participate in "organized health care arrangements" as defined under

HIPAA, "affiliated covered entities" also provided for by HIPAA, entities that participate in health care provider networks, and health plan networks. The Department has determined that these four elements sufficiently capture the components of a health care system.

"Medical information" is defined in the regulations as it appears in Civil Code section 56.05. This section is referenced in the Code as the definition of "medical information." The full definition is added for ease of the reader. A recent court case (*Eisenhower Medical Center v. Superior Court of Riverside County* (2014) 226 Cal.App.4th 430 [172 Cal.Rptr.3d 165]) held, in part, that the definition of "medical information" includes a patient's "individually identifiable information" that relates specifically to a patient's medical history, mental or physical condition, or treatment. The Department evaluates potential breaches in accord with the court's holding. However, as noted in footnote 4 of the opinion, "[i]t was remarked during oral argument that in some cases the very fact that a person is or was a patient of certain health care providers, such as an AIDS clinic, is more revelatory of the nature of that person's medical condition, history, or treatment. We are not presented with, and express no opinion concerning, such a situation." (*Id*. at p. 8.) Unless there is further legislation, case law, or regulation defining medical information to the contrary, the Department considers the information in the example cited above, i.e., the specific nature of a facility at which treatment is sought, to be medical information. The Department will determine if similar facts and circumstances constitute "medical information" on a case-by-case basis.

"Medical Staff" is defined to include licensed medical providers contracted to provide medical services to patients in a licensed facility. This definition is written to specifically include physicians practicing in a facility who may or may not be employees of that facility because these medical providers have the same or similar access to medical information as facility employees. Breaching confidential medical records is not an act in furtherance of the practice of medicine, as such, these regulations do not violate the bar on the corporate practice of medicine. The proposed regulations do not interfere with or influence a physician's professional judgment and practice of medicine. The definition of medical staff includes the employees and agents of the licensed medical provider to ensure that staff of the medical provider who have access to health care facility records by virtue of their employment are subject the same requirements as the health care facility.

"Reported event" is defined herein as it is in the Code and included in the regulation text for ease of the reader.

"Subsequent occurrence" is defined to provide clarity to the term as it is used in the Code. The Department structured this definition after considering many alternatives. The concept of a "subsequent occurrence" is inherently problematic as it implies that a breach and a subsequent breach need to be linked, either temporally or situationally. However, setting a fixed time element or situational requirement could be arbitrary. For example, the Department considered a definition that required a subsequent occurrence

to be limited to a breach that occurred within 24 hours of an initial breach. Similarly, the Department considered adding a component that required a subsequent occurrence to be limited situationally, such as if it related to the same hospital visit or injury. Ultimately, the Department rejected a bright line rule, and it constructed a definition that allows the Department to determine what constitutes a subsequent occurrence (based on what is substantially related) on a case-by-case basis. For example, assume a patient is in the hospital for a surgical procedure that requires a lengthy stay and during the stay the patient's medical information is breached by a nurse and the Department is notified of the breach as a reported event. Later in the patient's stay, another workforce member breaches the patient's medical information, which is also reported. Because these two breaches are substantially related, the second breach constitutes a subsequent occurrence. However, assume that patient is discharged and returns to the hospital two days later for an injury that is unrelated to the earlier surgical procedure, and once again the patient's medical information is breached and reported as a reported event. Despite the proximity in time, these two breaches are not substantially related and the most recent breach would not be a subsequent occurrence to the first breach. The Department will identify and evaluate subsequent occurrences on a case-by-case basis.

"Unauthorized" is defined as it is in the Code. Pursuant to the Code, "unauthorized" means the inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment, or other lawful use as permitted by the Confidentiality of Medical Information Act (Part 2.6 (commencing with section 56) of Division 1 of the Civil Code) or any other statute or regulation governing the lawful access, use, or disclosure of medical information. "Unauthorized" is defined herein as it is in the Code and included in the regulation text for ease of the reader.

