

CHPSO

California Hospital Patient Safety Organization (CHPSO)

Contract and information package

Instructions to sign up.....	2
About CHPSO.....	3
Privilege of Patient Safety Work Product.....	4
Confidentiality of Patient Safety Work Product.....	5

Instructions to sign up

Hospitals desiring to participate with CHPSO need to sign the [CHPSO—Participating Hospital Agreement](#) (click on link to obtain a copy of the agreement).

Patient Safety Organizations (PSO) are highly regulated, and most information that enters the patient safety evaluation system becomes patient safety work product (PSWP) and is confidential and privileged. The privilege is effective in all federal, state, local and tribal venues, both criminal and administrative. PSWP is not subject to subpoena, order, discovery, disclosure (e.g., FOIA requests), and cannot be admitted as evidence. It also cannot be admitted in a professional disciplinary proceeding of a body established or specifically authorized under state law.

The definition of PSWP is quite broad. Patient safety work product includes any data, reports, records, memoranda, analyses (such as root cause analyses), or written or oral statements (or copies of any of this material), which could improve patient safety, health care quality, or health care outcomes, that are assembled or developed by a provider for reporting to a PSO and are reported to a PSO. It also includes information that is documented as within a patient safety evaluation system that will be sent to a PSO and information developed by a PSO for the conduct of patient safety activities.

However, patient safety work product does not include a patient's medical record, billing and discharge information, or any other original patient or provider information; nor does it include information that is collected, maintained, or developed separately, or exists separately, from a patient safety evaluation system.

Participating providers need to follow the PSO regulation when protecting and sharing PSWP. For example, PSWP received from another provider can only be used for internal patient safety improvement efforts.

The contract contains three main sections: the main contract, a business associate agreement, and a workforce confidentiality agreement.

The main agreement embodies the rules of the PSO law and regulation and adds clauses appropriate to the planned CHPSO-hospital relationship. Much of the contract is educational in nature, as the requirements would exist even in the absence of any such clauses in the agreement.

The business associate agreement is pursuant to the HIPAA requirements. The PSO regulation does not alter the HIPAA responsibilities other than stating that, by definition, PSOs are HIPAA business associates of providers and their activities represent health care operations.

The workforce confidentiality agreement is only used when a person provides services for CHPSO. That person then signs a copy of the confidentiality agreement. This would occur, for example, when a person participates on a CHPSO advisory committee and in that capacity reviews PSWP from other providers. However, all persons participating in PSO activities need to understand the PSWP (and HIPAA) confidentiality protections. The sample Confidentiality of Patient Safety Work Product handout, included in this packet, may be used to educate employees.

About CHPSO

The California Hospital Patient Safety Organization (CHPSO), created by the California Hospital Association after approval from the board of directors, has received approval by HHS and is now listed by the Agency for Healthcare Research and Quality (AHRQ) as a Patient Safety Organization (PSO). CHPSO is the second organization in the nation to receive this designation. The list of approved PSOs is located at <http://www.pso.ahrq.gov/listing/psolist.htm>.

Until passage of the Patient Safety and Quality Improvement Act of 2005 (PSQIA), we did not have the appropriate tools to address systems issues and disseminate information learned from safety events. Quality improvement activities tended to be regulated by state laws, which generally addressed peer review of the qualifications and skills of individual practitioners. Systems review, and the types of activities that benefit systems learning, were not protected by the state laws. The lack of protection inhibited reporting and learning from these failures.

Systems failures, unlike individual failures, are often best addressed by sharing the experience with others (e.g., other hospitals). The PSQIA recognizes this, and created PSOs as a method of sharing and analyzing information within a sphere of confidentiality for both patient and provider, and privilege from discovery.

CHPSO's distinct advantage over other PSOs will be its focus on the laws, regulations and patient safety initiatives specific to California. Additionally, CHPSO will coordinate its efforts with the Regional Hospital Associations and existing patient safety collaboratives across the state. Hospitals sharing a common market area will be able to work together and focus their patient safety and quality improvement efforts on issues relevant to their community.

CHPSO will help hospitals evaluate errors and develop effective strategies to improve patient safety. It also will develop and disseminate information with respect to improving patient safety, such as recommendations, protocols, or information regarding best practices. In addition, CHPSO will help standardize reporting and accountability measures, improve the public's trust in hospitals and increase efficiency.

