CALIFORNIA HOSPITAL ASSOCIATION

Providing Leadership in Health Policy and Advocacy

December 7, 2018

California Department of Public Health
Office of Regulations
1415 L Street, Suite 500
Sacramento, CA 95814

Submitted via email to regulations@cdph.ca.gov

Subject: DPH-11-09: Medical Information Breach Proposed Regulations

To Whom It May Concern:

The California Hospital Association (CHA) — representing more than 400 hospitals and health systems and 97 percent of patient beds in the state — appreciates the opportunity to comment on the California Department of Public Health (CDPH) proposed regulations regarding medical information breaches. This letter will address two overarching issues, and then include technical comments on specific proposed sections.

Harmonization with HIPAA

At the outset, CHA applauds 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 and other stakeholders have long advocated for a uniform set of breach notification standards to help address the complexity of health information privacy laws. The more consistent state and federal laws are, the better both patients and providers can understand their rights and obligations thereunder. We are pleased that this rulemaking takes an important step in this direction. Our comments below will point out additional instances where greater harmonization could be accomplished in the proposed regulations.

Strict Liability vs. Negligence Standard

CHA has been greatly concerned that CDPH has issued fines against California hospitals for privacy breaches when there was no finding that the hospital was negligent in any way, contrary to the express language of the relevant statutes and the intent of the Legislature. Specifically, hospitals have received fines despite the fact that they implemented appropriate administrative, technical and physical safeguards — such as employee background checks, training, policies and procedures, auditing, monitoring, and disciplining — but, nevertheless, found themselves victimized by a hacker, thief or employee who stole patient information or deliberately and knowingly disclosed patient information. Fines have been issued even when a criminal act was involved and when the offending employee acknowledged that s/he received appropriate training, knew the disclosure was illegal and violated hospital policy.

This is exactly the type of circumstance that was discussed at length during negotiations on SB 541 (Stats. 2008, c. 605) and AB 211 (Stats. 2008, c. 602). As you may recall, 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 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 these requirements. The parties to the SB 541 discussions (legislators and their staff, Governor's administration staff, and 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 parties to the SB 541 discussion agreed that individuals would be held responsible for their bad deeds — rather than the clinic, health facility, home health agency or hospice, if the clinic, facility, home health agency or hospice had 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 the facility's ability to comply"; this is also why the enforcement agency was given the authority to take action against individuals.

The Governor's administration and CDPH staff assured CHA and other stakeholders, during the negotiations regarding the bill, that the language of Health and Safety Code Section 1280.15 that is highlighted in yellow below meant that the statute does not constitute a strict liability statute. Instead, the health care facility must be found by CDPH to have been negligent with respect to the implementation of appropriate administrative, technical, or physical safeguards 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. I was present at and participated in all major 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 woud be interpreted to impose fines on health care facilities only if they failed to implement proper administrative, technical and physical safeguards. 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.

I have attached contemporaneous corroboration of this interpretation of the meaning of the language that is highlighted above — 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."

As you know, 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 H&S 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.

Specific Sections

Section 79900. Applicability.

As a technical matter, I believe the term "health facility" and "facility" in paragraph (b) should be changed to "health care facility" for consistency and accordance with the definitions used in this regulation package.

Section 79901. Definitions.

79901(a). Access – 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."

79901(b)(1)(A). 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…"

79901(b)(1)(B). 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…"

79901(c). Business associate – 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."

79901(f). Detect – This definition lacks clarity. CHA 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.

We note that Health and Safety Code Section 1280.15 requires the reporting of "breaches," not incidents that may possibly be breaches. The Department lacks the statutory authority to require the reporting of incidents that might possibly be breaches, but are not. If determining whether an incident constitutes a breach were simple, it would not be unreasonable to start the clock ticking when a facility has a reasonable belief that a breach has occurred. However, because state and federal health information privacy laws are complicated, electronic health record and other information technology is very complicated, and the reporting timeline is so short, the clock should start ticking only when the facility has determined that a breach indeed occurred.

