FINAL STATEMENT OF REASONS

As authorized by Government Code Section 11346.9(d), the California Department of Public Health (Department) incorporates by reference all contents of the Initial Statement of Reasons (ISOR) into the Final Statement of Reasons. The information contained in the ISOR at the time of the initial public notice remains unchanged except for the following modifications:

Section 79901

Subparagraph (d)

The Department chose to base the definition of the term "business day" on the one found in Civil Code section 1689.5(e). The Department added Saturday as a non-business day and Martin Luther King's Birthday as a holiday in an attempt to conform with common business practice in the regulated entities. The Department removed Columbus Day from the regulation text as this holiday is generally a business day for most regulated entities. The definition differs sightly from the Civil Code language because the Department recognizes Saturdays and Martin Luther King's Birthday as non-business days.

Subparagraph (l)

In response to a public comment, the Department has clarified the definition of the term "contractor" used in the definition of "medical information". The definition of "medical information" is identical to Civil Code section 56.05 (j). This provision has a unique definition of the term "contractor" found in Civil Code section 56.05(d). By incorporating, the definition of "contractor" found in Civil Code section 56.05(d) this will increase clarity and ensure the completeness of the definition of "medical information" by aligning these regulations with the Civil Code.

Subparagraph (m)

In response to a public comment, the Department has revised the definition of the term "medical staff" to use the definition found in 22 CCR 70703(a)(1) (governing medical staff in General Acute Care Hospitals (GACHs)). This definition is needed in order to specify which individuals are considered "medical staff," and to ensure medical providers who are practicing in a health facility will be subject to these regulations.

Section 79902

Subparagraph (a)(1)(F)

In response to a public comment, the Department has deleted the phrase "including whether the medical information was actually acquired or viewed" from the existing text. If the information referred to in this provision was not "acquired or viewed" there would be no breach as defined.

Subparagraph (a)(1)(G)

In response to a public comment, the Department has added the qualifier "to the extent known" to this provision. The Department recognizes that health facilities may not

always know all the details of a medical information breach when reporting a breach to the Department. Therefore, the Department has revised this requirement so only information known to the facility when the breach is reported is required to be reported at that time.

Subparagraph (a)(4)
In response to a public comment, the Department has deleted the words “soon as” from the second sentence of this provision. This change was made so that this section conforms with the requirements in subparagraph (a)(2) that health facilities must submit further information that was not available at the time of the initial report in an organized manner in a reasonable timeframe. This change improves the clarity and consistency of the regulation.

Statements of Determinations

Local Mandate
The Department has determined that the proposed regulation does not impose any mandate on local agencies or school districts, nor are there any costs for which reimbursement is required by part 7 (commencing with Section 17500) of division 4 of the Government Code, nor are there any other nondiscretionary costs imposed.

Impact on Small Business
The Department has determination that the regulations would not have a significant statewide adverse economic impact directly affecting business, including the ability of California businesses to compete with businesses in other states. Thus, there will be no significant adverse economic impact on California businesses.

Alternatives Considered
The Department has determined that no reasonable alternative it considered or that has otherwise been identified and brought to the attention of the Department would be more effective in carrying out the purpose for which the regulation is proposed, would be as effective and less burdensome to affected private persons than the adopted regulation, or would be more cost effective to affected private persons and equally effective in implementing the statutory policy or other provision of law.

ATTACHMENTS TO THE FINAL STATEMENT OF REASONS

ADDENDUM I

45-Day Public Notice

Summary of Comments and Responses to Comments Received During the Initial Public Notice Period

The Department received comments from five commenters during the initial public notice period beginning July 3, 2020, through August 21, 2020. No request for a public hearing was received and no hearing was held.

LIST OF COMMENTERS (WT - Written Testimony)

1. Providence St. Joseph Health (PSJH)
2. Sutter Health (SH)
3. California Hospital Association (CHA)
4. Dignity Health (DH)
5. Health Services of LA County (HSLAC)

1. Comment Subject: Section 79901(a) Access
Commenter(s): PSJH
Comment: "This definition should be revised to clarify that "access" means that someone actually read, wrote, modified, or communicated data/information or otherwise used any system resource, not just that a person had the ability or means necessary to do so. For example, every employee has the ability to read or communicate data/information. However, the employee should be considered to have "accessed" the information only if they have actually read it or communicated it. In addition, it is unclear what it means to "otherwise use any system resource." We suggest revising the definition to read as follows: "Access means reading, writing, modifying, or communicating data/information."

Department Response: The Department rejects this proposed amendment because the current definition of "Access" is based upon the definition found in The Health Insurance Portability and Accountability Act (HIPAA) , which is intended to promote uniformity between state and federal law and to simplify regulatory compliance. The Department has decided to keep the current definition to retain consistency between federal and state regulations.

2. Comment Subject: Section 79901(b)(1)(A) Breach
Commenter(s): PSJH
Comment: "We believe this definition inadvertently omits web-based communication. We suggest revising "Any paper record, electronic mail, or facsimile transmission…" to read as follows: "Any paper record or electronic communication…"

Department Response: The Department rejects this proposed amendment because the change would conflict with the plain language of the underlying statute, Health and Safety Code Section 1280.15, which uses the language: "Any paper record, electronic

mail, or facsimile transmission". The proposed amendment would substantially increase the scope of what is excluded from the definition of a breach beyond what is described in the statute. The Department rejects the revised definition to maintain consistency between the statutes and regulations.

3. Comment Subject: Section 79901(b)(1)(A) Breach
Commenter(s): PSJH
Comment: "We believe this definition inadvertently omits web-based communications as well as business associates, which must comply with HIPAA regulations just as covered entities must comply. We suggest revising the beginning of this sentence as follows: "Any internal paper record, ~~electronic mail or facsimile transmission~~ or electronic communication outside the same health care facility or health care system sent to a covered entity or business associate…"

Department Response: The Department rejects this proposed amendment because the proposed changed would conflict with the plain language of the underlying statute, Health and Safety Code Section 1280.15, which uses the language: "Any paper record, electronic mail, or facsimile transmission." The proposed amendment would substantially increase the scope of what is excluded from the definition of a breach beyond what is described in the statute. To maintain consistency between the statutes and regulations, the Department rejects the revised definition.

The Department also considered and rejected the addition of "business associate" to this section because it would depart from the language in Health and Safety Code Section 1280.15.

4. Comment Subject: Section 79901(c) Business Associate
Commenter(s): PSJH
Comment: "[We] strongly urge CDPH to adopt the exact HIPAA definition of "business associate." It is unclear why the proposed definition includes only one of the two paragraphs in the HIPAA definition -- because the Initial Statement of Reasons states that the proposed definition of "business associate" is similar to the HIPAA definition, we think perhaps an error was made in the proposed regulation. Under HIPAA, "business associates" include contractors that, ***on behalf of the covered entity,*** create, receive, maintain or transmit protected health information for claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management and repricing. By including only half of the HIPAA definition of business associate, this definition would convert all contractors of covered entities that use PHI to "business associates" of those covered entities, even if they were performing activities for their own purposes rather than on behalf of the covered entity. For example, a hospital that contracts with 10 different insurance companies would find that those 10 insurance companies are business associates under this definition. This is not the case under HIPAA — under HIPAA, they remain covered entities and not business associates. The problems with this definition are compounded by the proposed

definition of “health care facility” (see our comments on this below). We suggest deleting the proposed definition and replacing it with “’Business associate’ shall have the meaning of the term as provided for in Section 160.103 of Title 45 of the Code of Federal Regulations.”

Department Response: The Department rejects this proposal as the current definition of “Business Associate” was drafted to include elements of the HIPAA definition of Business Associate, as well as other elements, to meet the purposes of Health and Safety Code Section 1280.15. The purpose of this definition is 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. Including all elements of the HIPAA definition is unnecessary to fulfill the purpose of this definition as used in these regulations. The Department considered adopting the proposed amendment but determined the entire HIPAA definition was unnecessary for the purpose of effectuating Health and Safety Code Section 1280.15.

5. Comment Subject: Section 79901(f) Detect
Commenter(s): PSJH
Comment: “This definition lacks clarity. PSJH believes it means that the clock starts ticking (for purposes of the 15-day reporting timeline) when either the health care facility or a business associate discovers a breach. We do not believe the definition of “detect” is meant to imply that: (1) a health care facility is required to report a breach of information held by a business associate (whether or not the information relates to a patient of the health care facility); or (2) a reasonable belief that a breach occurred is reportable.

PSJH suggests that this provision be revised as follows: “’Detect’ means the discovery of a breach, ~~or the reasonable belief that a breach occurred~~ by a health care facility ~~or business associate~~. A breach shall be treated as detected as of the first business day on which such breach is known to the health care facility ~~or business associate~~, or by exercising reasonable diligence ~~would~~should have been known to the health care facility or business associate. A health care facility ~~or business associate~~ shall be deemed to have knowledge of a breach if such a breach is known, or by exercising reasonable diligence ~~would~~should have been known, to any person other than the person committing the breach, who is a workforce member or agent of the health care facility ~~or a business associate~~.”

Department Response: The Department rejects these proposed amendments. The current language of the Department’s regulatory proposal mirrors the construction of HIPAA and effectuates the purposes of Health and Safety Code Section 1280.15. The Department’s proposed 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 considered these proposed amendments but rejected them as an important element of this definition is the requirement that health care facilities report not only when there is a certainty of breach but also when there is reasonably certainty a breach may have occurred, and these amendments prevented that important policy objective.

In addition, the Department's purpose 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. Thus, it is critical to include business associates in these regulations to protect patient information.

6. Comment Subject: Section 79901(i) Factors outside the control of the health care facility
Commenter(s): PSJH
Comment: "Factors outside the control of the health care facility" means any circumstance not within the reasonable control of the health care facility, including, but not limited to, fires, explosions, natural disasters, severe weather events, war, invasion, civil unrest, acts or threats of terrorism, ~~and~~ utility or infrastructure ~~failure.~~ failure, acts of workforce members in violation of employer policy, acts of business associates in violation of their business associate contracts, and acts of criminals."

Department Response: The Department rejects this proposed amendment. This definition is intended to capture events that are truly outside the control of a health care facility. 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. The Department considered these proposed amendments, but they do not align with the purpose of this definition and would violate the doctrine of non-delegable duties as found in California case law.

7. Comment Subject: Section 79901(a) Access
Commenter(s): SH
Comment: The issue with the aforementioned definition is that it is overly broad. Generally speaking, a large number of employees may have the ability and/or means to

"read, write, modify, or communicate data" containing medical information, but it is not a breach until they do in fact "read, write, modify, or communicate data". For example, when a patient submits to Sutter a request to receive a copy of their records pursuant to 45 C.F.R. § 164.524, the employee(s) gathering responsive records has the ability and means to view records of many other patients/individuals but only gathers documents pursuant to the request. Under the aforementioned definition, this would be considered to be "access" and therefore reportable under the proposed provision relating to medical information breach. Sutter would recommend modifying the definition to provide a more concrete "access" and remove the language "the ability or means necessary".

Department Response: The Department rejects this proposed amendment because the current definition of "Access" is based upon the definition found in the Health Insurance Portability and Accountability Act (HIPAA) in an effort to promote uniformity between state and federal law and to simplify compliance for the regulated community. The Department desires consistency between federal regulations and state regulations. The Department considered the proposed definition, but it does not conform with HIPAA, as such the Department has decided to retain the current definition.

8. Comment Subject: Section 79901(f) Detect
Commenter(s): SH
Comment: "The issue with the aforementioned definition is that the word "detect", as defined, is vague, ambiguous, and overly broad in so much as the detection of the breach is directly linked to the discovery of the breach. Detection of a breach and discovery of a breach are entirely different occurrences. We suggest that "detect" should mean the substantiation of a breach via a discovery investigation. The discovery of a breach more likely than not requires an investigation to determine if any unauthorized use, access or acquisition of the data actually occurred. While it may be that a breach is identified immediately when it is "detected", detection does not always mean that a breach occurred. Licensed facilities need to have the ability to conduct a thorough investigation of a "detected" issue to determine whether or not the facts constitute a breach. Due to the ever-growing complexity of electronic health records and access thereto, it may take significantly longer than 15-business days to reasonably determine that a breach occurred. Sutter recommends that this definition should be amended to provide that once a breach is confirmed, or reasonably confirmed based upon an investigation, to have occurred, the 15-business day reporting requirement should begin.