"Workforce" is defined as employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a health care facility or business associate, is under the direct control of such health care facility or business associate whether or not they are paid by the health care facility or business associate. This definition is modeled after the definition in HIPAA (45 C.F.R. § 160.103 (2014)); however, the Department's definition includes the term "health care facility.".

Section 79902. Breach Reporting Requirements.

Adopt subdivision (a) that offers additional detail regarding the requirements for breach reports that health care facilities must provide to the Department in the event of a breach. Under the proposed regulations, a health care facility may report a breach to the Department via fax, email, phone, Department website, or mail. Health care facilities are required to notify the Department no later than 15 business days after a breach has been detected as provided for in the Code.

Adopt subdivision (a)(1)(A)-(M) that relates to breach reporting requirements. In reporting the breach of a patient's medical information, the Department has identified 13 separate data elements that a health care facility must provide to the Department.

These data elements are intended to provide the Department with all the information necessary to conduct a thorough investigation of a breach and assess a potential administrative penalty as efficiently and fairly as possible. The Department reviewed HIPAA's requirements for reporting breaches to HHS (45 C.F.R. § 164.408 (2013)); however, such requirements run counter to the requirements of the Code and as such were not helpful to the Department in drafting these regulations.

Adopt subdivision (a)(2) that requires health care facilities to report additional information relevant to a breach as it becomes available beyond the 15-business day timeline. The Department is aware that a health care facility may not have all of the required data elements within the 15-business day reporting requirement. The Department will permit a health care facility to submit additional information as it becomes available, so long as a health care facility is making a good faith effort to provide the data elements in a timely fashion. The Department considered, as an alternative, requiring the reporting of a breach within 15 business days strictly, but decided that providing some flexibility to a health care facility, in light of the varied nature of breaches, is preferable.

Adopt subdivision (a)(3) that provides that in the event a health care facility fails to report a medical information breach to the Department, the health care facility may be subject to administrative penalty pursuant to the Code, not to exceed the statutory limits set forth therein. The department considered alternatives including requiring the assessment of an administrative penalty if a health care facility fails to notify the department but chose to maintain flexibility in assessing penalties

Adopt subdivision (a)(4) that provides that a breach shall not be deemed reported unless the health care facility has provided the Department with the data elements required pursuant to subdivision (a)(1). As noted above, the Department acknowledges that not all such data elements may immediately be available. However, a health care facility must make a good faith effort to provide the required data elements to the Department as they become available and without any unreasonable delay. The Department will determine whether the delay is "unreasonable" on a case-by-case basis. In assessing reasonability, the Department will consider factors including, but not limited to, the size of the affected population, lack of sufficient information in the reporting of an incident to make a determination of compliance, time passed between the time of an incident and its discovery, whether the cause of an incident was a business associate or workforce member, and availability of staff to respond to an incident. The Department has included this section as it has experienced several instances when health care facilities were reluctant to turn over information relating to breaches, or when a health care facility attempted to require the Department to take additional administrative steps to access the data elements needed for the Department's investigation. These efforts on the part of some health care facilities have served only to impede the Department's investigations. Thus, the Department has found it necessary to address such actions in the proposed regulations, including clarifying that should a health care facility withhold information relating to an investigation by the

Department, the health care facility is subject to administrative penalties pursuant to section 79902(a)(3).

Adopt subdivision (a)(5) that provides a requirement for a health care facility to document instances in which it has performed a risk assessment pursuant to section 79901(b)(1)(F) and determined that there has not been a breach. The Department includes this requirement to serve as a check in a health care facility's unilateral determination of whether a breach exceeds the risk assessment test. The Department is aware that, in weighing the risks of a breach, it may be in a health care facility's interest to find that a breach did not occur. As a counterbalance to this interest, the Department shall require a health care facility to collect and maintain the documentation used to make its determination. The Department, as allowed by law, may inspect a health care facility, and under these proposed regulations, a health care facility must provide a centralized record of each such risk assessment. The Department requires health care facilities to keep such records for six years from the time of the breach. Currently, HIPAA requires a similar record-keeping period (45 C.F.R. § 164.530(j)(2) (2009)) and the Department adopts this period in the interest of harmony between state and federal law.