In addition, Health and Safety Code Section 1280.15 did not give CDPH the authority to regulate business assoicates, and did not give CDPH the authority to make health care facilities responsible for the acts or omissions of business associates. Indeed, state law contains no such concept as "business associate."

Finally, we note that this provision is inconsistent with HIPAA. Under HIPAA, a business associate's discovery of a breach is imputed to the covered entity only when the business associate is acting as an agent of a covered entity. HIPAA provides that:

1. Where the business associate is an agent of the covered entity, the clock starts when the business associate detects the breach.
2. Where the business associate is not an agent of the covered entity, but is only an independent contractor, then the clock starts when the business associate notifies the covered entity. (See 45 C.F.R. Section 164.404(a)(2); 74 Fed.Reg. 42740 and 42754 (Aug. 24, 2009).)

CHA 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 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 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~~."

79901(i). External factors - CHA objects to the inclusion of a definition of "external factors." The Legislature, in Health and Safety Code Section 1280.15, directed CDPH to:

> consider the clinic's, health facility's, agency's, or hospice's history of compliance with this section and other related state and federal statutes and regulations, the extent to which the facility detected violations and took preventative action to immediately correct and prevent past violations from recurring, and ***factors outside its control*** that restricted the facility's ability to comply with this section. (emphasis added)

The Legislature did not direct CDPH to restrict its consideration to only "external" factors outside the health care facility's control. It directed CDPH to consider <u>all</u> 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, but deliberately disregarded their training and committed a breach of patient medical information anyway. (See discussion under heading of "Strict Liability vs. Negligence Standard" on page 1.) It was also intended to include thieves and other criminals. We suggest revising this definition as follows:

~~"External factors"~~ "<u>Factors outside the control of the health care facility"</u> 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. "External factors" does not include the acts of the health care facility, business associate, or their respective workforce members."~~ <u>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.</u>

79901(j). Health care facility – this definition includes "business associates" within the definition of "health care facility." This inclusion makes clinics, health facilities, home health agencies, and hospices responsible for breaches of their business associates. This is manifestly beyond CDPH's statutory

authority. There is no evidence whatsoever that the Legislature intended to make hospitals or other health care facilities responsible for reporting medical privacy breaches by their business associates (law firms, accounting firms, consultants, accreditation agencies, etc.). If the Legislature had intended to do this, it would have included language in Health and Safety Code Section 1280.15 doing so, and would have given CDPH the authority to investigate these types of businesses. The problems with this definition are compounded by the proposed definition of "business associate" (see our comments on this above). These proposed regulations, if these definitions are not corrected, would require every clinic, health facility, home health agency, or hospice that has a contract with Blue Cross to report to CDPH every breach that Blue Cross experiences, within 15 days of Blue Cross's detection of the incident. This is clearly not what the Legislature said, nor what it intended. CHA 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 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 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~~."

79901(l). Medical information -- CHA suggests referring to the definition of "medical information" in Civil Code Section 56.05, instead of copying the entire definition into the regulation. If the Legislature changes Civil Code Section 56.05 in the future, the regulation and the statutory definition could become inconsistent, leading to confusion. We suggest revising this definition as follows: "'Medical information' shall have the meaning of the term as provided for in Section 56.05 of the California Civil Code."

79901(p). Workforce -- We strongly urge CDPH to adopt the exact HIPAA definition of "workforce." It is inapproporiate to include the medical staff in the definition of "workforce," because in California, a health care facility is prohibited by state law (the corporate practice of medicine doctrine) from controlling the action of independent medical professionals. In addition, including medical staff and their employees in the definition of "workforce" would mean that hospitals would become responsible for the actions of the staff in doctor's offices in the community. The California Legislature did not include doctor's office employees in SB 541.

