State of California—Health and Human Services Agency
California Department of Public Health

**Dr. Sonia Angell**
*Director and State Public Health Officer*

**GAVIN NEWSOM**
*Governor*

**NOTICE OF PROPOSED RULEMAKING**
**Title 22. Social Security**
**DPH-11-009 Medical Information Breach**
**Notice Published: July 3, 2020**

Notice is hereby given that the California Department of Public Health (Department) is proposing the regulation described below. This notice of proposed rulemaking commences a rulemaking to make the regulations permanent after considering all comments, objections, and recommendations regarding the regulation.

## PUBLIC PROCEEDINGS

The Department is conducting a 45-day written public proceeding during which time any interested person or such person's duly authorized representative may present statements, arguments or contentions (all of which are hereinafter referred to as comments) relevant to the action described in the Informative Digest/Policy Statement Overview section of this notice.

To request copies of the regulatory proposal in an alternate format, please write or call: Hannah Strom-Martin, Office of Regulations, 1415 L Street Suite 500, Sacramento, CA 95814, at (916) 440-7371, email to hannah.strom-martin@cdph.ca.gov or use the California Relay Service by dialing 711.

## WRITTEN COMMENT PERIOD

Written comments pertaining to this proposal, regardless of the method of transmittal, must be received by Office of Regulations by 5:00 p.m. on August 18, 2020, which is hereby designated as the close of the written comment period. Comments received after this date will not be considered timely.

Written comments may be submitted as follows:

1. By email to: regulations@cdph.ca.gov. It is requested that email transmission of comments, particularly those with attachments, contain the regulation package identifier "DPH-11-009 Medical Information Breach" in the subject line to facilitate timely identification and review of the comment;
2. By fax transmission to: (916) 319-9821;
3. By postal service or hand delivered to: California Department of Public Health, Office of Regulations, 1415 L Street, Suite 500, Sacramento, CA 95814.

All submitted comments should include the regulation package identifier, **"DPH-11-009 Medical Information Breach,"** along with the commentor's name and email or mailing address.

## PUBLIC HEARING

A public hearing has not been scheduled for this rulemaking. However, the Department will conduct a hearing if a written request for a public hearing is received from any interested person, or his or her duly authorized representative, no later than 15 days prior to the close of the written comment period, pursuant to Government Code Section 11346.8.

## ASSISTIVE SERVICES

For individuals with disabilities, the Department will provide assistive services such as the conversion of written materials into Braille, large print, audiocassette, and computer disk. For public hearings, assistive services can include sign-language interpretation, real-time captioning, note takes, reading or writing assistance. To request these assistive services, please call (916) 558-1710 or (California Relay at 711 or 1-800-735-2929), email regulations@cdph.ca.gov, or write to the Office of Regulations at the address noted above. Note: The range of assistive services available may be limited if requests are made less than 10 business days prior to a public hearing.

## AUTHORITY AND REFERENCE

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

## INFORMATIVE DIGEST/POLICY STATEMENT OVERVIEW:

### Summary of Proposal

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

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

### Background

The Department has regulatory oversight for more than 30 types of health care facilities and providers and approximately 10,000 facilities. The proposed regulations relate to the Department's assessment of administrative penalties for breaches of patient medical information by these health care facilities. Breaches of patient medical information are a serious national problem. One study found that 94% of hospitals

experienced data breaches between the years 2010 and 2012. [1] In California alone, the Department received an estimated 8,400 reported breaches between January 1, 2016 and December 31, 2017. These proposed regulations clarify how the Department will enforce the Code.

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

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

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

**Anticipated Benefits**

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

**EVALUATION AS TO WHETHER THE PROPOSED REGULATION ARE INCONSISTENT OR INCOMPATIBLE WITH EXISTING STATE AND FEDERAL REGULATIONS**
The Department has determined that the proposed regulations are compatible and consistent with existing state and federal laws. Under the Health Insurance Portability and Accountability Act (HIPAA), the federal government has established provisions relating to medical information breaches. In drafting these proposed regulations, the Department has extensively used the HIPAA regulations as a model for developing its own. However, in some cases the HIPAA provisions differ from the final regulations proposed herein. These differences are often the result of variation between existing state and federal law as they relate to privacy and medical information (i.e. differences between underlying statutorily defined terms). In other cases, the Department has modeled its regulations after HIPAA regulations, but constructed them differently when

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

the Department finds such changes are in the best interest of the people of California. HIPAA's provisions are meant to be a "floor" for patient protection standards, and a state may enact its own laws and regulations under certain circumstances, including, but not limited to, when the state's law provides greater protection. (45 C.F.R. §§ 160.201-205 (2013).) Therefore, the Department concludes that the proposed regulations are consistent with existing state and federal laws.