Adopt subdivision (b) that requires health care facilities to notify a patient or the patient's representative of a medical information breach, as provided in the Code. Additionally, the section provides for the method of notification by a health care facility. The regulation provides that the patient or patient's representative must be notified by first-class mail or electronic mail, if the individual has agreed to notification by electronic mail and that agreement has not been withdrawn. This language provides clarity to health care facilities about how they may notify the patient or patient's representative. In determining the means by which notifications should be sent, the Department based its regulations on requirements found in federal law. (45 C.F.R. § 164.404(d) (2009).) The Department considered the addition of several other provisions found in HIPAA relating to such notice. For example, HIPAA has lengthy provisions relating to substitute notice and additional notice in urgent situations. However, the Department weighed these options and determined that the notice requirements as written in the regulations are sufficient. The Department further considered including a provision that would require, among other things, health care facilities to notify local media outlets in the event the health care facility breached the medical information of 500 or more patients. Such a requirement would mirror existing federal law for similar events. However, the Department ultimately determined that such a requirement would be duplicative, as a health care facility already must do so under 45 Code of Federal Regulations part 164.408(b) (2013).

Adopt subdivision (b)(1)(A)-(E) that provides additional detail about the information a health care facility must provide to the patient or patient's representative. The Department specifies five elements that need to be included in the notice sent by the health care facility so that these notifications may be uniform to patients and reasonably notify patients of a breach. The elements included were largely modeled on reporting

requirements to patients currently found in HIPAA (45 C.F.R. § 164.404(c) (2009)), although the Department modified these requirements slightly to comport with the proposed regulatory scheme and state law.

Adopt subdivision (b)(2) that requires notifications to the patient or patient's representative to be provided in plain language. This section was included to help alleviate any confusion that a patient or patient's representative might experience upon receiving such a notice.

Adopt subdivision (b)(3) that provides that in the event a health care facility fails to notify the patient or the patient's representative about a medical information breach, the health care facility may be subject to administrative penalty pursuant to the Code, not to exceed the statutory limits set forth therein. The department considered alternatives including requiring the assessment of an administrative penalty if a health care facility fails to notify or delays notifying patients but chose to maintain flexibility in assessing penalties. Some breaches may involve millions of patients' information requiring a lengthy and involved notification process. In consideration of the difficulties inherent in the process of notifying patients of a breach incident the department maintains flexibility in assessing this administrative penalty.

Section 79903. Administrative Penalties.

Adopt subdivision (a) that provides that in the event the Department determines that a health care facility breaches a patient's medical information, the health care facility will be subject to administrative penalty pursuant to the Code, not to exceed the statutory limits set forth therein.

Adopt subdivision (b) that sets forth the base penalty amount for a breach. In determining how to create a penalty framework, the Department considered many alternatives. In the framework that the Department has selected, each breach of a patient's medical information will be initially assessed a base penalty of $15,000. Once this penalty is assessed, the breach will be considered in light of the penalty adjustment factors provided for in section 79904. Thus, the base penalty of $15,000 will be adjusted upwards or downwards, based on these factors. The Department has determined that this approach provides a simple and straightforward framework for the assessment of breach penalties that will be easy for the regulated community to understand and relatively simple to apply. The Department is hopeful that this framework will allow for the expedient assessment of penalties; something that the relevant health care industry has expressed concerns about to the Department in the past. In selecting the amount of $15,000 for the base penalty for a breach, the Department considered many factors. First and foremost, the Department wanted to create some form of graduated penalty amounts, depending on the nature of a breach. That is, the Department wanted flexibility to assess higher or lower penalties when appropriate. The Code allows for a minimum of a $0 penalty and the maximum of a $25,000 penalty. The proposed

$15,000 base penalty amount reflects the severity of a breach violation yet allows for penalty adjustment factors to be implemented, if they apply.