Furthermore, the definition impermissibly places upon the licensed facility the liability for the acts and omissions of its business associates to whom it entrusts medical information. While federal law provides limited circumstances in which the knowledge of the business associate can be imputed onto its covered entity, the aforementioned definition of "detect" makes no similar qualification. Rather it would find a licensed facility liable for regulatory penalties and findings if its' business associate experiences a breach whether or not they know or even have reason to know of the incident. In order to mitigate the risk, the aforementioned definition would require the licensed facility to

maintain control over the privacy and security of medical information not in its control, and even control the business associates use/processing of such medication information, thus defeating the entire business associate relationship. Therefore, Sutter would further recommend the deletion of "business associate" from the definition entirely in order to promote uniformity between state and federal law."

Department Response: The Department rejects these proposed amendments as the current language mirrors the construction of HIPAA and the effectuates the purposes of Health and Safety Code Section 1280.15. 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 considered these proposed amendments but rejected them as an important element of this definition is the requirement that health care facilities report not only when there is a certainty of breach but also when there is reasonably certainty a breach may have occurred, and these amendments prevented that important policy objective.

The Department's purpose 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. Thus, it is critical to include business associates in these regulations to protect patient information.

9. Comment Subject: Section 79901(r) Workforce
Commenter(s): SH
Comment: "The issue with the aforementioned definition is that it makes health care facilities responsible for unscrupulous employees, medical staff, and other individuals whose actions are outside the scope of their employment or beyond the boundaries of the relationship. Healthcare facilities should not be responsible for the actions of employees, medical staff, volunteers, or other individuals if such actions are intentional, malicious, and/or outside the reasonable parameters of an employer-employee relationship. Accordingly, Sutter would recommend the deletion of both "business associate" and "whether or not they are paid by the health care facility or business associate" within the definition."

Department Response: The Department rejects the proposed deletions as they would fundamentally undermine the overarching purpose of the regulations to ensure health

care facility's workforce, including business associates, is held responsible for the protection of patient information. Under the doctrine of non-delegable duties, health facilities 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. The Department considered these deletions but doing so would so weaken this regulatory program as to make in ineffective. If adopted, such deletions would also relieve health care facilitates of non-delegable duties.

10. Comment Subject: Administrative Procedures Act: Authority
Commenter(s): CHA
Comment: "The proposed regulations do not comply with the "authority" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq., as they permit CDPH to cite and fine health facilities for breaches beyond those allowed by the authorizing statute.

As mentioned in previous comments, CHA has been greatly concerned that CDPH has issued fines against California hospitals for privacy breaches when there was no finding by CDPH that the hospital failed to implement (or inadequately implemented) an administrative, physical, or technical safeguard. This is contrary to the express language of the relevant statutes and the intent of the Legislature.

Specifically, Health and Safety Code Section 1280.18(a) requires 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." "Administrative safeguards," "physical safeguards," and "technical safeguards" are defined in HIPAA.[1] Examples of these safeguards include conducting a risk analysis, implementing access controls and validation procedures, and instituting automatic log-offs, respectively. A complete list of all 18 administrative, physical, and technical safeguards as well as their 33 component requirements may be found here.

Health and Safety Code Section 1280.15(a) refers to these safeguards when setting forth a health facility's responsibilities with respect to privacy breaches. Specifically, Section 1280.15(a) states that:

A clinic, health facility, home health agency, or hospice licensed pursuant to Section 1204, 1250, 1725, or 1745 shall prevent unlawful or unauthorized access to, and use or

[1] 45 C.F.R. Sections 164.308, 164.310, and 164.312, respectively.

disclosure of, patients' medical information, as defined in subdivision (g) of Section 56.05 of the Civil Code *and consistent with Section 1280.18… (emphasis added)*

Notably, this statute does *not* require health facilities to prevent *all* unlawful or unauthorized access to patients' medical records. It instead requires health facilities to implement reasonable safeguards to prevent unlawful and unauthorized access. The stakeholders involved in developing the legislation that enacted the authorizing statutes understood that a health facility could take all reasonable steps to prevent breaches, but still be victimized by a rogue employee or a criminal hacker. The stakeholders negotiated a legislative package that incentivized hospitals to strengthen their privacy safeguards and gave CDPH the ability to investigate and fine hospitals that failed to do so. The Legislature adopted language requiring health facilities to "*reasonably* safeguard"[2] confidential medical information and specified that a health facility is not to be held responsible for breaches due to "factors outside its control."[3] These words evidence the Legislature's intent that a health facility should be fined only for a breach *when the facility itself has done something wrong* – that is, the facility has been negligent in some way.

In fact, these precise circumstances were discussed at length during negotiations on Senate Bill (SB) 541 (Stats. 2008, c. 605) and Assembly Bill (AB) 211 (Stats. 2008, c. 602) (the authorizing statutes for these proposed regulations). As you may know, the impetus for SB 541 was a California hospital employee who gave health information about celebrities to her husband, who sold it to the *National Enquirer*. The purpose of SB 541 and AB 211 was twofold: (1) to require clinics, health facilities, home health agencies and hospices to improve their privacy and security practices and (2) to authorize the state to enforce appropriate "administrative, technical, and physical safeguards" as stated in Health and Safety Code Section 1280.18 against facilities and individuals.

The parties to the SB 541 and AB 211 discussions (legislators and their staff, Governor's administration staff, CDPH staff, and various interest groups) understood and agreed that laws do not prevent all bad things. For example, the stakeholders noted that murder is illegal, but it still happens. The stakeholders agreed that facilities should be held responsible for training employees and implementing appropriate administrative, physical, and technical safeguards — but they would not be responsible if a breach happened in spite of all this work. Instead, individual wrongdoers (often criminals) would be held responsible for their bad deeds — rather than the clinic, health facility, home health agency, or hospice that implemented appropriate safeguards. This is the meaning behind the language in the law requiring the enforcement agency to

[2] Health and Safety Code Section 1280.15(a) (emphasis added).
[3] Health and Safety Code Sections 1280.15(a) and 1280.18(b).

"consider… factors beyond the provider's immediate control that restricted the facility's ability to comply." This is also why the enforcement agency (now CDPH) was given the authority to take action against individuals.

During the bill negotiations, the Governor's administration and CDPH staff assured legislators, CHA, and other stakeholders that the Health and Safety Code Section 1280.15 language highlighted below meant that the statute does not constitute a strict liability statute (that is, the facility is strictly liable even if it did nothing wrong). Instead, the health care facility must be found by CDPH to have been negligent and failed to properly implement an appropriate administrative, technical, or physical safeguard in order to be fined. In other words, in cases involving a facility with a "rogue" employee, CDPH would not fine the facility; instead, it would refer the matter to the California Office of Health Information Integrity (Cal-OHII) to act against the individual. (The authority to act against the individual was transferred from Cal-OHII to CDPH in June 2014.)

Health and Safety Code Section 1280.15. (a) A clinic, health facility, home health agency, or hospice licensed pursuant to Section 1204, 1250, 1725, or 1745 shall prevent unlawful or unauthorized access to, and use or disclosure of, patients' medical information, as defined in subdivision (g) of Section 56.05 of the Civil Code and consistent with Section 1280.18 …

Health and Safety Code Section 1280.18. (a) 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.

(b) In exercising its duties pursuant to this division, the office shall consider the provider's capability, complexity, size, and history of compliance with this section and other related state and federal statutes and regulations, the extent to which the provider detected violations and took steps to immediately correct and prevent past violations from reoccurring, and factors beyond the provider's immediate control that restricted the facility's ability to comply with this section.

(c) The department may conduct joint investigations of individuals and health facilities for violations of this section and Section 1280.15, respectively.

The fact that SB 541 created a negligence standard rather than a strict liability standard was not a minor or peripheral issue. It was a major issue and was thoroughly discussed by all involved legislators and stakeholders. I was present at and participated in all major legislator/stakeholder negotiation meetings on SB 541 and AB 211 in 2008. CHA eventually took a "neutral" position on SB 541 because of CDPH's assurances that the law would be interpreted to impose fines on health care facilities only if they failed to implement an appropriate administrative, technical, or physical safeguard. CHA took a

"support" position on AB 211, because we agreed that facilities should implement appropriate safeguards and that individual wrongdoers should be held accountable if they deliberately commit a breach.

I have attached contemporaneous corroboration of this interpretation of the meaning of the language that is highlighted on page 1 — see email message from Jennifer Kent of Governor Schwarzenegger's office to Margaret Pena (Senate), Connie Delgado (CHA), and Monica Wagoner (CDPH) dated August 21, 2008. Jennifer is responding to Connie's question about why the language in Health and Safety Code Section 1280.15 (in SB 541) was not amended to clarify that it constitutes a "reasonable standard" rather than a "strict liability" standard, as all parties to the negotiations on the bill package had agreed. Jennifer responded that Health and Safety Code Section 1280.15 did not need to be amended to achieve this goal, because it references the "reasonable standard" in AB 211 (Health and Safety Code Section 130203, since remodified to Health and Safety Code Section 1280.18). Jennifer states, "SB 541 [H&S 1280.15] references the section in AB 211 that makes it a reasonable standard — 'consistent with Section 130203 [now H&S 1280.18]' — so we didn't need to change it because we changed it in the other bill."

When interpreting a statute, "[a] construction making some words surplusage is to be avoided. The words of the statute must be construed in context, keeping in mind the statutory purpose. In addition, statutes or statutory sections relating to the same subject must be harmonized, both internally and with each other, to the extent possible." (*The Regents of the University of California v. Superior Court (Melinda Platter real party in interest)*, 220 Cal.App.4th 549 (2013)). The words found in Health and Safety Code Section 1280.15 — "consistent with Section 130203 [now Health and Safety Code Section 1280.18]"— must be given meaning. The email of August 21, 2008 provides the correct interpretation. This meaning must be incorporated into CDPH's regulations.

As mentioned above, the proposed regulation does not comply with the "authority" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq., as it permits CDPH to cite and fine health facilities for breaches beyond those described by the authorizing statute.

Department Response: The Department does not lack authority to promulgate regulations. In their assessment of the Department's actions, the commenter has misstated the law. This statute contains a strict liability standard, not a lesser standard that allows facilities to avoid liability for the actions of their agents. These rules are built on the idea that health care facilities are responsible for the actions of their agents when those agents do not meet the legal obligations to protect patient information. Health care facilities cannot delegate the duty to protect patient information.

The plain language of the controlling statute demonstrates that this is a strict liability statute. Specifically, it reads in part, that a health 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." (Health & Saf. Code § 1280.15.) By including the words, "shall prevent," the legislature sought to impose strict liability upon health facilities if a breach of patients' medical information occurs. When interpreting a statute, courts are obligated "to give significance and effect to each word and phrase and to avoid a construction that makes any part of the statute superfluous or meaningless." (Shaw v. People ex rel. Chiang, 175 Cal.App.4th 577, 600 (2009) (citations omitted); see also Corley v. United States, 556 U.S. 303, 315 (2009) (emphasizing, "one of the most basic interpretive canons, that a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant").) The plain language of this statute directs the Department to impose a penalty when there is a medical information breach.

Furthermore, a court must ascertain the intent of the Legislature in order to "effectuate the purpose of the law." (Alexander v. Superior Court, 5 Cal.4th1218, 1226 (1993). As noted in the above section, the legislative intent is clear in its direction that a penalty must be imposed in order to curb continued breaches. The statutory reference to section 1280.18 is for purposes of identifying a factor in deciding the penalty assessment the Department may issue when a violation occurs. This is the plain language reading section 1280.15 which gives the Department discretionary authority in determining the appropriate penalty amounts, if any, that may be assessed. One of the factors to consider is whether a health care facility has complied with related statutes and regulations to determine the appropriate penalty amount. Section 1280.18 requires a facility to (1) establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information; and (2) to reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use, or disclosure. It does not indicate that a facility would be further relieved of wrongdoing by simply demonstrating these safeguards.

The commenter ignores the plain language of the statute as well as the legislature's intent to hold facilities responsible for their failures to prevent breaches. It is reasonable to infer that the legislature intended the Department to specifically determine whether the facility violated these requirements before determining a penalty amount.

11. Comment Subject: Administrative Procedures Act: Authority
Commenter(s): CHA
Comment: The proposed regulations make health facilities responsible for the actions of third parties — business associates and medical staff members. However, this does not comply with the "authority" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq. The authorizing statutes do not address business associates or medical staff members, nor do they say or imply that health facilities should be responsible for the actions of other entities. On the contrary, the Legislature explicitly stated that a health facility should *not* be responsible for "factors

outside its control"[4] and gave CDPH the legal authority to take enforcement actions directly against business associates, medical staff members, and any other entity or individual responsible for a privacy breach.[5] Therefore, the proposed regulations must be amended to delete the term "business associate" in the definitions of "detect," "factors outside the control of the health care facility," and "workforce," and to delete "medical staff" from the definition of "health care facility."

