CALIFORNIA HOSPITAL ASSOCIATION

Providing Leadership in Health Policy and Advocacy

August 20, 2020

Heidi Steinecker
Deputy Director, Center for Health Care Quality
California Department of Public Health
c/o Office of Regulations
1415 L Street, Suite 500
Sacramento, CA 95814

Submitted via email to Heidi Steinecker and the CDPH Office of Regulations (regulations@cdph.ca.gov)

Subject: DPH-11-009: Medical Information Breach Proposed Regulations

Dear Ms. Steinecker:

The California Hospital Association (CHA) — representing more than 400 hospitals and health systems and 97% of patient beds in the state — appreciates the opportunity to comment on the California Department of Public Health (CDPH) proposed regulations on medical information breaches. CHA member hospitals work hard to design systems that protect patient privacy and to notify patients when human mistakes or illegal behavior result in breaches. We are committed to working with CDPH on this important effort.

CHA is grateful to CDPH for its revisions to the proposed regulations following the comment periods in 2018 and 2019. In addition, we applaud CDPH for its efforts to harmonize the proposed regulations with the federal Breach Notification Rule promulgated by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

CHA continues to have several concerns with the proposed regulations. We first describe two overarching concepts, and then focus on specific sections of the regulations.

Standard for Assessing a Fine Against a Health Facility

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 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 unathorized 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 "consider… factors beyond the provider's immediate control that restricted

[1] 45 C.F.R. Sections 164.308, 164.310, and 164.312, respectively.
[2] Health and Safety Code Section 1280.15(a) (emphasis added).
[3] Health and Safety Code Sections 1280.15(a) and 1280.18(b).

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 take action against the individual. (The authority to take action 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 recodified 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.

Business Associates and Medical Staff

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 defintion 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.

[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."

Specific Sections

Section 79901. Definitions.

Section 79901(a). Access – This definition should be revised to clarify that "access" means that someone *actually* 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 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 *actually* 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 has the *ability* to read any medical record in the system. However, the system administrator should be considered to have accessed a record only if she *actually* 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."

Section 77901(b)(1)(A). Breach – 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."

Section 77901(b)(1)(B). Breach – 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.

Section 77901(b)(1)(E). Breach — 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 pharase "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 facilty" and into the definition of "health care system.

Section 77901(c). Business Associate — 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").

Section 79901(f). Detect — 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.

Section 79901(i). Factors outside the control of the health care facility —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.

Section 77901(j). Health care facility — 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 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."

Section 79901(k). Health care system — 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 idividuals. 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.

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

Section 77901(l). Medical information — 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.

Section 79901(m). Medical staff — 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 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 clincal 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

[7] Title 22, California Code of Regulations, Section 70701.
[8] *O'Byrne v. Santa Monica-UCLA Med. Ctr.*, 94 Cal. App. 4th 797 (2001).

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 Admnistrative Procedure Act.** If the California 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]

Section 79902. Breach Reporting Requirements.

Section 79902(a)(1). 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:."

Section 79902(a)(1)(D). 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.

[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.
[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."

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.

Section 79902(a)(1)(F). 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.

Section 79902(a)(1)(G). **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.

Section 79902(a)(1)(K). 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.

Section 79902(a)(1)(M). **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.

Section 79902(a)(4). 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.

Section 79902(a)(5). 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.

Section 79903. Administrative Penalties.

Section 79903(a). 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.

Section 79903(b). **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.

Section 79903(c). 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.

Section 79904. Penalty Adjustment Factors.

Section 77904. 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.**

Section 79904(a)(4). 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.

Thank you for the opportunity to comment on these important regulations. If you have any questions, please do not hesitate to contact me at lrichardson@calhospital.org or (916) 834-7611.

Sincerely,

/s/

Lois J. Richardson
Vice President and Legal Counsel