Currently, the Department does not assess administrative penalties for most inadvertent yet unauthorized access and disclosures of patient medical information. However, breaches that occur as a result of health care facilities' negligence can be just as harmful to a patient as those that are willful or malicious in nature. Thus, the Department determined that the proposed base amount will create an incentive for health care facilities to improve internal policies and procedures related to medical information protection.

The Department also considered creating a large matrix that assessed a penalty for all breaches (regardless of the nature of the breach) at a percentage of the statutory maximum, based on the type of facility involved. The Department ultimately decided against this alternative as it was unwieldy, confusing to apply, and potentially arbitrary in its base penalty percentages. As another alternative, the Department considered creating categories of breaches and assessing penalties based on the type of breaches. This required multiple sets of penalty adjustment factors that were cumbersome to apply. By creating a single breach category for penalty assessment and then applying appropriate adjustment factors the Department has crafted a framework that is simple to apply and easy to understand.

Adopt subdivision (c) that sets forth the standards for dealing with subsequent occurrences of a breach. The rationale and application of subsequent occurrences are discussed at length in the definition of the term, above. The Department chose to use the penalty amount of 70% of the final penalty amount based on the Code. The Code provides that the Department "may assess an administrative penalty for a violation of this section of up to twenty-five thousand dollars ($25,000) per patient whose medical information was unlawfully or without authorization accessed, used, or disclosed, and up to seventeen thousand five hundred dollars ($17,500) per subsequent occurrence." As the Code provides that the maximum penalty for a subsequent occurrence is 70% of the maximum amount of the initial violation, the Department concluded that all subsequent occurrences should be based on this percentage. So, for example, assume a breach occurs and a base penalty is assessed at an amount of $15,000 pursuant to section 79903(b). Assume further that various penalty adjustment factors are applied pursuant to section 79904, resulting in a final penalty of $10,000. In the event of a subsequent occurrence, a penalty of $7,000 will be assessed (the sum of $10,000 x .70), but then that subsequent occurrence will further be subject to the penalty adjustment factors of section 79904. However, no penalty shall exceed the statutory maximum of $17,500 per subsequent occurrence. Therefore, in a scenario where the penalty adjustment factors are applied to the subsequent occurrence penalty amount and the sum is greater than the statutory maximum, the final penalty amount shall be capped at $17,500.

Section 79904. Penalty Adjustment Factors

Adopt subdivision (a) that provides that once the base penalty has been applied, pursuant to section 79903 (b) or (c), the Department is to adjust the penalty, if applicable, based on the penalty adjustment factors found within this section. There are four adjustment factors. The first three – compliance history, preventative actions to immediately correct and prevent past violations from recurring, and factors outside the control of the health care facility– are required by the Code. The final factor, "Any other factors applicable to the specific circumstances surrounding the breach, as identified by the Department" preserves the Department's "full discretion to consider all factors" in determining the amount of an administrative penalty, as granted by the Code. Allowing for the identification of additional factors applicable to specific circumstances surrounding a breach gives the Department latitude to adjust penalty amounts appropriately for unique circumstances.

Adopt subdivision (a)(1) that expands upon the Code's requirement that the Department factor into the administrative penalty assessed a health care facility's compliance history with the Code and other related stated and federal privacy statutes and regulations. However, the Code does not address how far back the Department shall consider this history. After some deliberation, the Department decided that it will factor in a health care facility's compliance history for the previous three calendar years. The Department considered various temporal options – one year and two years, for example – but decided three years provided the Department with the most accurate basis for determining compliance history. The Department also determined that three years provides additional incentive to be compliant with state and federal law.