It does make sense to include "business associates" and "medical staff" in the definition of "health care system," a term that is designed to include various health facility partners in caring for patients. It does not make sense to include them in the definition of the "health care facility" itself. CHA recommends that CDPH make this revision.

Department Response: The Department rejects this comment because the Department has the "authority" to promulgate these regulations and the commenter misstates the law. This statute contains a strict liability standard, not a lesser standard that allows facilities to avoid liability for the actions of their agents. The commenter misstates the law in asserting that "a health facility should not be responsible for "factors outside its control"; instead, the statute requires the Department to "*consider*…factors outside [the facility's]…control that restricted the facility's ability to comply with this section" in "determining whether to investigate an incident, and the amount of an administrative penalty, if any…" (Health and Safety Code section 1280.15, emphasis added.)These rules are built on the idea that health care facilities are responsible for the actions of their agents when those agents do not meet the legal obligations to protect patient information. Health care facilities cannot delegate this duty to protect patient information.

12. Comment Subject: Section 79901(a) Access
Commenter(s): CHA, HSLAC
Comment: "This definition should be revised to clarify that "access" means that someone read, wrote, modified, or communicated data/information, not just that a person had the ability or means necessary to do so. **The proposed definition does not comply with the "consistency" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq., as it violates the holding of Sutter Health et al. v. Superior Court of Sacramento County (Atkins et al. real parties in interest), 227 Cal.App.4th 1546 (July 21, 2014).** In that case, a thief stole a

[4] Health and Safety Code Sections 1280.15(a) and 1280.18(b).
[5] Health and Safety Code Section 1280.17 states, "The department may assess an administrative fine against any person or any provider of health care, whether licensed or unlicensed, for any violation of Section 1280.18 of this code or Part 2.6 (commencing with Section 56) of Division 1 of the Civil Code in an amount as provided in Section 56.36 of the Civil Code."

hospital's computer that contained medical records. The court concluded that there was no breach because the medical information "was not actually viewed by an unauthorized person." The court went on to state that "[t]he mere possession of the medical information or records by an unauthorized person was insufficient to establish breach of confidentiality if the unauthorized person has not viewed the information or records."

This regulation should consider a person to have "accessed" medical information only if the person has read, wrote, modified, or communicated it. To illustrate the problem with this definition, consider the system administrator of a hospital's electronic health records system. The system administrator can read any medical record in the system. However, the system administrator should be considered to have accessed a record only if she read a medical record that she had no legitimate purpose for reading.

In addition, the phrase "otherwise use any system resource" is completely unclear. **This phrase should be explained or deleted, as it does not comply with the "clarity" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq.**

We suggest revising Section 77901(a) to read as follows: "Access means reading, writing, modifying, or communicating data/information."

Department Response: The Department rejects this proposed amendment because the current definition of "Access" is based upon the definition found in The Health Insurance Portability and Accountability Act (HIPAA) in an effort to promote uniformity between state and federal law and to simplify compliance for the regulated community. As the Department desires consistency between federal regulations and state regulations the Department, after considering the proposed definition that does not conform with HIPAA, has decided to retain the current definition.

In addition, the Department believes this definition meets the "clarity" standard of the Administrative Procedure Act as the Department's definition is consistent with current case law.

The case referenced in the proposed amendment relates to patients seeking damages for the negligent release of their own medical information as afforded by the private right of action in the Confidentiality of Medical Information Act (CMIA) under Civil Code section 56 et seq. Sutter Health et al. v. Superior Court of Sacramento County (Atkins et al. real parties in interest), 227 Cal.App.4th 1546 (July 21, 2014). The court found that " section 56.1010, subdivision (a) makes it clear that *preserving the confidentiality* of the medical information, not necessarily preventing others from gaining possession of the paper-based or electronic information itself, is the focus of the legislation. *Id*. at 1556. Therefore, if the confidentiality is not breached, the statute is not violated."

The court interprets a breach of medical information within the context of a specific provision in the CMIA and the standard by which confidentiality is breached hinges on the preservation of confidentiality. In contrast, the Health and Safety code section 1280.15 requires a duty to *prevent* unlawful or unauthorized access to, and use or disclosure of medical information [emphasis added]. The standards between the two statutes vastly differ from one another. Additionally, unlike Civil Code section 56.36, the Health and Safety Code does not contain a parallel requirement that the Department prove an injury and damages in order to investigate and assess a penalty for unauthorized or unlawful access to medical information. Further, SB 541 established Health and Safety Code section 1280.15 in part because the CMIA was found inadequate in addressing unauthorized access to medical information, "access events" or "snooping" into patient medical records. Therefore, the applicability of any case law interpreting the CMIA would not correspond to the standard for establishing a breach pursuant to Section 1280.15.

Therefore, the current definition of "access" is consistent with the Department's separate enforcement of unauthorized or unlawful access to medical information pursuant to Health and Safety Code section 1280.15.

13. Comment Subject: Section 77901(b)(1)(A) Breach
Commenter(s): CHA
Comment: "This paragraph omits web-based communications. We suggest using the term "electronic communication" instead of "electronic mail or facsimile transmission," or, alternatively, adding in the term "electronic communication."

Department Response: The Department rejects this proposed amendment because the proposed changed would conflict with the plain language of the underlying statute, Health and Safety Code Section 1280.15, which uses the language, "Any paper record, electronic mail, or facsimile transmission". The Department considered the proposed amendment which would substantially increase the scope of what is excluded from the definition of a breach beyond what is described in the statute and rejected the revised definition. In order to maintain consistency between the statutes and regulations clarifying those statutes, the Department rejects the revised definition.

14. Comment Subject: Section 77901(b)(1)(B) Breach
Commenter(s): CHA
Comment: This paragraph omits web-based communications. We suggest using the term "electronic communication" instead of "electronic mail or facsimile transmission," or, alternatively, adding in the term "electronic communication." In addition, the term "business associate" should be included after "covered entity." Covered entities and business associates are both required to comply with HIPAA, must maintain the confidentiality of medical information in the same manner, and are subject to the same HIPAA penalties for noncompliance.

Department Response: The Department rejects this proposed amendment because the proposed changed would conflict with the plain language of the underlying statute, Health and Safety Code Section 1280.15, which uses that language "Any paper record, electronic mail, or facsimile transmission". The Department considered the proposed amendment which would substantially increase the scope of what is excluded from the definition of a breach beyond what is described in the statute and rejected the revised definition. In order to maintain consistency between the statutes and regulations clarifying those statutes, the Department rejects the revised definition. The Department also considered and rejected the addition of "business associate" to this section because it would also depart from the definition of Health and Safety Code Section 1280.15.

15. Comment Subject: Section 77901(b)(1)(E) Breach
Commenter(s): CHA
Comment: "The phrase "Any 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 shall be presumed a breach unless it is excluded by section 79901(b)(1)(F)" should be deleted. **The inclusion of this phrase does not comply with the "consistency" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq., as it directly violates the holding of *Sutter Health et al. v. Superior Court of Sacramento County (Atkins et al. real parties in interest),* 227 Cal.App.4th 1546 (July 21, 2014).** In that case, a thief stole a hospital's computer that contained medical records. The court concluded that there was no breach because the medical information "was not actually viewed by an unauthorized person." The court went on to state that "[t]he mere possession of the medical information or records by an unauthorized person was insufficient to establish breach of confidentiality if the unauthorized person has not viewed the information or records."

In addition, paragraphs 79901(b)(1)(C), (E), and (F) should be revised to be consistent with paragraphs (A) and (B). Paragraphs (A) and (B) use the phrase "same health care facility or health care system," whereas (C), (E), and (F) use the phrase "health care facility or business associate." The phrase "health care facility or health care system" properly recognizes the relationship between health facilities, business associates, and medical staff members. However, making this change requires also making the change described under the header "**Business Associates and Medical Staff,"** above – moving business associates and medical staff out of the definition of "health care facility" and into the definition of "health care system."

Department Response: The Department rejects this proposed amendment because the current definition of "Breach" is based upon the definition found in The Health Insurance Portability and Accountability Act (HIPAA) in an effort to promote uniformity between state and federal law and to simplify compliance for the regulated community. As the Department desires consistency between federal regulations and state

regulations the Department, after considering the proposed definition that does not conform with HIPAA, has decided to retain the current definition.

In addition, the Department believes this definition meets the "clarity" standard of the Administrative Procedure Act as the Department's definition is consistent with current case law. The case referenced in the proposed amendment relates to patients seeking damages for the negligent release of their own medical information as afforded by the private right of action in the Confidentiality of Medical Information Act (CMIA) under Civil Code section 56 et seq. Sutter Health et al. v. Superior Court of Sacramento County (Atkins et al. real parties in interest), 227 Cal.App.4th 1546 (July 21, 2014). The court found that " section 56.1010, subdivision (a) makes it clear that *preserving the confidentiality* of the medical information, not necessarily preventing others from gaining possession of the paper-based or electronic information itself, is the focus of the legislation. *Id*. at 1556. Therefore, if the confidentiality is not breached, the statute is not violated."

The court interprets a breach of medical information within the context of a specific provision in the CMIA and the standard by which a confidentiality is breached hinges on the preservation of confidentiality. In contrast, Health and Safety code section 1280.15 requires a duty to *prevent* unlawful or unauthorized access to, and use or disclosure of medical information [emphasis added]. The standards of the two statutes vastly differ from one another. Additionally, unlike Civil Code section 56.36, the Health and Safety Code does not contain a parallel requirement that the Department prove an injury and damages in order to investigate and assess a penalty for unauthorized or unlawful access to medical information. Further, SB 541 established Health and Safety Code section 1280.15 in part because the CMIA was found inadequate in addressing unauthorized access to medical information, "access events" or "snooping" into patient medical records. Therefore, the applicability of any case law interpreting the CMIA would not correspond to the standard for establishing a breach pursuant to Section 1280.15.

Therefore, the current definition of "access" is consistent with the Department's separate enforcement of unauthorized or unlawful access to medical information pursuant to Health and Safety Code section 1280.15.

16. Comment Subject: Section 77901(c) Business Associate
Commenter(s): CHA
Comment: "As mentioned earlier in this letter, CHA believes that making health facilities responsible for business associates exceeds CDPH's statutory authority. In addition, we note that Paragraphs (1) and (2) of this definition are very similar to the HIPAA definition of the term "business associate," but are not identical. Reading the proposed definition and the HIPAA definition side by side, it is not apparent if the differences in the language are intentional and signify something, or are unintentional. If the concept of business associates is retained in this regulation, CHA suggests making

the definitions identical (except for substituting the state term “medical information” for the federal term “protected health information”).**”**

Department Response: The Department rejects the proposed deletions as they would fundamentally undermine the overarching purpose of the regulations to ensure the health care facility’s agents, including business associates, are responsible for the protection of patient information. Under the doctrine of non-delegable duties, health facilities are responsible for the actions of their workforce and their business associates. Interpreting the statute to include workforce member and business associate 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. The Department considered these deletions but doing so would so weaken this regulatory program as to make it ineffective. If adopted, such deletions would relieve health care facilitates of non-delegable duties.

17. Comment Subject: Section 79901(f) Detect
Commenter(s): CHA, HSLAC
Comment: “This provision requires a health facility to report a “reasonable belief that a breach occurred” within 15 days of the time that a health care facility, business associate, or agent, “by exercising reasonable diligence would have known” that a breach occurred. **This provision does not comply with the “authority” standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq.** First, the authorizing statute, Health and Safety Code Section 1280.15, does not require reporting of security incidents (which are defined in 45 C.F.R. Section 164.304) – it requires reporting only of actual breaches. This was a deliberate policy decision by the Legislature. Second, the authorizing statute does not require reporting when a health facility “should have known” something happened. The statute requires reporting only when the health facility knows of a breach – that is, it has actual knowledge. Third, the statute does not address business associates at all – the California Legislature did not give CDPH the statutory authority to regulate a group of individuals/entities called “business associates.” Finally, the term “agent” is not defined and lacks the clarity required by the Administrative Procedure Act. CHA recommends that this definition be revised to read as follows:

“Detect” means the discovery of a breach by a health care facility. A breach shall be treated as detected as of the first business day on which such breach is known to the health care facility. A health care facility shall be deemed to have knowledge of a breach if such a breach is known to any person who is a workforce member, other than the person committing the breach.”

Department Response: The Department rejects these proposed amendments as the current language mirrors the construction of HIPAA and effectuates the purposes of Health and Safety Code Section 1280.15. 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 considered these proposed amendments but rejected them as an important element of this definition is the requirement that health care facilities report not only when there is a certainty of breach but also when there is reasonable certainty a breach may have occurred, and these amendments prevented that important policy objective.

