



NOTICE OF PROPOSED EMERGENCY RULEMAKING ACTION

Title 22, California Code of Regulations
Sections 97177.15 and 97224

The Office of Statewide Health Planning and Development (“the Office”) proposes to use the emergency rulemaking process to amend two sections in current regulations that relate to the transmission of confidential patient information in order to delete a regulatory requirement to use a data encryption system that may have security vulnerability.

Government Code section 11346.1(a)(2) requires that, at least five working days prior to submission of the proposed emergency action to the Office of Administrative Law, the adopting agency provide a notice of the proposed emergency action to every person who has filed a request for notice of regulatory action with the agency. After submission of the proposed emergency to the Office of Administrative Law, the Office of Administrative Law shall allow interested persons five calendar days to submit comments on the proposed emergency regulations as set forth in Government Code section 11349.6.

At the conclusion of the five working day notice period, the Office will submit the proposed emergency regulations to the Office of Administrative Law.

Specific language proposed to be adopted:

§ 97177.15. Method of Data Transmission.

For discharges beginning January 1, 2009:

A hospital shall use the CORC system for transmitting reports, utilizing a Microsoft supported version of the Internet Explorer web browser that supports a secure Internet connection utilizing the Secure Hypertext Transfer Protocol (HTTPS or https) and 128-bit cipher strength Secure Socket Layer (SSL) through either:

- (a) Online transmission of a report as an electronic data file, or
- (b) Online entry of individual records as a batch submission.

Authority cited: Section 128810, Health and Safety Code.

Reference: Section 128745, Health and Safety Code.

§ 97244. Method of Submission.

(a) Reporting facilities shall use the MIRCAl system for submitting reports. Data shall be reported utilizing a Microsoft supported version of the Internet Explorer web browser ~~that supports a secure Internet connection utilizing the Secure Hypertext Transfer Protocol (HTTPS or https) and 128-bit cypher strength Secure Socket Layer (SSL)~~ through either:

- (1) Online transmission of data reports as electronic data files, or
- (2) Online entry of individual records.

Authority cited: Section 128755, Health and Safety Code.

Reference: Sections 128735, 128736 and 128737, Health and Safety Code.

Finding of Emergency:

These regulations are being amended on an emergency basis to avoid serious harm to the public peace, health, safety, or general welfare.

Description of Specific Facts Demonstrating the Existence of an Emergency and the Need for Immediate Action

California law (Health and Safety Code Sections 128735(g), 128736, 128737, and 128745(c)) requires that hospitals and licensed freestanding ambulatory surgery centers file certain information with the Office of Statewide Health Planning and Development about patients receiving medical care in their facilities. The reported information includes identifiable confidential medical information. Data are filed using mandatory on-line reporting systems that require use of data encryption.

The Office has existing regulations that define the methods of data transmission/-submission using those on-line systems. These regulations – sections 97177.15 and 97244 of Title 22 - specify use of a Microsoft Internet Explorer web browser that supports a secure Internet connection utilizing HTTPS and Secure Socket Layer (SSL) technology, an encryption technology.

SSL technology has become outdated and has recently been found to have security vulnerability. On January 8, 2015, the Office received a notice from the Department of Technology that in order to fully remediate the SSL security vulnerability, OTech will completely disable SSL. All OTech client departments, including the Office, will be required to instead use the replacement encryption technology, Transport Layer Security (TLS), which is now standard. This remediation will start February 13, 2015.

The Office must immediately amend the two regulatory sections that require use of SSL technology in order to avoid mandating use of an outdated technology with security vulnerabilities by facilities that are reporting identifiable patient medical information to the Office. This is necessary both to protect patient privacy and to comply with the OTech remediation requirement.

The proposed regulatory changes to sections 97244 and 97177.15 will delete the regulatory text containing the browser requirements that include SSL. The regulatory text is also modified to require that a Microsoft supported version of Internet Explorer be used; while older versions of Internet Explorer that are no longer supported by Microsoft may only accept SSL, the supported versions of Internet Explorer will accept TLS.

In addition to being dangerously outdated, the references to the browser system requirements including SSL are also unnecessary. The current on-line reporting systems - MIRCal and CORC - require the use of data encryption and can be used with SSL, but can also be used with TLS, the more current standard. Because use of the MIRCal and CORC systems for on-line reporting is separately mandated in the regulations, and each of these systems requires data encryption, there is no need to list the encryption requirement in sections 97244 and 97177.15.

Approximately 16.6 million patient records are transmitted to the Office over the course of each year. These regulatory changes must be made immediately to prevent a serious security risk to medical privacy that could impact millions of Californians. Exposure of their personal medical information would cause serious harm to the public health, safety, and general welfare. Delaying action to allow for the standard notice and comment period would be inconsistent with the public interest; each additional period of delay could put additional records and patients at risk.