Adopt subdivision (a)(2) that, similar to subdivision (a)(1), provides for the application of a penalty adjustment factor. As required by the Code, the Department factors in the extent to which the health care facility detected a violation and took preventative action to immediately correct and prevent past violations from recurring. For example, if a health care facility takes action within 24 hours of a breach, the health care facility's penalty may be adjusted downward. However, if a health care facility is slow to respond to a breach despite its ability to respond faster, a penalty may be adjusted upward. Due to the unique nature of each incident and variation in facility resources, the Department will evaluate health facility responses on a case-by-case basis.

Adopt subdivision (a)(3) that creates a penalty adjustment factor for instances when "factors outside the control of the health care facility" restrict a health care facility's ability to comply with the Code. Factors outside the control of the health care facility is defined and discussed at length in the Definitions section. The Department has determined that a substantial penalty adjustment downward is appropriate in the event of a factor outside the control of the health care facility, as the term is defined. Common sense suggests that in the event of some devastating natural disaster or other similar situation, a health care facility cannot reasonably be held fully or partially liable. However, a health care facility is required to have developed and maintained disaster and emergency policies and procedures and implemented them during such an event.

Adopt subdivision (a)(4) that allows the Department to weigh other factors applicable to specific circumstances surrounding a breach. The Code grants the Department "full discretion to consider all factors when determining . . . the amount of an administrative penalty, if any." Due to the wide variety of breaches being reported, the Department determined that it is in the best interest of patients and the regulated community for the Department to use the full discretion granted by the Code and have the ability to identify and weigh appropriate factors based on the unique circumstances of a breach.

Adopt subdivision (b) that provides for the Department to exercise its full discretion in reducing a final penalty amount. Such discretion applies to situations in which a final assessed penalty amount represents in the Department's determination too great of a burden on a health facility, or if an amount is deemed excessive due to the unique circumstances particular to a breach. In determining whether a penalty is unduly burdensome or excessive, the Department may rely on subdivision (b) to reduce an administrative penalty to zero. The Department does not anticipate using this provision frequently. However, the Department determined that it would be in the public's interest to provide an avenue for relief in this manner, if needed. For example, if a hospital is struggling to stay open due to financial stress and a patient was not placed at risk for harm due to a breach, the Department could weigh such factors in determining whether to issue a penalty at all.

Section 79905. Small and Rural Hospitals; Primary Care Clinics; and Skilled Nursing Facilities.

Adopt subdivision (a) that provides an option for a small and rural hospital, as defined in Health and Safety Code section 124840, that has been assessed an administrative penalty to submit a written request for an extended payment plan if immediate full payment of the penalty would cause financial hardship to the hospital. This subdivision is necessary to address the statutory mandate of section (e) of the Code and to describe a process for the Department to review these special circumstances. The Department based this proposed section on the recently approved Hospital Administrative Penalties regulation package, which provides for similar provisions related to administrative penalties. (Cal. Reg. Notice Register 2012, No. 43-Z, p. 1564.)

Adopt subdivision (b) that provides for additional considerations to be given to primary care clinics as defined in Health and Safety Code section 1204(a). This subdivision is necessary to address the statutory mandate of section (e) of the Code. The Department, while taking into consideration such circumstances, shall reduce the base penalty by one-half. The base penalty for primary care clinics, however, is still subject to the penalty adjustment factors pursuant to section 79904. The penalty adjustment factors shall also be reduced by one-half, resulting in a maximum increase or decrease of $5,000 from the base penalty. The Department chose a reduction of one-half as it is a substantial reduction and takes into consideration the unique role of these health care facilities. The Department considered alternative reductions to the final penalty but

determined that alternative reductions would limit the effectiveness of the Department's efforts to discourage breaches.

Adopt subdivision (c) that provides regulatory language that captures statutory requirements found in section (e) of the Code. In the event any health care facility subject to Health and Safety Code section 1423, 1424, 1424.1, or 1424.5 may be assessed an administrative penalty under the Code and Health and Safety Code section 1423, 1424, 1424.1, or 1424.5, the Department will issue only the higher penalty, as required by the Code. This provision is included in the proposed text for ease of the reader.