In addition, The Department deliberately included business associates in this definition to further important public policy goals. The Department's purpose for including business associates is that the parties enter 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. Thus, it is critical to include business associates in these regulations to protect patient information.

18. Comment Subject: Section 79901(i) Factors outside the control of the health care facility
Commenter(s): CHA, HSLAC
Comment: "The proposed regulation purports to restrict CDPH's consideration of exculpatory factors in a manner not permitted by the authorizing statutes. **This limitation does not comply with the "authority" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq.** Specifically, the Legislature directed CDPH to consider *all* factors outside the health care facility's control. As described earlier in this letter, this language was specifically intended by the Legislature to include "rogue employees" who had been properly trained in privacy laws and policies, and were working at a facility that implemented appropriate administrative, physical and technical safeguards, but deliberately disregarded all this and committed a breach of patient medical information anyway (see discussion under heading of "Standard for Assessing a Fine Against a Health Facility" on page 1). The statute's reference to "factors outside [the facility's] control" was also intended to include thieves and other criminals. We suggest revising this definition as follows:

"Factors outside the control of the health care facility" means any circumstance not within the reasonable control of the health care facility, including, but not limited to, fires, explosions, natural disasters, severe weather events, war, invasion, civil unrest, acts or threats of terrorism, ~~and~~ utility or infrastructure ~~failure. "Factors outside the control of~~

~~the "health care facility" does not include the acts of the health care facility, business associate, or their respective workforce members."~~failure, acts of workforce members in violation of employer policy, acts of business associates in violation of their business associate contracts, and acts of criminals."

Department Response: The Department rejects this proposed amendment. This definition is intended to capture events that are truly outside the control of a health care facility. Health facilities, under the doctrine of non-delegable duties, are responsible for the actions of their workforce members, agents, and 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. The Department considered these proposed amendments, but they go against the purpose of this definition and would violate the doctrine of non-delegable duties as found in California case law.

19. Comment Subject: Section 77901(j) Health care facility
Commenter(s): CHA, HSLAC
Comment: "As discussed previously in this letter, the term "health care facility" should not include the terms "business associate" or "medical staff," as this **does not comply with the "authority" or "consistency" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq.** California law prohibits hospitals (with limited exceptions) from employing physicians or influencing their professional activities.[6] The California Legislature has enacted these laws to protect the professional independence of physicians, and to avoid having physicians' loyalty divided between an employer (the hospital) and the patient. These laws seek to prevent hospitals from exercising control over physicians and how they practice medicine, and to prohibit hospitals from interfering in the physician/patient relationship. The proposed regulations are inconsistent with California's prohibition on the corporate practice of medicine, and exceed the statutory authority granted by the Legislature.

CDPH has been given the authority by the Legislature to enforce medical privacy laws directly against individuals (such as business associates and medical staff members) in Health and Safety Code Section 1280.17 ("The department may assess an administrative fine against any person or any provider of health care, whether licensed or unlicensed, for any violation of Section 1280.18 of this code or Part 2.6 (commencing with Section 56) of Division 1 of the Civil Code in an amount as provided in Section

[6] Business and Professions Code Section 2400 et seq., which codifies the ban on the corporate practice of medicine.

56.36 of the Civil Code"). This is how the Legislature intended CDPH to enforce medical privacy laws against third parties — not indirectly by making hospitals liable for their actions. Thus, we urge that the proposed regulation be revised to delete the terms "business associate" and "medical staff."

Department Response: The Department rejects the proposed deletions as they would fundamentally undermine the overarching purpose of the regulations to ensure health care facility's workforce, including business associates, is held responsible for the protection of patient information. 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. The Department considered these deletions but doing so would so weaken this regulatory program as to make in ineffective. If adopted, such deletions would also relieve health care facilitates of non-delegable duties. These regulations meet both the authority and consistency standards established by the Administrative Procedures Act as they are in conformance with the underlying statue Health and Safety Code Section 1280.15 and the existing case law on responsibilities of heath care facility for actions of their workforce.

20. Comment Subject: Section 79901(k) Health care system
Commenter(s): CHA
Comment: "CHA recommends adding the terms "business associate" and "medical staff" to the definition of "health care system." It makes sense for the larger concept of "system" to include these individuals. Making this revision and revising Sections 79901(b)(1)(C), (E), and (F) would properly recognize the relationship between health facilities, business associates, and medical staff members."

Department Response: The Department rejects these proposed additions to this definition. This definition, in its current form, developed in consultation with the California Hospital Association, is sufficient to include all necessary elements of a health care system. As currently drafted this definition includes: 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 proposed additions of "medical staff" and "business associate" would be duplicative of existing statute and is rejected as these terms are already included in the definition of health care facility.

21. Comment Subject: Section 77901(l) Medical information
Commenter(s): CHA
Comment: "This definition is fine as far as it goes. However, it may be confusing because the term "contractor" as used in Civil Code Section 56.05 (and thus in this

regulation) has an unusual definition that would not be understood by persons reading the regulation alone. As used in Civil Code Section 56.05(d), "Contractor" means:

[A]ny person or entity that is a medical group, independent practice association, pharmaceutical benefits manager, or a medical service organization and is not a health care service plan or provider of health care. "Contractor" does not include insurance institutions as defined in subdivision (k) of Section 791.02 of the Insurance Code or pharmaceutical benefits managers licensed pursuant to the Knox-Keene Health Care Service Plan Act of 1975 (Chapter 2.2 (commencing with Section 1340) of Division 2 of the Health and Safety Code).

CHA suggests including the definition of "contractor" in the regulations, or simply referring to Civil Code Section 56.05 without also copying it in the regulations."

Department Response: The Department agreed with the comment made by CHA and has adopted their proposed amendments. The Department has clarified the definition of the term "contractor" used in the definition of "medical information". The definition of "medical information" is identical to Civil Code section 56.05 (j). This provision has a unique definition of the term "contractor" found in Civil Code section 56.05(d). By incorporating, the definition of "contractor" found in Civil Code section 56.05(d) this will increase clarity and ensure the completeness of the definition of "medical information".

22. Comment Subject: Section 79901(m) Medical staff
Commenter(s): CHA, HSLAC
Comment: "It is unclear to CHA whether CDPH really intends for the definition of "medical staff" to mean only those medical providers who have entered into a contract with the health care facility. We wonder whether CDPH is under the impression that all providers on a health facility's medical staff are "contracted," which is not the case.

Under California law, a medical staff member is a physician, dentist, podiatrist, or clinical psychologist who has been appointed to the medical staff by the hospital's governing body.[7] Most of these professionals have not entered into a contract with the hospital. Typically, a hospital contracts with physicians to provide emergency, radiology, anesthesiology, and pathology services. Hospitals may also contract with physicians to provide hospitalist or medical director services. However, most physicians on a hospital's medical staff — such as cardiologists, surgeons, obstetricians, etc. — do not enter into a contract with the hospital. These physicians are independent practitioners who have met the hospitals' criteria for admission to the medical staff and agree to

[7] Title 22, California Code of Regulations, Section 70701.

comply with the Medical Staff Bylaws and Rules and Regulations. California courts have ruled[8] that these bylaws do not constitute a contract.

Also, it is unclear what is meant by the phrase "on behalf of a health care facility" in the proposed definition. Under California law, medical staff members provide services directly to their patients. The physician decides which hospital to admit the patient to, when to visit the patient in the hospital, which services to provide to the patient, and bills the patient for services rendered. The physician is not providing services "on behalf of" the hospital. Physician services are very different from hospital services (which are generally provided by nurses, physical therapists, respiratory therapists, etc.).

If CDPH intends for "medical staff" to mean all physicians, dentists, podiatrists, and clinical psychologists who have been appointed to a hospital's medical staff, then CHA recommends omitting this definition altogether. The term "medical staff" is clear under existing law. On the other hand, if CDPH intends for this term to mean "licensed medical providers contracted to provide services on behalf of a health care facility," then CHA recommends that CDPH also define "licensed medical providers." For example, does this mean only physicians, or all providers licensed under Division 2 of the Business and Professions Code (which includes nurses, pharmacists, midwives, marriage and family therapists, licensed clinical social workers, and the full gamut of health care professionals)? Furthermore, if CDPH intends "medical staff" to mean only a subset of the physicians practicing in the hospital, CHA also recommends that CDPH define "on behalf of a health care facility" so we can understand which practitioners are included in the definition.

In addition, the Legislature has not granted CDPH the authority to make hospitals or other health facilities liable for the actions of physicians' employees or agents. The proposed regulations assign liability to the hospital for physicians' employees and agents — even if those individuals work in the physician's office or in a completely separate business and have no relationship whatsoever with the hospital. The hospital has no way of controlling these individuals.[9] Indeed, the hospital has no way of even knowing who these individuals are, let alone training, monitoring, or disciplining them. These individuals might include the doctor's office staff — nurses, receptionists, billing clerks, janitors, medical records clerks, etc. — who never step foot into the hospital. Including medical staff employees and agents in this definition **does not comply with the "authority" standard of the Administrative Procedure Act.** If the California

---

[8] *O'Byrne v. Santa Monica-UCLA Med. Ctr.*, 94 Cal. App. 4th 797 (2001).

[9] As already mentioned, the hospital does not contract with most physicians on the medical staff, and thus cannot control medical staff employees or agents via a contract with the physician.

Legislature had wanted health facilities to be responsible for the actions of individuals they had never encountered, the Legislature could have said so. It did not. On the contrary, as mentioned previously in this letter, the Legislature explicitly stated that a health facility should *not* be responsible for "factors outside its control"[10] and gave CDPH the legal authority to take enforcement actions directly against business associates, medical staff members, and any other entity or individual responsible for a privacy breach.[11]"

Department Response: The Department partially agrees with this substance of this comment and the Department has revised the definition of the term "medical staff". The Department has adopted the same definition of "medical staff" as found in the regulations governing medical staff in General Acute Care Hospitals (GACH) in in 22 CCR 70703(a)(1). This definition will increase clarity as to which individuals this definition applies and ensure medical providers who are practicing in a health facility will be subject to these regulations.

23. Comment Subject: Section 79902(a)(1)(K) Required Elements --
Commenter(s): DH
Comment: "The proposed regulations continue to include an expanded list of required elements that must be in a facility's report to the Department. A number of the items are new. Among them at Section 79902(a)(1) is subsection K: "any other instances of a reported event that includes a breach of that patient's medical information by the health care facility." This new requirement will impose extremely costly burdens on facilities for little or no benefit to patients.

Like most hospitals, Dignity Health's hospital compliance events (including potential breach events) are documented in a computer application that is not connected with the patient electronic record. Each privacy event investigation is separately documented in a secure system, including a listing (usually in the form of an excel spreadsheet) of all the names and addresses of the affected patients. In a large hospital, over the course of several years there will be many such events and documents.

The hospital's accounting of disclosures process will often (perhaps usually) not be of help with this new required element. While the HIPAA Privacy Rule contains a patient

---

[10] Health and Safety Code Sections 1280.15(a) and 1280.18(b).

[11] Health and Safety Code Section 1280.17 states, "The department may assess an administrative fine against any person or any provider of health care, whether licensed or unlicensed, for any violation of Section 1280.18 of this code or Part 2.6 (commencing with Section 56) of Division 1 of the Civil Code in an amount as provided in Section 56.36 of the Civil Code."

right to an accounting of disclosure, Dignity Health (like all other covered entities) receives extremely few such requests. The Privacy Rule does not require that a hospital maintain a running list of all disclosures in order to provide an accounting to a patient; many hospitals will compile an accounting of disclosures only if and when a patient asks for such a list. This means that many (and probably most) hospitals will not have one place in which to look to find out if a particular patient has been included in a past breach event.

In such circumstances, identifying all prior breaches for a patient requires looking through literally every single privacy event at the facility, checking on every name. Obviously, that would be an extremely labor intensive and costly process. The process would be analogous to what one could imagine CDPH would have to go through if it were required to determine from its own records of breaches if a specific patient had ever before been a victim of a prior breach.

The burden of the requirement is truly overwhelming, and it is hard to see any, much less commensurate, benefit for patients. Patients will have already known about all other prior events involving their information, having already received written notice of those events. There is no statutory mandate to provide this information to the Department, and it is unclear what use the Department will make of the information. Given the problems identified here, **Dignity Health very strongly urges the Department to eliminate Subsection K of Section 79902(a)(1) because it imposes severe burdens on health care facilities without any perceptible benefit."**

Department Response: The Department reject this proposed deletion as this requirement does not impose severe burdens on health care facilities without any perceptible benefits and helps the Department in the completion of its work. Health care facilities must already collect and store this information as part of the facility's obligations under HIPAA, 45 C.F.R. § 164.316 (b). In addition, this information is useful to the Department in the calculation of penalties as compliance history is a factor in setting penalty amounts. The Department in considering this deletion perceives no benefit to facilities if these obligations were reduced and the impediment in the critical work of calculating penalties.