Privilege of Patient Safety Work Product

From 42CFR3.204:

(a) **Privilege.** Notwithstanding any other provision of Federal, State, local, or Tribal law and subject to paragraph (b) of this section and § 3.208 of this subpart, **patient safety work product shall be privileged and shall not be:**

(1) **Subject to a** Federal, State, local, or Tribal civil, criminal, or administrative **subpoena or order**, including in a Federal, State, local, or Tribal civil or administrative disciplinary proceeding against a provider;

(2) **Subject to discovery** in connection with a Federal, State, local, or Tribal civil, criminal, or administrative proceeding, including in a Federal, State, local, or Tribal civil or administrative disciplinary proceeding against a provider;

(3) **Subject to disclosure** pursuant to section 552 of Title 5, United States Code (commonly known as the Freedom of Information Act) or any other similar Federal, State, local, or Tribal law;

(4) **Admitted as evidence** in any Federal, State, local, or Tribal governmental civil proceeding, criminal proceeding, administrative rulemaking proceeding, or administrative adjudicatory proceeding, including any such proceeding against a provider; or

(5) **Admitted in a professional disciplinary proceeding** of a professional disciplinary body established or specifically authorized under State law.

(b) **Exceptions to privilege.** Privilege shall not apply to (and shall not be construed to prohibit) one or more of the following disclosures:

(1) Disclosure of relevant patient safety work product for use in a criminal proceeding [but only after a court makes an *in camera* determination that such patient safety work product contains evidence of a criminal act and that such patient safety

work product is material to the proceeding and not reasonably available from any other source].

(2) Disclosure to the extent required to [protect from retaliation a person who reports patient safety information].

(3) Disclosure pursuant to provider authorizations subject to the [requirements for recording valid authorizations from all identified providers].

(4) Disclosure of non-identifiable patient safety work product....

(c) **Implementation and enforcement by the Secretary.** Privilege shall not apply to (and shall not be construed to prohibit) disclosures of relevant patient safety work product to or by the Secretary if such patient safety work product is needed to investigate or determine compliance, or to seek or impose civil money penalties, with respect to this part or the HIPAA Privacy Rule, or to make or support decisions with respect to listing of a PSO.

* * *

§ 3.208 Continued protection of patient safety work product.

(a) Except as provided in paragraph (b) of this section, **patient safety work product disclosed in accordance with this subpart, or disclosed impermissibly, shall continue to be privileged and confidential.**

(b)(1) Patient safety work product disclosed for use in a criminal proceeding ... continues to be privileged, but is no longer confidential.

(2) Non-identifiable patient safety work product that is disclosed is no longer privileged or confidential and not subject to the regulations under this part.

(3) Paragraph (b) of this section applies only to the specific patient safety work product disclosed.

Confidentiality of Patient Safety Work Product

Information for Providers and PSO Workforce

Patient Safety Work Product must not be disclosed, except in very specific circumstances and subject to very specific restrictions. The most relevant exceptions for healthcare providers and PSO workforce members are as follows:

Note: the Patient Safety Activities Exception (see bold text below) is the most common one that providers and PSOs will be working with. Disclosures pursuant to the other exceptions should have prior review by counsel or other knowledgeable party before permitting any disclosure.

PERMITTED DISCLOSURES

- **Patient Safety Activities – PSWP may be disclosed:**
 - **Between the Provider and the PSO – i.e.:**
 - **From the provider to the PSO, for Patient Safety Activities, and**
 - **From the PSO to the disclosing provider, for Patient Safety Activities**
 - **To a contractor of a Provider or a PSO**
 - **For contracted Patient Safety Activities**
 - **Contractor may not further disclose, except back to the contracted provider or PSO**
 - **Among affiliated providers, for Patient Safety Activities**
 - **From one PSO to another PSO or another provider, *if***
 - **Direct identifiers (which are defined in the regulations) of any providers, affiliated organizations, corporate parents, subsidiaries, practice partners, employers, members of the workforce, or household members of such providers are removed; and**
 - **With respect to any Individually identifiable health information within the PSWP, direct identifiers (a limited data set, defined by regulation) are removed**
 - **See table at end for list of direct identifiers**
- **Business operations** – A provider or PSO may disclose to attorneys, accountants or other professionals for business operations purposes.
 - Further disclosure (except back to the contracting entity) is prohibited
- **Authorized by identified providers** – Disclosure is permitted if all identified providers authorize the disclosure.
 - Authorization must be in writing, signed by the provider, and
 - Must state the nature and scope of the disclosure
- **Accrediting bodies** – PSWP may be (but is not required to be) disclosed to an accrediting body if:
 - Any identified provider agrees to the disclosure; or
 - Direct identifiers of any provider (or affiliated organizations, corporate parents, subsidiaries, practice partners, employers, members of the workforce, or household members) are removed