Reasonable Alternatives (Gov. Code, § 11346.2(b)(4)(A))

Reasonable alternatives to the proposed regulations are addressed throughout this Initial Statement of Reasons in the detailed discussions of each section.

Reference Documents

- Ponemon Inst., Third Annual Benchmark Study on Patient Privacy & Data Security (December 2012).
- Redspin, Inc., Breach Report 2013: Protected Health Information (PHI) (February 2014).
- The Health Insurance Portability and Accountability Act of 1996 (Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996), Parts 160 and 164.
- Federal Register vol 78, no. 17, Jan. 25, 2013 (Part II).
- Cal. Reg. Notice Register 2012, No. 43-Z, p. 1564.
- *California Assn. of Health Facilities v. Department of Health Services* (1997) 16 Cal.4th 284 [65 Cal.Rptr.2d 872].
- *Eisenhower Medical Center v. Superior Court of Riverside County* (2014) 226 Cal. App. 4th 430 [172 Cal.Rptr.3d 165].

Specific Technologies or Equipment

This regulation does not mandate the use of specific technologies or equipment.

Significant Adverse Impact on Business

No facts, evidence, documents, testimony, or other evidence of any significant adverse economic impact on business have been identified because depending on the type and frequency of information breach, a penalty would vary from no cost to a potentially substantial cost. However, this regulatory action has a built-in procedure to adjust costs for facilities for which penalties are a burden.

Reasonable Alternatives the Department Has Identified That Would Lessen Any Adverse Impact on Small Business, Including Ability to Compete

The Department has determined that the proposed regulatory action would have no significant adverse economic impact on California business enterprises and individuals, including the ability of California businesses to compete with businesses in other states. Additionally, reasonable alternatives to the proposed regulation that would lessen any adverse impact on small businesses including the ability to compete are discussed throughout the Initial Statement of Reasons.

Effect on Small Business

The Department has determined that there would be an effect on small business because small businesses will be legally required to comply with the regulation and may incur a financial penalty from the enforcement of the regulation. Depending on the type and frequency of information breach, a penalty would vary from no cost to a potentially substantial cost. However, the proposed regulation has a mechanism to adjust costs for facilities for which penalties are a burden.

STATEMENTS OF DETERMINATION

Alternatives Considered

The Department has determined that no reasonable alternative considered, identified, or otherwise brought to the attention of the Department would be more effective in carrying out the purpose for which the action is proposed or would be as effective as and less burdensome to affected private persons than the proposed action.

Local Mandate Determination

The Department has determined that the proposed regulations do not impose a mandate on local agencies or school districts that requires state reimbursement.

Economic Impact Determination

The Department has made an initial determination that these regulations would not have a significant statewide adverse economic impact directly affecting businesses, including the ability of California businesses to compete with businesses in other states. The proposed regulations would not significantly affect:

- The creation or elimination of jobs within the state because the Department estimates that the regulation's financial impact would be cost neutral and affected regulated entities are already paying the financial penalties as appropriate under existing statutes.
- The creation of new businesses or the elimination of existing businesses within the state because the Department estimates that the regulation's financial impact would be cost neutral and both existing and potential new businesses would pay similar financial penalties as appropriate under existing statutes.
- The expansion of businesses currently doing business within the state because the Department estimates that the regulation's financial impact would be cost neutral and affected regulated entities are already paying the financial penalties as appropriate under existing statutes.
- The regulatory action protects the patient's privacy rights regarding disclosures of medical information. Maintain security standards to prevent breaches which creates a positive impact to the health, safety and welfare of California. Also, the economy is not impacted because the Department estimates that cost is neutral as affected regulated entities are already paying the financial penalties as appropriate under existing statutes.

Effect on Housing Costs

The Department has determined that the regulations will have no impact on housing costs.