24. Comment Subject: Section 77901(j) Health care facility
Commenter(s): DH
Comment: "In the prior iteration of the regulations, CDPH defined the term "workforce" to include "the medical staff and the medical staff's employees." In its prior comments, Dignity Health pointed out that under California's prohibition on the corporate practice of medicine, hospitals were prohibited from employing or otherwise controlling the work of physicians who have medical staff privileges, and strongly urged CDPH to remove medical staff and their employees from the definition of "workforce."

CDPH did so, but has now transferred the medical staff and their employees to the definition of "health care facility." This change continues CDPH's efforts to impose

responsibilities and possible enforcement penalties on hospitals and other health facilities that are prohibited by law from exercising control over the physicians on their staffs.

In California, the medical staff of a hospital is a self-governing association, and is decidedly NOT under the direct control of the hospital. All physicians on the medical staff are each separate providers of health care (see California Civil Code section 56.05(j)) and covered entities, obligated under both state and federal law to comply with state and federal privacy obligations as separate providers of health care from the hospital.

Expansion of a hospital's liability to the actions of medical staff members, and especially to the medical staff members' employees could be seen as an unwarranted effort of CDPH to regulate those entities that are not within the scope of its statutory authority, limited as it is to specific licensed health care facilities. **Dignity Health strongly urges the Department to eliminate the medical staff and the employees of each medical staff physician from the definition of health care facility, and to enforce the privacy obligations of physician providers of health care in the other ways that are available to the Department.**

Department Response: The Department rejects the proposed deletions as they would fundamentally undermine the overarching purpose of the regulations to ensure health care facility's workforce, including business associates, is held responsible for the protection of patient information. Under the doctrine of non-delegable duties, health facilities 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. The Department considered these deletions but doing so would so weaken this regulatory program as to make in ineffective. If adopted, such deletions would also relieve health care facilitates of non-delegable duties.

In addition, the Department does not believe that the practice of medicine includes the violation patient confidentiality or failure to protect patient information and as such, issues related to the corporate practice of medicine are not implicated by the regulations.

25. Comment Subject: Sections 79902(a) and (a)(1) Breach Reporting Requirements
Commenter(s): PSJH, HSLAC
Comment: Because health facilities are required to report breaches to CDPH within 15 days, much of the information in the list of information to be reported will not yet be available. CDPH should amend Section 79902(a) and (a)(1) as follows:

(a)"A health care facility, excluding a business associate, shall report to the Department a breach of a patient's medical information, or a breach reasonably believed to have occurred, no later than ~~15~~30business days after the breach has been detected."

(a)(1) "In its reporting of a breach, the health care facility shall provide the Department, in writing and signed by a representative of the health care facility, the following to the extent known…"

Department Response: The Department partially rejects the amendments suggested by this comment and partial accepts them. The Department rejects the suggestion that the time to report a breach should be extended to 30 days as this doubles the amount of time before patients can be notified and mitigation measures can be taken. The department has partially adopted the amendment by adding the qualifier "to the extent known" to this provision. The Department recognizes that health facilities may not always know all the details of a medical information breach when reporting a breach to the Department. Therefore, the Department has revised this requirement so only information known to the facility when the breach is reported is required to be reported at that time.

26. Comment Subject: Section 79902(a)(1)(D) Breach Reporting Requirements
Commenter(s): PSJH, HSLAC
Comment: "PSJH suggests that CDPH delete the requirement that health care facilities report patient names in the initial breach report to CDPH. We recognize that CDPH is entitled to this information, and are willing to provide it immediately upon request. However, many times CDPH will not need patient names in order to fulfill its oversight responsibilities. Requiring patient names in the initial report will lead to lists of names of patients being transmitted between facilities and CDPH, which could potentially lead to more breaches."

Department Response: The Department rejects this proposed deletion as the names of patients can be critical to the Department when investigating breaches. The Department often needs the names of patients whose information has been breached when conducting investigations to contact those who have had their information breached. The Department considered this recommendation but rejected it given that it would make investigations of breaches more difficult and the risk of further disclosures are minimal.

27. Comment Subject: Section 79902(a)(1)(F) Breach Reporting Requirements
Commenter(s): PSJH
Comment: "This provision requires the health care facility to report a description of the events surrounding the breach, including "whether the medical information was actually acquired or viewed." PSJH would appreciate clarification on what types of events CDPH believes would be considered breaches where the medical information was not actually acquired or viewed. If none, then this provision should be deleted from the proposed regulation."

Department Response: The Department has considered this comment and has accepted the proposed deletion. The Department has deleted the phrase “including whether the medical information was actually acquired or viewed” from the existing text. This change was made to enhance clarity. If information was not “acquired or viewed” there may not have been a breach as defined.

28. Comment Subject: Section 79902(a)(1)(G) Breach Reporting Requirements
Commenter(s): PSJH
Comment: “PSJH objects to the requirement to include the name and contact information of individuals who “performed” the breach. First of all, this information will not be known in many cases, such as when hackers or thieves access information. At a minimum, this provision should be modified by the phrase “if applicable.” Secondly, as CDPH knows, many health facilities are unionized. Before a health facility can determine that a union member employee has violated the law or the employer’s policies and procedures, the employee is entitled to due process, including union representation during investigative interviews. Health care facilities are not able to require union representatives to conclude their process within 15 days and may be constrained by unions and collective bargaining agreements from disclosing this information at all.”

Department Response: The Department has considered the proposed amendment and has adopted a modified change. The Department has added the qualifier “to the extent known” to this provision. The Department recognizes that health facilities may not always know all the details of a medical information breach when reporting a breach to the Department. Therefore, the Department has revised this requirement so only information known to the facility when the breach is reported is required to be reported at that time.

29. Comment Subject: Section 79902(a)(1)(K) Breach Reporting Requirements
Commenter(s): PSJH
Comment:). This provision would require health care facilities to create and maintain a list of every patient whose medical information was ever breached and keep this information in perpetuity. Given that some breaches can include thousands of patients (or more), this is an extremely onerous and costly administrative requirement that will not result in any new information or other benefit to the patient or to CDPH. There is no statutory authority for such a requirement. PSJH requests that this provision be deleted. At the very least, the time period over which a health care facility would have to look back should be limited to two years.

Department Response: The Department rejects this comment as this requirement does not represent a new requirement that would be burdensome to comply with as it is already a provision of federal law. HIPAA currently requires that health care facilities maintain this information for 6 years, 45 C.F.R. § 164.316 (b). To ensure continuity with federal law and practice, health care facilities will be required to maintain this

information. A two-year retention period would be insufficient for the purposes of the Department in publishing these regulations.

30. Comment Subject: Section 79902(a)(1)(M) Breach Reporting Requirements
Commenter(s): PSJH
Comment: "This provision would require, in some instances, a health care facility to divulge information covered by the attorney-client privilege, attorney work product privilege or peer review privilege. PSJH suggests that this provision be revised as follows "Any audit reports, witness statements, or other documents that the facility relied upon in determining that breach occurred, except for documents subject to an evidentiary privilege recognized in the California Evidence Code."

Department Response: The Department reject this proposed amendment as it unnecessarily burdens Departmental operations. The Department does not wish to encourage health care facilities to make more documents privileged to avoid Department oversight. Further, the Department is permitted to review licensed health facility records, such as root cause analysis or peer review privileged information as part of its investigations. Government Code section 11181; Health and Safety Code sections 1227 & 1278; Fox v. Kramer (2000) 22 Cal.4th 531; Arnett v. Dal Cielo (1996) 14 Cal.4th 4, 10, 56 Cal.Rptr.2d 706, 923 P.2d 1 (Arnett).

31. Comment Subject: Section 79902(a)(5) Breach Reporting Requirements
Commenter(s): PSJH
Comment: "This provision requires a health care facility to compile and retain reams of information related to incidents that do not rise to the level of a reportable breach. While we agree that it is rational for CDPH to require health care facilities to maintain and produce their risk assessments, it is not a good use of scarce health care dollars to require health care facilities to create files of information ("any and all materials…") about such incidents. PSJH suggests that CDPH revise this provision as follows:

"In the event a health care facility has performed, pursuant to section 79901(b)(1)(F), a risk assessment and has determined that an incident does not constitute a breach of a patient's medical information~~, the health care facility shall maintain a centralized record of each non-breach incident, along with any and all materials the health care facility relied upon in performing the risk assessment. All such centralized records~~ the risk assessment shall be maintained by the health care facility and available for inspection by the Department at all times. ~~A health care facility shall retain records relating to such a risk assessment~~ for a period of at least six years from the time of the incident."

Department Response: The Department rejects the revisions made in this comment as the purpose of these regulations to have the records of risk assessments and the associate information. The Department requires access to these records of risk assessments to property conduct its oversight function. In addition, HIPAA currently requires that health care facility maintain these records for 6 years, 45 C.F.R. § 164.316

(b). As such, health care facilities will have a minimal burden in creating and maintaining these records.

32. Comment Subject: Section 79902 Breach Reporting Requirements
Commenter(s): PSJH
Comment: "Under Section 79902 "Breach Reporting Requirements," PSJH recommends that CDPH include timelines for the Department to investigate and respond to a health facility's report of a suspected breach.

- CDPH should extend the time to complete the Statement of Deficiencies/Plan of Correction (Form 2567) from 10 to 15 working days.
- CDPH should provide the event tracking number for each breach report and confirm receipt of the breach notification within 5 business days to the covered entity. It is important that the covered entity receive this timely information so that it can easily reference the report when contacted by CDPH.
- PSJH recommends that CDPH implement a consistent process for reviewing, investigating and tracking a breach report. For example, if a reportable breach occurs at the corporate level and that same breach impacts multiple health facilities with individual licenses, the organization should be able to submit a single corrective action plan rather than separate plans for each licensed facility. Under some circumstances, CDPH's local offices have accepted and rejected some corrective action plans for a single breach from one corporate entity with multiple licensed facilities across the state. PSJH strongly encourages CDPH to adopt a simplified and consistent process for a health system to submit a single corrective action plan for a breach."

Department Response: The Department rejects the proposed amendments as they are unnecessary as they are current Department practice. The Department collects and evaluates breach reporting statistics. The Department has a consistent process for investigating, reviewing, and tracking breach reports through one central team. The Department considered this proposed amendment but determined that current processes were sufficient to address the issues raised by this comment.

33. Comment Subject: Section 79902(a) Breach Reporting Requirements
Commenter(s): SH
Comment: a) A health care facility, excluding a business associate, shall report to the Department a breach of a patient's medical information, or a breach reasonably believed to have occurred, no later than 15 business days after the breach has been detected.

The issue with the aforementioned requirement is that the standard "reasonably believed to have occurred" is vague and confusing. Reasonable belief may be interpreted differently among different entities which creates subjective standards for breach reporting purposes. Moreover, the Department's interpretation is generally more narrowly construed rather than liberally construed. It's a subjective standard that the Department will then make an objective determination on. It is important that the

Department give objective clear and definite factors that determine if a breach has occurred. Therefore, the language should state as follows: “A health care facility shall report to the Department a breach of a patient’s medical information when it is detected via a reasonable investigation.”

Department Response: The Department rejects the proposed amendment as the definition of “Breach” is sufficient to determining when a breach has occurred. The Department considered the proposed amendment but finds that the definition of breach in Section 77901(b)(1) is comprehensive and specific enough to avoid subjective standards for breach reporting purposes.

34. Comment Subject: Section 79902 (1)(d) Breach Reporting Requirements: Name of Patient(s) affected;
Commenter(s): SH
Comment: “The issue with the aforementioned reportable category is that while CDPH is entitled to the names of the affected patients, it is not necessary in order for CDPH to perform oversight over licensed facilities. Further, requiring this information at the initial reporting of the breach could lead to incomplete reporting and unintended disclosures. Often the full scope of a medical information breach is not known until a thorough investigation is completed and while some individuals may be initially thought to have been affected by the breach due to the proximity of their electronic information to affected data, they may ultimately be determined to not be involved after the conclusion of the investigation

Requiring licensed facilities to identify individuals in its initial disclosure may mean the identification of individuals that are thereafter found not to have been involved in the breach. Additional issues with the above requirements are that they are preliminary and usually partial until a supplemental investigation reveals more accurate and complete information. Therefore, reporting or disclosing names of patients in the initial reporting will be premature and should only be required if the Department requests a list of involved patients and/or once it has been determined with reasonable certainty that the patient was in fact involved in the incident.”

