



Initial Statement Of Reasons

Title 22, California Code of Regulations
Sections 97177.15 and 97244

Background Information

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.

Until the emergency regulations went into effect, February 9, 2015, each of these sections specified 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.

Problem Statement

SSL technology has become outdated and has been found to have security vulnerability.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 would 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 began February 13, 2015.

To deal with the security vulnerability, with the attendant risk to patient privacy, the Office needed to delete the outdated requirements to use SSL.

Purpose and Benefits of this Regulatory Action

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.

The Office is proposing to permanently amend the two regulatory sections that require use of SSL encryption 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. The amended regulations provide greater protection of data confidentiality and patient privacy.

Specific Purpose of Each Amendment

Section 97177.15: The specific proposed regulatory changes to section 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 system - CORC - requires 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 CORC system for on-line reporting is separately mandated in the regulations, and the system requires data encryption, there is no need to list the encryption requirement in section 97177.15.

Section 97244: The specific proposed regulatory changes to section 97244 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 system - MIRCal - requires 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 system for on-line reporting is separately mandated in the regulations, and the system requires data encryption, there is no need to list the encryption requirement in section 97244.

Necessity

It is necessary to amend both Section 97177.15 and Section 97244, 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.

Approximately 16.6 million patient records are transmitted to the Office over the course of each year. These regulatory changes are necessary 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.

Economic Impact Assessment

Repeal of the mandate to use the outdated SSL encryption technology when filing patient data with the Office is not anticipated to impose any new costs on the reporting facilities.

Therefore, the Office concludes that this regulatory action will not affect the following:

- The creation of jobs within the state
- The elimination of jobs within the state
- The creation of new businesses within the state
- The elimination of existing businesses within the state
- The expansion of businesses currently doing business in the state

The benefit to the public is that patient privacy will be more stringently protected.

Technical, Theoretical, and Empirical Study, Reports, or Similar Documents Relied Upon

The Office did not rely upon any technical, theoretical, and empirical studies, reports, or similar documents in proposing the amendment of these regulations.

Reasonable Alternatives

The Office has not identified any alternatives to the proposed regulation that would be less burdensome and equally effective in achieving the purpose of the regulation, and no alternatives have otherwise been identified and brought to the attention of the Office.

The Office has not identified any reasonable alternatives to the proposed regulatory action, including alternatives that would lessen any adverse impact on small business. There is no anticipated adverse impact on small business.

Evidence Supporting Finding of No Significant Adverse Economic Impact on Business

The Office has made an initial determination that permanent adoption of the proposed regulations would not have a significant adverse economic impact on business because it is not anticipated to impose any costs on business. 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.