Section 79902. Breach Reporting Requirements.
79902(a). The proposed language purports to require health care facilities to report to CDPH suspected breaches. However, the Legislature gave CDPH the authority to require reporting only of actual breaches, not "suspected" breaches. The language of the statute says:

> (b) (1) A clinic, health facility, home health agency, or hospice to which subdivision (a) applies shall report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information to the department…

Therefore, the words "or a suspected breach" should be deleted from the proposed regulation to comply with the "authority" requirement of the Administrative Procedure Act, Government Code Section 11346 *et seq.* In addition, the term "suspected breach" is vague and ambiguous, and subject to varying interpretations. It therefore does not comply with the "clarity" requirement of the Administrative Procedure Act, Government Code Section 11346 *et seq.*

Also, this provision purports to require business associates of clinics, health facilities, home health agencies, and hospices to report breaches to CDPH. As noted above, the language of 77902(a) states that "A health care facility shall report to the Department a breach…" Because a "health care facility" is defined in proposed Section 77901 to include business associates, then all business associates would be required to report breaches to CDPH. However, the Legislature did not give CDPH the statutory authority to require business associates — such as law firms, accounting firms, consultants, accreditation agencies, etc. — to report breaches to CDPH. This provision vastly exceeds CDPH's statutory authority in violation of the Administrative Procedure Act, Government Code Section 11346 *et seq.* This problem can be solved by revising the definition of "health care facility" as noted in our comments above.

79902(a)(1). 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 acknowledges this fact in the Initial Statement of Reasons and Section 79902(a)(3), where it requires health facilities to report information relevant to the breach as it becomes available after the 15 days. CDPH should also acknowledge this by amending Section 79902(a)(1) as follows: "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 <u>to the extent known …"</u>

79902(a)(1)(D). CHA 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. Keeping patient names as private as possible is especially important where the health care facility is an acute psychiatric hospital.

79902(a)(1)(F). 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." However, 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* (*Dorothy Atkins et al., Real Parties in Interest),* the California appellate court stated that "No breach of confidentiality takes place until an unauthorized person views the medical information." CHA 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 — as the courts have decided — then this provision should be deleted from the proposed regulation.

79902(a)(1)(G). CHA 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.

79902(a)(1)(K). 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. CHA 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.

79902(a)(1)(M). 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. CHA 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."

79902(a)(2). CHA suggests that this provision be revised as follows: "A health care facility shall report any additional significant information relevant to the breach, as it becomes available…"

79902(a)(3). This provision ***requires*** CDPH to assess a late fee penalty. The authorizing statute, however, gives CDPH the ***authority*** to assess a late fee penalty, but does not ***require*** CDPH to do so in every case. The word "shall" must be changed to the word "may" to align with CDPH's statutory authority.

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. 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."

79902(b). This provision requires a health care facility to notify a patient or "patient's representative" of a breach. However, the term "patient's representative" is undefined. CHA strongly urges CDPH to clearly define this term. This term, if undefined, renders this provision of the regulation unclear in violation of the Administrative Procedure Act, Government Code

Section 11346 *et seq.* Specifically, Government Code Section 11349(c) defines "clarity" to mean "written or displayed so that the meaning of regulations will be easily understood by those persons directly affected by them." This regulation does not clarify when a health care facility must notify a patient representative instead of the patient, or who is considered a patient representative. Health care facility employees tasked with notifying patients/patient representatives and CDPH surveyors tasked with enforcing the regulation, both need clarity on these crucial questions. It is important to keep in mind that if a health care facility were to notify the wrong person of a breach, this could constitute an additional breach. Clarify is needed to avoid this potential error.

Section 79903. Administrative Penalties.
79903(a). This provision incorrectly interprets Health and Safety Code Section 1280.15. (See the discussion above under "Strict Liability vs. Negligence Standard," 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 appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information."

79903(b). 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. CHA 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.

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. This provision should be revised to do so.

79904. Penalty Adjustment Factors.
77904. 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.

79904(a)(4). CHA 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.

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) 552-7611.

Sincerely,

Lois J. Richardson
Vice President and Legal Counsel