Department Response: The Department has considered the proposed amendment and has adopted a modified change. The Department has added the qualifier “to the extent known” to this provision. The Department recognizes that health facilities may not always know all the details of a medical information breach when reporting a breach to the Department. Therefore, the Department has revised this requirement so only information known to the facility is required to be reported at that time.

35. Comment Subject: Section 79902 (g) Breach Reporting Requirements: Names of **who performed the breach**
Commenter(s): SH
Comment: “The issue with the aforementioned reportable category is that often this information is simply not known to the licensed facilities reporting the breach. Due to the

sophistication of many cyber criminals and fraudsters, this may be an impossible category to report. Further to the extent that it was a workforce member involved in the unauthorized access, their identity may be protected either contractually or otherwise. As CDPH is aware, many licensed facilities are unionized and any employees involved in the breach of medical information are provided due process. This process is likely to take more than the 15 days in which a licensed facility must report the incident to the Department. Accordingly, Sutter recommends that this requirement be modified "To the extent known, …"

Further, this requirement would require, in limited situations, licensed facilities to disclose information covered by an evidentiary privilege recognized under the California Evidence Code. For example, witness statements from employees of the licensed facility will likely be protected from disclosure by the attorney-client privilege. Witnesses should both feel and be free to disclose and report fellow employee misconduct without the fear that their identities will be disclosed and/or released. If witnesses feel that their identities will be disclosed or released, this could hinder the candid and truthful reporting of alleged breaches and have a chilling effect that would cause those witnesses who were willing to report breaches to reconsider their actions.

Accordingly, Sutter recommends that the definition should be amended to recognize statements and information subject to an evidentiary privilege."

Department Response: The Department has considered the proposed amendment related to "to the extent known" language and has adopted a modified change. The Department has added the qualifier "to the extent known" to this provision. The Department recognizes that health facilities may not always know all the details of a medical information breach when reporting a breach to the Department. Therefore, the Department has revised this requirement so only information known to the facility when the breach is reported is required to be reported at that time.

The Department rejects the proposed amended that would recognize various privileges. The Department is permitted to review some privileged information pursuant to its authority to investigate an issue to secure compliance with licensing requirements. Interviewing workforce members is also a part of the investigation process—this authority is not going to be reduced. Further, the Department is permitted to review licensed health facility records, such as root cause analysis or peer review privileged information as part of its investigations. Government Code section 11181; Health and Safety Code sections 1227 & 1278; Fox v. Kramer (2000) 22 Cal.4th 531; Arnett v. Dal Cielo (1996) 14 Cal.4th 4, 10, 56 Cal.Rptr.2d 706, 923 P.2d 1 (Arnett).

36. Comment Subject: Section 79902(J) Corrective Action
Commenter(s): SH
Comment: "The issue with the aforementioned reportable category is that a "description of any corrective or mitigating action" may include information which is not disclosable. As CDPH is aware, many licensed facilities are unionized. There could be limits to what

can and cannot be disclosed with employment/corrective actions against individuals involved in a breach because of collective bargaining agreements. Further there could be limits as to the type of corrective/mitigating action that the licensed facility can take due to those same agreements. As drafted this requirement does not account for such instances. Sutter recommends that the above requirement be modified such that it is not a category of information that must be reported."

Department Response: The Department rejects the proposed changes to these requirements as the commenter misinterprets the purpose of these regulations. The Department's purpose in establishing this requirement is to investigate and review how health care facilities reacted to a breach, including new, modified, or refresher training for staff and documentation of remedial actions. The Department is not asking for specific disciplinary action taken again specific employees. The Department considered the commenter's proposed amendment but rejected it as overly restrictive.

37. Comment Subject: Section 79902 (K) Records Retention
Commenter(s): SH
Comment: "The issue with the aforementioned reportable category is that it will create an administrative and financial burden on licensed facilities by requiring massive storage of PHI to be created and maintained for six years solely for reporting purposes. Licensed facilities have two options for compliance, either adding significant amount of data to legacy systems that lack the streamlining and flexibility in order to comply or expending significant amount of capital in developing new systems for the sole purpose of maintaining the necessary data.

Further, administratively, this requires licensed facilities to actually create and maintain significant caches of data containing medical information. These caches are unnecessary duplicates of sensitive information that is unnecessarily increasing licensed facilities potential catastrophic exposure to potential breaches. This could lead to an even larger breach if a licensed facility's system is unfortunately compromised. Therefore, Sutter recommends that this provision be deleted in its entirety, or at a maximum only require licensed facilities maintain records for two years or less."

Department Response: The Department rejects the revisions made in this comment as the purpose of these regulations to have the records of risk assessments. The Department needs access to these records of risk assessments in order to property conduct it oversight function. In addition, HIPAA currently requires that health care facility maintain these records for 6 years. As such, health care facilities will have a minimum burden in creating and maintaining these records.

38. Comment Subject: Section 79902 (M) Privileges
Commenter(s): SH
Comment: "The issue with the aforementioned reportable category is that it doesn't expressly provide for qualified legal exceptions for data that is covered under a recognized evidentiary privilege such as attorney-client or attorney work product. This

would require licensed facilities to disclose information, statements and documents which are otherwise protected. For example, in the process of a licensed facility's breach investigations, there may be confidential attorney-work product, such as audit reports or internal memoranda, which are created and relied upon in making the determination of whether or not a breach occurred. Disclosing such confidential and privileged information would mean that attorneys may be less inclined to create work product, work through alternative theories for the fear that it will be misconstrued or confiscated by the Department when reviewing details of the reported incident.

Additionally, communications between the attorneys and workforce (which may include witness statements) may also be attorney-client privileged communication. By requiring that these communications be disclosed, the Department would be chilling the candid and open communication that is the bedrock of the attorney-client relationship. If a workforce member knows that their communication with the attorney will be disclosed, they may be less willing to be open about any possible breach by naming specific individuals or issues for the fear of retaliation or retribution.

Therefore, Sutter recommends that in an effort to protect long established evidentiary privileges, the newly proposed medical breach information regulation should accommodate such privileged data and make them exceptions to the reporting requirements.

Department Response: The Department rejects this proposed amendment as it unnecessarily burdens Departmental operations. The Department does not want to make it more difficult to conduct investigations because more documents are protected by a privileged. In addition, the Department does not want to have health care facilities to make more documents privileged to avoid Department oversight. Finally, the Department does not intend to ask for documents that are privileged.

The Department rejects the proposed amended that would recognize various privileges. The Department is permitted to review some privileged information pursuant to its authority to investigate an issue to secure compliance with licensing requirements. Interviewing workforce members is also a part of the investigation process—this authority is not going to be reduced. Further, the Department is permitted to review licensed health facility records, such as root cause analysis or peer review privileged information as part of its investigations. Government Code section 11181; Health and Safety Code sections 1227 & 1278; Fox v. Kramer (2000) 22 Cal.4th 531; Arnett v. Dal Cielo (1996) 14 Cal.4th 4, 10, 56 Cal.Rptr.2d 706, 923 P.2d 1 (Arnett).

39. Comment Subject: Section 79902 (3), (4)
Commenter(s): SH
Comment: "The issue with the aforementioned requirement that a breach is not considered "reported" unless all categories of information are reported is impractical. For example, it may be impossible to determine with certainty the time that the breach occurred (Section 79902(a)(1)(A)) or the names of the patients affected (Section

79902(a)(1)(D)) or whom actually committed the unauthorized access (Section 79902(a)(1)(G)). Further, as a general issue, most of the categories of information the Department requires to be reported will not yet be available to the reporting licensed facility within 15 days. While the Department has attempted to account for this possibility within this provision, in its Statement of Reasons, the Department states that it will determine whether delay in providing information is unreasonable on a "case-by-case basis." The exceptions are therefore arbitrary and subjective to the individual reviewing the reported breach. There is no exception to the rule or guidance on how it will be determined and this leaves all licensed facilities in uncertainty as to what information will be accepted by the Department as sufficient and what will not. In one situation, the Department may determine the information provided by the licensed facility to be sufficient, but in a similar instance, reporting the same information within the same time frame may be considered insufficient.

Finally, some categories of information are protected from disclosure under attorney-client privilege and attorney work product exception and cannot be disclosed. However, as currently drafted, unless and until all categories are reported, the Department may determine to levy fines and penalties against the licensed facility. This means that the licensed facilities must either disclosed privileged information or risk being fined for non-compliance until they do.

Therefore, Sutter would recommend that the provision should be modified with "to the extent available" or "as reasonably possible" to acknowledge the ongoing nature of investigations and provides some flexibility for facilities to perform a thorough investigation rather than provide incomplete and possibly incorrect information under fear of being penalized. Further, as previously stated and advocated, the newly proposed regulation should expressly state qualified exceptions to the breach reporting requirements that are legally enforceable and recognized, i.e. attorney-client privilege and attorney work product."

Department Response: The Department rejected the proposed amendment that recognizes privilege as it unnecessarily burdens Departmental operations. The Department does not wish to encourage health care facilities to make more documents privileged to avoid Department oversight. Further, the Department is permitted to review licensed health facility records, such as root cause analysis or peer review privileged information as part of its investigations. Government Code section 11181; Health and Safety Code sections 1227 & 1278; Fox v. Kramer (2000) 22 Cal.4th 531; Arnett v. Dal Cielo (1996) 14 Cal.4th 4, 10, 56 Cal.Rptr.2d 706, 923 P.2d 1 (Arnett).

In addition, the Department has considered the proposed amendment related to "to the extent available" language and has adopted a modified change. The Department has added the qualifier "to the extent known" to this provision. The Department recognizes that health facilities may not always know all the details of a medical information breach when reporting a breach to the Department. Therefore, the Department has revised this

requirement so only information known to the facility when the breach is reported is required to be reported at that time

40. Comment Subject: Section 79902(a)(1).
Commenter(s): CHA
Comment: "Health and Safety Code Section 1280.15 requires health care facilities to report the fact that a breach has occurred to CDPH within 15 business days. However, this statute does not require the facility to complete its entire investigation in this time period. In fact, in many cases it will be impossible to do so. CDPH recognizes this time limitation in Section 77902(a)(2) where it requires the facility to report additional information as it becomes available after the 15 business days. We suggest that Section 77902(a)(1) be clarified to accord with this understanding, and state that the facility must provide "the following, to the extent known:."

Department Response: The Department has considered the proposed amendment related to "to the extent known" language and has adopted a modified change. The Department has added the qualifier "to the extent known" to this provision. The Department recognizes that health facilities may not always know all the details of a medical information breach when reporting a breach to the Department. Therefore, the Department has revised this requirement so only information known to the facility when the breach is reported is required to be reported at that time

41. Comment Subject: Section 79902(a)(1)(D)
Commenter(s): CHA, HSLAC
Comment: "The proposed regulations require health facilities to report to CDPH, in the initial breach report, the names of patients whose privacy was breached. **This requirement does not comply with the "necessity" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq.** and, indeed, will only result in broader dissemination of private patient health information. In the interest of protecting patient privacy as much as possible, CHA urges that CDPH delete the requirement that health facilities report patient names in the initial breach report. Instead, CHA recommends that health facilities be required to report the number of patients breached in the initial report, but not the patient names. We recognize that CDPH is entitled to patient names as part of its investigation, and hospitals are willing to provide them immediately upon CDPH investigator request. However, CDPH rarely needs patient names in order to fulfill its oversight responsibilities.

Consider a past incident where a hospital's computer — containing 4 million patient names and associated information — was stolen. What would CDPH do with 4 million patient names? It is neither necessary nor sensible for the hospital to report the 4 million patient names to CDPH in the initial report. This requirement would lead to lists of patient names being transmitted between facilities and CDPH, which will potentially lead to more breaches. Keeping patient names as private as possible is especially important when the health care facility is an acute psychiatric hospital."

Department Response: The Department asserts that this provision satisfies the "necessity" standard of the Administrative Procedures Act as there is substantial evidence of need for a regulation to effectuate the purpose of the statute. The Department rejects this proposed deletion as the names of patients can be critical to the Department when investigating breaches. The Department often needs the names of patients whose information been breached when conducting investigations in order to contact those who have had their information breached. In addition, this information is necessary for the purpose of the investigation and penalty calculations. For the penalty, the Department takes into account each instance of a breach of one person's information as well as the number of patients' information that was breached. The Department considered this recommendation but rejected it given that it would make investigations of breaches more difficult and the risk of further disclosures are minimal.