- **Nonidentifiable PSWP** – May be disclosed.
 - The regulations set out specific requirements for “nonidentification.”
- **Research** – This exception allows disclosure to researchers conducting certain types of research projects. If protected health information is involved, HIPAA also applies.
- **Food and Drug Administration** – PSWP may be disclosed to the FDA:
 - By a provider concerning an FDA-regulated product or activity,
 - By an entity required to report to the FDA about the quality, safety, or effectiveness of an FDA-regulated product or activity, or
 - By a contractor acting on behalf of the FDA or entity for these purposes
- **Law enforcement** – PSWP may be disclosed to law enforcement personnel if:
 - The PSWP contains evidence of a criminal act;
 - The PSWP is material to the proceedings; and
 - The PSWP is not reasonably available from any other source
- **Criminal proceedings** – But only after a court makes an *in-camera* (in closed chambers) determination that:
 - If the information relates to an event that either constitutes the commission of a crime, or for which the disclosing person reasonably believes constitutes the commission of a crime, provided that the disclosing person believes, reasonably under the circumstances, that the patient safety work product that is disclosed is necessary for criminal law enforcement purposes.
 -
- **Disclosure to permit equitable relief for reporting individuals** – This exception allows use of PSWP by individuals who claim they have been the victim of an adverse employment action because the individual reported information to a PSO (either directly to the PSO or with the intent of having it reported to the PSO).
 - There must be a “protective order” issued by the court or administrative tribunal to protect the confidentiality of PSWP used in the proceeding

VIOLATIONS & ENFORCEMENT

- An individual who knowingly or recklessly violates the confidentiality provisions is subject to a civil money penalty of up to \$10,000 for each act constituting such violation.
- Safe Harbor - a *provider* whose workforce member discloses PSWP is not deemed to have violated the Act if that workforce member disclosure does *not* include written or oral statements that:
 - Assess the quality of care of an identifiable provider, or
 - Describe or pertain to one or more actions or failures to act by an identifiable provider

Note: the individual workforce member of the provider would still be subject to possible penalties if the disclosure is knowing or reckless. This safe harbor does not apply to the PSO itself – i.e., a PSO workforce member’s disclosure is attributable to the PSO.

- The Act is enforced by the Secretary of Health and Human Services.
 - PSWP may be disclosed to (and the Secretary may require disclosure of PSWP) to investigate or determine compliance with the Patient Safety Act or with HIPAA.

Direct identifiers that need to be removed when one provider discloses PSWP to another provider	
The following direct identifiers of any providers and of affiliated organizations, corporate parents, subsidiaries, practice partners, employers, members of the workforce, or household members of such providers	The following direct identifiers of the patient or of relatives, employers, or household members of the patient
Names	Names
Postal address information, other than town or city, State and zip code	Postal address information, other than town or city, State and zip code
Telephone numbers	Telephone numbers
Fax numbers	Fax numbers
Electronic mail addresses	Electronic mail addresses
Social security numbers or taxpayer identification numbers	Social security numbers
Provider or practitioner credentialing or DEA numbers	Medical record numbers
National provider identification Number	Health plan beneficiary numbers
	Account numbers
Certificate/license numbers	Certificate/license numbers
	Vehicle identifiers and serial numbers, including license plate numbers
	Device identifiers and serial numbers
Web Universal Resource Locators (URLs)	Web Universal Resource Locators (URLs)
Internet Protocol (IP) address numbers	Internet Protocol (IP) address numbers
Biometric identifiers, including finger and voice prints	Biometric identifiers, including finger and voice prints
Full face photographic images and any comparable images	Full face photographic images and any comparable images