Informative Digest

1. Summary of Existing Law and Regulations and the Effect of the Proposed Rulemaking

Hospitals and freestanding ambulatory surgery clinics licensed by the California Department of Public Health are required by law to file certain patient-level information with the Office at specified intervals.

Health and Safety Code section 128735, subdivision (g), requires that each hospital file a Hospital Discharge Abstract Data Record for each patient discharged from the hospital. Health and Safety Code section 128736 requires that each hospital file an

Emergency Care Data Record for each patient encounter in a hospital emergency department, and Health and Safety Code section 128737 requires that each general acute hospital and licensed freestanding ambulatory surgery center file an Ambulatory Surgery Data Record for each patient encounter during which at least one ambulatory surgery procedure is performed. These three programs are often referred to as the patient data programs.

In addition, Health and Safety Code section 128745, subdivision (c), requires that each hospital at which Coronary Artery Bypass Graft (CABG) surgery is performed file a patient data record for each patient on whom CABG surgery is performed. This specific program is referred to as the California CABG Outcomes Reporting Program (CCORP), as the data are used to produce reports on outcomes of care.

Each of the patient data records reported to the Office in these four programs includes a set of data elements that are specified in statute and/or regulation. The data records include individually identifiable medical information.

The patient records are submitted to the Office electronically. The patient data programs use the MIRCal system for online reporting (22 CCR §97212) and the CABG program uses the CORC system for online reporting (22 CCR §97170). The Office many years ago also adopted regulations that specify the method of electronic data submission using these systems - Title 22, CCR, §97244 for MIRCal and Title 22, CCR, §97177.15 for CORC.

Each of these sections specifies use of a Microsoft Internet Explorer web browser that supports a secure Internet connection utilizing HTTPS and Secure Socket Layer (SSL) technology, an encryption technology. As explained above, the Office is proposing to delete the outdated requirements to use SSL. One other small change is made -- because older versions of the Microsoft Internet Explorer browser that are no longer supported by Microsoft may only accept SSL, the text is also modified to require that a Microsoft supported version of Internet Explorer be used; current versions will accept TLS.

The current MIRCal and CORC systems require the use of data encryption. Currently, they can be used with SSL, but also can be used with TLS, the more current standard. Because use of the MIRCal and CORC systems for on-line reporting is separately mandated in regulations, and each of these systems requires data encryption, there is no need to list the encryption requirements in sections 97244 and 97177.15.

Healthcare facilities today all must have the capacity to transmit identifiable patient health information securely, including the use of encryption technology. SSL is outdated technology, and the industry standard is now TLS. In today's healthcare environment, it can reasonably be presumed that health facilities that transmit data to the Office have the capacity to submit data using the more current TLS standard. The Office must make sure it does not specifically mandate the use of the less secure technology.

2. Policy Statement Overview

The Health and Safety Code provisions requiring that patient data be reported to the Office also require that the Office protect patients' rights of confidentiality. In light of these specific provisions, as well as the California Information Practices Act of 1977 (Civil Code section 1798 et seq.), the Office must at all times insure that the systems used to collect and store confidential patient information are secure consistent with current technological capabilities and healthcare industry practice.

3. Evaluation of Inconsistency/Incompatibility with Existing State Regulations

As required by Government Code section 11346.5, subdivision (a)(3)(D), the Office evaluated the language contained in the proposed amendments. The Office has determined that these proposed regulations are not inconsistent with or incompatible with existing state regulations. These regulations relate to existing programs.

Local Mandate Determination and Cost Estimates: The Office has determined that the regulation does not impose a mandate on local agencies or schools districts.

OSHPD has made the following estimates:

- a. Cost or savings to any state agency: None.
- b. Cost to any local agency or school district which must be reimbursed in accordance with Government Code sections 17500 through 17630: None
- c. Other nondiscretionary cost or savings imposed on local agencies: None
- d. Cost or savings in federal funding to the state: None.

Availability of Documents on the Internet

Copies of the Notice of Proposed Emergency Action and the text of the regulations in underline and strikeout can be accessed through our website at

<http://www.oshpd.ca.gov/LawsRegs/NewRegulations.html>

Contact Information

Any questions or concerns may be addressed to:

Stephen Pollitt
Information Security Officer
Office of Statewide Health Planning and Development
400 R Street, Room 338
Sacramento, CA 95811
Phone: (916) 326-3620
Email: stephen.pollitt@oshpd.ca.gov
Web: <http://www.oshpd.ca.gov>

January 26, 2015