42. Comment Subject: Section 79902(a)(1)(F)
Commenter(s): CHA
Comment: "This provision does not make sense. It purports to require a health facility to inform CDPH, in a breach report, whether "the medical information was actually acquired or viewed." However, according to California's appellate courts, no violation of state law or patient privacy has occurred unless the medical information was actually viewed. **Therefore, this provision does not comply with the "consistency" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq.** As discussed previously in this letter, California courts have held that if a person's medical information is not viewed, then no breach has occurred. In *Sutter Health et al. v. Superior Court of Sacramento (Atkins et al., real parties in interest), 227 Cal.App.4th 1546 (July 21, 2014),* the California appellate court stated that, "No breach of confidentiality takes place until an unauthorized person views the medical information." If this provision is not deleted, we ask that CDPH clarify what types of events it believes would be considered breaches if the medical information was not actually acquired or viewed."

Department Response: The Department asserts this requirement satisfies the "consistency" standards of the Administrative Procedures Act as the commenter is misinterpreting case law.

The case referenced in the proposed amendment relates to patients seeking damages for the negligent release of their own medical information as afforded by the private right of action in the Confidentiality of Medical Information Act (CMIA) under Civil Code section 56 et seq. Sutter Health et al. v. Superior Court of Sacramento County (Atkins et al. real parties in interest), 227 Cal.App.4th 1546 (July 21, 2014). The court found that " section 56.1010, subdivision (a) makes it clear that *preserving the confidentiality* of the medical information, not necessarily preventing others from gaining possession of the paper-based or electronic information itself, is the focus of the legislation. *Id*. at 1556. Therefore, if the confidentiality is not breached, the statute is not violated."

The court interprets a breach of medical information within the context of a specific provision in the CMIA and the standard by which a confidentiality is breached hinges on the preservation of confidentiality. In contrast, the Health and Safety code section 1280.15 requires a duty to *prevent* unlawful or unauthorized access to and use or disclosure of medical information [emphasis added]. The standards between the two statutes vastly differ from one another. Additionally, unlike Civil Code section 56.36, the Health and Safety Code does not contain a parallel requirement that the Department prove an injury and damages in order to investigate and assess a penalty for an unauthorized or unlawful access to medical information. Further, SB 541 established the Health and Safety Code section 1280.15 in part because the CMIA was found inadequate in addressing unauthorized access to medical information "access events" or "snooping" into patient medical records. Therefore, the applicability of any case law interpreting the CMIA would not correspond to the standard for establishing a breach pursuant to Section 1280.15.

Therefore, the current definition of "access" is consistent with the Department's separate enforcement of unauthorized or unlawful access to medical information pursuant to Health and Safety Code section 1280.15.

43. Comment Subject: Section 79902(a)(1)(G)
Commenter(s): CHA, HSLAC
Comment: The requirement to include, in the initial breach report, the name and contact information of individuals who "performed" a breach and any unauthorized person who received the medical information does not comply with the "necessity" or "consistency" standard of the Administrative Procedure Act, as defined in Government Code Section 11349 et seq. First of all, this information will not be known in many cases, such as when hackers or thieves access information. At a minimum, this provision should be modified by the phrase "if applicable and known." Secondly, before a health facility can determine that an employee or other person has violated the law or the employer's policies and procedures, the employee is entitled to due process, including union representation during investigative interviews. This often will take more than 15 days. Many health facilities are unionized, and unable to require union representatives to conclude their process within 15 days, and also may be constrained by unions and collective bargaining agreements from disclosing this information at all. The California Legislature did not abrogate employees' employment rights in Health and Safety Code Section 1280.15.

Department Response: The Department has considered the proposed amendment related to "to the extent known" language and has adopted a modified change. The Department has added the qualifier "to the extent known" to this provision. The Department recognizes that health facilities may not always know all the details of a medical information breach when reporting a breach to the Department. Therefore, the Department has revised this requirement so only information known to the facility when the breach is reported is required to be reported at that time

44. Comment Subject: Section 79902(a)(1)(K).
Commenter(s): CHA, HSLAC
Comment: "This provision would require health care facilities to create and maintain a database of every patient whose medical information was breached, and keep this information for six years. **This provision does not meet the "necessity" or "authority" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq**. Given that some breaches can include tens of thousands of patients (or more), this is an extremely onerous and costly administrative requirement that will not provide any information that CDPH needs or can use to enforce Health and Safety Code Section 1280.15. It also will not provide any benefit to patients. Quite the opposite, it will divert funds away from patient care uses to data entry and database administration. There is no statutory authority for CDPH to require health facilities to create this new system, and the statute contemplates no use for the information that would be generated. In addition, hospitals have not been required to maintain this information for breaches not required to be reported at the federal level, and thus will not be able to comply in the first six years after adoption of this provision, if indeed it is adopted despite its noncompliance with the Administrative Procedure Act standards. For these reasons, this provision should be stricken."

Department Response: The Department rejects the proposed deletion recommended by this comment as health care facility are already required to maintain this information under HIPAA, 45 C.F.R. § 164.316 (b). The Department is harmonizing state and federal standards in order to ensure patient projection and lessen the burden on the regulated community.

In addition, the Department asserts that the record developed in this rulemaking is more than sufficient to demonstrate that this rulemaking meets the "necessity" standard of the Administrative Procedures Act. The Department also has "authority", in Health and Safety Code Sections 131000, 131050, 131051, 131052 and 131200, to adopt these regulations.

45. Comment Subject: Section 79902(a)(1)(M).
Commenter(s): CHA, HSLAC
Comment: "This provision does not meet the "necessity" or "consistency" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq., as it would require, in some instances, a health care facility to divulge information covered by the attorney-client privilege, attorney work product privilege, or peer review privilege. If the California Legislature had intended to amend those laws, it would have done so explicitly. In addition, it has been our experience that CDPH investigators need guidance from hospital staff to properly read audit logs, and that hospitals must spend significant resources in redacting other patients' names from them prior to producing them. Therefore, these documents should be made available upon CDPH request rather than in the initial report. CHA urges that this provision be moved out of the initial report portion of the regulation and revised as follows:

Upon Department request, a health care facility shall provide ~~Any~~ audit reports, witness statements, or other documents that the facility relied upon in determining that a breach occurred except for documents subject to an evidentiary privilege recognized in the California Evidence Code."

Department Response: The Department rejects this proposed amendment as it unnecessarily burdens Departmental operations. The Department does not want to make it more difficult to conduct investigations because more documents are protected by a privileged. In addition, the Department does not want to have health care facilities to make more documents privileged to avoid Department oversight. Finally, the Department does not intend to ask for documents that are privileged.

The Department rejects the proposed amended that would recognize various privileges. The Department is permitted to review some privileged information pursuant to its authority to investigate an issue to secure compliance with licensing requirements. Interviewing workforce members is also a part of the investigation process—this authority is not going to be reduced. Further, the Department is permitted to review licensed health facility records, such as root cause analysis or peer review privileged information as part of its investigations. Government Code section 11181; Health and Safety Code sections 1227 & 1278; Fox v. Kramer (2000) 22 Cal.4th 531; Arnett v. Dal Cielo (1996) 14 Cal.4th 4, 10, 56 Cal.Rptr.2d 706, 923 P.2d 1 (Arnett).

In addition, the Department asserts that the record developed in this rulemaking is more than sufficient to demonstrate that this rulemaking meets the "necessity" standard of the Administrative Procedures Act. These regulations are also "consistent" as these regulations are, as required by Government Code Section 11349 (D), "in harmony with, and not in conflict with or contradictory to, existing statutes, court decisions, or other provisions of law."

46. Comment Subject: Section 79902(a)(4).
Commenter(s): CHA
Comment: "This provision is slightly inconsistent with Section 79902(a)(2), which requires that additional information be reported to CDPH "as it becomes available to the health care facility." CHA suggests that 79902(a)(4) be revised slightly to mirror (a)(2), as follows:

(4) A breach shall not be deemed reported to the Department unless the health care facility has provided, or made a good faith effort to provide, to the Department the items required in section 79902(a)(1). Any items required for reporting under section 79902(a)(1) not available to the health care facility at the time of the reporting shall be provided to the Department as ~~soon as~~ they are available to the health care facility. Any unreasonable delays in reporting by the health care facility pursuant to this subdivision are subject to an administrative penalty…"

This revision will allow health facilities to submit information to CDPH in a reasonable timeframe, but in an organized manner, rather than piecemeal as soon as each bit of information becomes available.

Department Response: In response to a public comment, the Department has added the qualifier "to the extent known" to 79902(A)(1)(G). The Department recognizes that health facilities may not always know all the details of a medical information breach when reporting a breach to the Department. Therefore, the Department has revised this requirement so only information known to the facility when the breach is reported is required to be reported at that time.

In response to a public comment, the Department has deleted the words "soon as" from the second sentence of this provision. This change was made so that this section conforms with the requirements in subparagraph (a)(2) that health facilities must submit further information that was not available at the time of the initial report in an organized manner in a reasonable timeframe. This change improves the clarity and consistency of the regulation.

47. Comment Subject: Section 79902(a)(5).
Commenter(s): CHA, HSLAC
Comment: "This provision requires a health care facility to compile and retain reams of information related to incidents that do not rise to the level of a reportable breach. **This requirement does not comply with the "necessity" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq.** While we agree that it is rational for CDPH to require health care facilities to maintain and produce their risk assessments, it is not a good use of scarce health care dollars to require health care facilities to create files of information ("any and all materials…") about such minor incidents. CHA suggests that CDPH revise this provision as follows:

In the event a health care facility has performed, pursuant to section 79901(b)(1)(F), a risk assessment and has determined that an incident does not constitute a breach of a patient's medical information, ~~the health care facility shall maintain a centralized record of each non-breach incident, along with any and all materials the health care facility relied upon in performing the risk assessment. All such centralized records~~ the risk assessment shall be maintained by the health care facility and available for inspection by the Department at all times~~ A health care facility shall retain records relating to such a risk assessment~~ for a period of at least six years from the time of the incident."

Department Response: The Department rejects the revisions made in this comment as the purpose of these regulations to have the records of risk assessments and the associate information. The Department requires access to these records of risk assessments in order to property conduct its oversight function. In addition, HIPAA currently requires that health care facility maintain these records for 6 years, 45 C.F.R. § 164.316 (b). As such, health care facilities will have a minimal burden in creating and maintaining these records.

In addition, the Department asserts that the record developed in this rulemaking is more than sufficient to demonstrate that this rulemaking meets the "necessity" standard of the Administrative Procedures Act.

48. Comment Subject: 79903(a).
Commenter(s): PSJH
Comment: PSJH suggests that this provision be revised as follows: "The Department may impose an administrative penalty upon a health care facility if the Department determines that the health care facility has committed a breach of a patient's medical information resulting from a failure of that facility to implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information."

Department Response: The Department rejects this comment because the commenter's suggestions are based on a misunderstanding of the underlying statute. This statute contains a strict liability standard, not a lesser standard that allows facilities to avoid liability for the actions of their agents. These rules are built on the idea that health care facilities are responsible for the actions of their agents when those agents do not meet the legal obligations to protect patient information. Health care facilities cannot delegate this duty to protect patient information.

The plain language of the controlling statute indicates this is a strict liability statute. Specifically, it reads, in part, that a health 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." (Health & Saf. Code § 1280.15.) By including the words, "shall prevent," the legislature sought to impose strict liability upon health facilities if a breach of patients' medical information occurs. When interpreting a statute, courts are obligated "to give significance and effect to each word and phrase and to avoid a construction that makes any part of the statute superfluous or meaningless." (Shaw v. People ex rel. Chiang, 175 Cal.App.4th 577, 600 (2009) (citations omitted); see also Corley v. United States, 556 U.S. 303, 315 (2009) (emphasizing, "one of the most basic interpretive canons, that a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant").) The plain language of this statute directs the Department to impose a penalty when there is a medical information breach.

Furthermore, a court must ascertain the intent of the Legislature in order to "effectuate the purpose of the law." (Alexander v. Superior Court, 5 Cal.4th1218, 1226 (1993). As noted in the above section, the legislative intent is clear in its direction that a penalty must be imposed in order to curb continued breaches. The statutory reference to section 1280.18 is for purposes of identifying a factor in deciding the penalty assessment the Department may issue when a violation occurs. This is the plain language reading of section 1280.15 which gives the Department discretionary authority in determining the appropriate penalty amounts, if any, that may be assessed. One of the factors to consider is whether a facility has complied with related statutes and

regulations to determine the appropriate penalty amount. Section 1280.18 requires a facility to (1) establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information; and (2) to reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use, or disclosure. It does not indicate that a facility would be further relieved of wrongdoing by simply demonstrating these safeguards.