**FORMS INCORPORATED BY REFERENCE**
None.

**MANDATED BY FEDERAL LAW OR REGULATIONS**
Not applicable.

**OTHER STATUTORY REQUIREMENTS**
Not applicable.

**LOCAL MANDATE**
The Department has determined that this regulatory action would not impose a 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.

## DISCLOSURES REGARDING THE PROPOSED ACTION

**FISCAL IMPACT ESTIMATES**

**A) Cost to any local agencies or school districts that must be reimbursed pursuant to Section 17561 of Government Code:**
The proposed regulations do not impose costs on any local agency or school district for which reimbursement would be required pursuant to part 7 (commencing with section 17500) of division 4 of the Government Code.

**B) The cost or savings to any state agency:**
The Department estimates that the overall effect will be cost neutral as affected regulated entities are already paying the financial penalties as appropriate under existing statutes. State operated facilities may receive fines if they fail to comply with patient medical information requirements.

**C) Impact on any cost or savings in federal funding of the program:**
There is no federal funding affected by the proposed regulatory action.

**D) Other nondiscretionary costs or savings imposed on local agencies:**
The proposed regulations do not impose other nondiscretionary costs or savings on any local agencies.

**HOUSING COSTS**

The Department has determined that the regulations will not have an impact on housing costs.

**SIGNIFICANT STATEWIDE ADVERSE ECONOMIC IMPACT DIRECTLY AFFECTING BUSINESS, INCLUDING ABILITY TO COMPETE**

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

**STATEMENT OF THE RESULTS OF THE ECONOMIC IMPACT ASSESSMENT**

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

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

**COST IMPACTS ON REPRESENTATIVE PERSON OR BUSINESS**

The Department is not aware of any cost impacts that a representative private person or business would necessarily incur in reasonable compliance with the proposed action.

**BUSINESS REPORTING REQUIREMENT**

The proposed regulations require health care facilities to report to the Department details regarding unlawful or unauthorized access to patients' medical information. The Department has found that this is necessary for the health, safety, and welfare of the people of the state.

## EFFECT ON SMALL BUSINESS

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

## SPECIFIC TECHNOLOGIES OR EQUIPMENT

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

## ALTERNATIVES CONSIDERED

In accordance with Government Code section 11346.5, subdivision (a)(13), the Department has determined that no reasonable alternative it considered or that has otherwise been identified and brought to the attention of the agency would be more effective in carrying out the purpose for which the action is proposed or would be as effective and less burdensome to affected private persons than the proposed action or would be more cost-effective to affected private persons and equally effective in implementing the statutory policy or other provision of law.

The Department invites interested persons to present statements or arguments with respect to the proposed regulations at the scheduled hearing or during the written comment period.

## TECHNICAL, THERETICAL, AND/OR EMPIRICAL STUDIES, REPORTS OR DOCUMENTS RELIED UPON

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

## CONTACT PERSON

Inquiries regarding the substance of the proposed regulations described in this notice may be directed to Krisheidy Guerrero, email krisheidy.guerrero@cdph.ca.gov, phone (916) 327-0643. All other inquiries concerning the action described in this notice may be directed to Hannah Strom-Martin, Office of Regulations, at (916)440-7371, email hannah.strom-martin@cdph.ca.gov, or to the designated backup contact, Christy Correa, at (916) 440-7764, email christy.correa@cdph.ca.gov.

## AVAILABILITY STATEMENTS

The Department has prepared and has available for public review an initial statement of reasons for the proposed regulations, all the information upon which the proposed regulations are based, and the text of the proposed regulations. The Office of Regulations, at the address previously noted, will be the location of public records, including reports, documentation, and other material related to the proposed regulations.

In order to request that a copy of this public notice, the regulation text, and the initial statement of reasons or alternate formats for these documents be mailed to you, please call (916) 440-7371 (or the California Relay Service at 711), or send an email to regulations@cdph.ca.gov, or write to the Office of Regulations at the address previously noted. Upon specific request, these documents will be made available in Braille, large print, audiocassette, or computer disk.

The full text of any regulation which is changed or modified from the express terms of the proposed action will be made available by the Department's Office of Regulations at least 15 days prior to the date on which the Department adopts, amends, or repeals the resulting regulation.

A copy of the final statement of reasons when prepared will be available upon request from the Office of Regulations.

## INTERNET ACCESS

Materials regarding the action described in this notice (including this public notice, the text of the proposed regulations, and the initial statement of reasons) that are available via the Internet may be accessed at www.cdph.ca.gov and by clicking on the following: Programs, Office of Regulations, and the Proposed Regulations link.