The commenter ignores the plain language of the statute as well as the Legislature's intent to hold facilities responsible for their failures to prevent breaches. It is reasonable to infer that the Legislature directed the Department to specifically determine whether the facility violated these requirements before determining a penalty amount.

49. Comment Subject: 79903(b).
Commenter(s): PSJH
Comment: "This provision provides no guidance to the regulated industry or to CDPH surveyors as to the circumstances under which an administrative penalty is "warranted." It leaves complete discretion to CDPH. This will lead to the inconsistent and arbitrary imposition of penalties —precisely an outcome that regulations should be designed to avoid. In addition, the base penalty should be variable, similar to the base penalties in CDPH's regulations under Title 22, California Code of Regulations, Section 70951 *et seq.* These currently existing administrative penalty regulations recognize that different degrees of intentional or negligent behavior call for different base penalties. PSJH urges that CDPH recognize this fact in these regulations, also. Further, the base penalty amounts should be rationally related: it makes no sense for the base penalty for a privacy violation to be $15,000, while the base penalty for a medical error can be as low as $5,000 (20% of $25,000). The medical breach regulations should consider, as do the existing administrative penalty regulations, the widespread or isolated nature of the violation (scope) and the severity of the harm to the patient, if any."

Department Response: The Department rejects the changes requested by this comment. The current penalty adjustment factors are drawn from Health and Safety Code section 1280.15(a) which establish the factors the Department must consider when establishing penalty amounts. The Department asserts that these standards are sufficient to ensure uniform application of these provisions.

50. Comment Subject: 79903(c)
Commenter(s): PSJH
Comment: "This provision does not take into consideration the widespread or isolated nature of the violation (scope) or the severity of the harm to the patient, if any. This provision should be revised to do so."

Department Response: The Department rejects this the premise underlying this comment. The Department does take into consideration how widespread or isolated the nature of a violation is when establishing penalty amounts.

51. Comment Subject: Section 79903(a)
Commenter(s): CHA
Comment: As discussed earlier in this letter, the authorizing statute establishes a negligence standard, not a strict liability standard. **Thus, this provision does not comply with the "authority" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq.** (see the discussion under "Standard for Assessing a Fine Against a Health Facility," starting on page 1 of this letter). CHA suggests that this provision be revised as follows:

The Department may impose an administrative penalty upon a health care facility if the Department determines that the health care facility has committed a breach of a patient's medical information resulting from a failure of that facility to implement an appropriate administrative, technical, or physical safeguard to protect the privacy of a patient's medical information.

Department Response: The Department rejects this comment because the commenter's suggestions are based on a misunderstanding of the underlying statute. This statute contains a strict liability standard, not a lesser standard that allows facilities to avoid liability for the actions of their agents. The commenter misstates the law in asserting that "a health facility should not be responsible for "factors outside its control"; instead, the statute requires the Department to "*consider*…factors outside [the facility's]…control that restricted the facility's ability to comply with this section" in "determining whether to investigate an incident, and the amount of an administrative penalty, if any…" (Health and Safety Code section 1280.15, emphasis added.) These rules are built on the idea that health care facilities are responsible for the actions of their agents when those agents do not meet the legal obligations to protect patient information. Health care facilities cannot delegate this duty to protect patient information.

The plain language of the controlling statute demonstrates that this is a strict liability statute. Specifically, it reads, in part, that a health 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." (Health & Saf. Code § 1280.15.) By including the words, "shall prevent," the legislature sought to impose strict liability upon health facilities if a breach of patients' medical information occurs. When interpreting a statute, courts are obligated "to give significance and effect to each word and phrase and to avoid a construction that makes any part of the statute superfluous or meaningless." (Shaw v. People ex rel. Chiang, 175 Cal.App.4th 577, 600 (2009) (citations omitted); see also Corley v. United States, 556 U.S. 303, 315 (2009) (emphasizing, "one of the most basic interpretive canons, that a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant").) The plain language of this statute directs the Department to impose a penalty when there is a medical information breach.

Furthermore, a court must ascertain the intent of the Legislature in order to "effectuate the purpose of the law." (Alexander v. Superior Court, 5 Cal.4th1218, 1226 (1993). As noted in the above section, the legislative intent is clear in its direction that a penalty must be imposed in order to curb the continued breaches. The statutory reference to section 1280.18 is for purposes of identifying a factor in deciding the penalty assessment the Department may issue when a violation occurs. This is the plain language reading of section 1280.15 which gives the Department discretionary authority in determining the appropriate penalty amounts, if any, that may be assessed. One of the factors to consider is whether a facility has complied with related statutes and regulations to determine the appropriate penalty amount. Section 1280.18 requires a facility to (1) establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information; and (2) to reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use, or disclosure. It does not indicate that a facility would be further relieved of wrongdoing by simply demonstrating these safeguards.

The commenter ignores the plain language of the statute as well as the Legislature's intent to hold facilities responsible for their failures to prevent breaches. It is reasonable to infer that the Legislature directed the Department to specifically determine whether the facility violated these requirements before determining a penalty amount. If a facility has complied with 1280.15, yet a breach still occurs, then the Department may consider this as a mitigating factor, amongst others, when issuing the penalty amount

52. Comment Subject: Section 79903(b)
Commenter(s): CHA
Comment: "This provision does not comply with the "clarity" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq., as it provides no guidance to the regulated industry or to CDPH surveyors for the circumstances under which an administrative penalty is "warranted." This will lead to the inconsistent and arbitrary imposition of penalties — precisely an outcome that regulations should be designed to avoid. In addition, the base penalty should be variable — similar to the base penalties in CDPH's regulations under Title 22, California Code of Regulations, Section 70951 et seq. — recognizing that different degrees of intentional or negligent behavior call for different base penalties. CHA urges CDPH to recognize this fact in these regulations as well. Furthermore, the base penalty amounts should be rationally related. It makes no sense for the base penalty for a privacy violation to be $15,000, while the base penalty for a medical error can be as low as $5,000 (20% of $25,000). The medical breach regulations should consider, as do the existing administrative penalty regulations, the widespread or isolated nature of the violation (scope) and the severity of the harm to the patient, if any."

Department Response: The Department rejects the changes requested by this comment. The current penalty adjustment factors are drawn from Health and Safety Code section 1280.15(a) which establish the factors the Department must consider

when establishing penalty amounts. The Department asserts that these standards are sufficient to ensure uniform application of these provisions.

53. Comment Subject: Section 79903(c)
Commenter(s): CHA
Comment: This provision does not take into consideration the widespread or isolated nature of the violation (scope) or the severity of the harm to the patient, if any. It should be revised to do so.

Department Response: The Department rejects this the premise underlying this comment. The Department does take into consideration how widespread or isolated the nature of a violation is when establishing penalty amounts.

54. Comment Subject: Section 77904.
Commenter(s): PSJH
Comment: "This section provides no guidance to surveyors, or information to health care facilities, about how CDPH will apply the factors that it is required by statute to apply in assessing penalties. This is a major omission and should be a major point in this regulation package."

Department Response: The Department rejects the changes requested by this comment. The current penalty adjustment factors are drawn from Health and Safety Code section 1280.15(a) which establish the factors the Department must consider when establishing penalty amounts. The Department asserts that these standards are sufficient to ensure uniform application of these provisions.

55. Comment Subject: 79904(a)(4).
Commenter(s): PSJH
Comment: "PSJH suggests that CDPH add a sentence to this provision, reading as follows: "The Department shall identify for the health care facility, in writing, the other factors that were considered and how each factor affected the penalty to be assessed." This will help keep CDPH personnel who set penalty amounts consistent among facilities and over time and let facilities know what they should and should not do in the future."

Department Response: The Department rejects the changes requested by this comment. The current penalty adjustment factors are drawn from Health and Safety Code section 1280.15(a) which establish the factors the Department must consider when establishing penalty amounts. The Department asserts that these standards are sufficient to ensure uniform application of these provisions. In addition, the Department already provides the heath care facility with documentation containing the calculation of the penalties.

56. Comment Subject: Section 77904.
Commenter(s): CHA
Comment: This section provides no guidance to surveyors, or information to health care facilities, about how CDPH will apply the statutorily-required factors in assessing penalties. This is a major omission in this regulation package, whereas it should be a major point of clarification. **The proposed regulation does not comply with the "clarity" standard of the Administrative Procedure Act as defined in Government Code Section 11349 et seq., in that it neglects to address how CDPH will apply the statutory factors.**

Department Response: The Department rejects the changes requested by this comment. The current penalty adjustment factors are drawn from Health and Safety Code section 1280.15(a) which establish the factors the Department must consider when establishing penalty amounts. The Department asserts that these standards are sufficient to ensure uniform application of these provisions. In addition, the Department already provides the heath care facility with documentation containing the calculation of the penalties.

In addition, the Department asserts that these regulations are written so that the meaning of regulations will be easily understood by those persons directly affected by them as required by Government Code Section 11349(c).

59. Comment Subject: Section 79904(a)(4
Commenter(s): CHA, HSLAC
Comment: CHA requests that CDPH add a sentence to this provision that reads as follows: "The Department shall identify for the health care facility, in writing, the other factors that were considered and how each factor affected the penalty to be assessed." This will help keep CDPH personnel who set penalty amounts consistent among facilities and over time, and will inform facilities about what they should and should not do in the future.

Department Response: The Department rejects the changes requested by this comment. The current penalty adjustment factors are drawn from Health and Safety Code section 1280.15(a) which establish the factors the Department must consider when establishing penalty amounts. The Department asserts that these standards are sufficient to ensure uniform application of these provisions. In addition, the Department already provides the heath care facility with documentation containing the calculation of the penalties.

ATTACHMENTS TO THE FINAL STATEMENT OF REASONS

ADDENDUM II

15 Day Public Notice

Summary of Comments and Responses to Comments Received During the Public Availability Period

The Department received one comment from one commenter during the public availability notice period beginning December 9, 2020, through December 28, 2020.

LIST OF COMMENTERS (WT - Written Testimony)

1. Dignity Health (DH)

1. Comment Subject: 79902(a)(1)(K). Required Elements --
Commenter(s): DH
Comment: Required Elements – "The proposed regulations continue to include an expanded list of required elements that must be in a facility's report to the Department. Among them at Section 79902(a)(1) is subsection K: "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." This new requirement will impose extremely costly burdens on facilities for little or no benefit to patients.

Like most hospitals, Dignity Health's hospital compliance events (including potential breach events) are documented in a computer application that is not connected with the patient electronic record. Each privacy event investigation is separately documented in a secure system, including a listing (usually in the form of an excel spreadsheet) of all the names and addresses of the affected patients. In a large hospital, over the course of several years there will be many such events and documents.

The hospital's accounting of disclosures process will often (perhaps usually) not be of help with this new required element. While the HIPAA Privacy Rule contains a patient right to an accounting of disclosure, Dignity Health (like all other covered entities) receives **extremely few** such requests. The Privacy Rule does not require that a hospital maintain a running list of all disclosures in order to provide an accounting to a patient; many hospitals will compile an accounting of disclosures only if and when a patient asks for such a list. This means that many (and probably most) hospitals will not have one place in which to look to find out if a particular patient has been included in a past breach event.

In such circumstances, identifying all prior breaches for a patient requires looking through literally every single privacy event at the facility, checking on every name. Obviously, that would be an ***extremely labor intensive and costly*** process. The process would be analogous to what one could imagine CDPH would have to go through if it were required to determine from its own records of breaches if a specific patient had ever before been a victim of a prior breach within the last six years. Even if CDPH itself organizes its breaches by patient name, and could easily identify all the

breaches experienced by a specific patient within the last 6 years, it should not assume that all licensed facilities organize their documentation similarly – which would be required in order to comply with Subsection K.

The burden of the requirement is truly overwhelming, and it is difficult to see any, much less commensurate, benefit for patients. Patients will have already known about all other prior events involving their information, having already received written notice of those events. There is no statutory mandate to provide this information to the Department, and it is unclear what use the Department will make of the information. Given the problems identified here, **Dignity Health very strongly urges the Department to eliminate Subsection K of Section 79902(a)(1) because it imposes severe burdens on health care facilities without any perceptible benefit.**

Department Response: The Department reject this proposed deletion as this requirement does not impose severe burdens on health care facilities without any perceptible benefits and helps the Department in the completion of its work. Health care facilities must already collect and store this information as part of the facility's obligations under HIPAA, 45 C.F.R. § 164.316 (b). In addition, this information is useful to the Department in the calculation of penalties as compliance history is a factor in setting penalty amounts. The Department in considering this deletion perceives no benefit to facilities if these obligations were reduced and the impediment in the critical work of calculating penalties.