UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

1111 Franklin Street
Oakland, CA 94607-5200
Phone: (510) 987-9074
http://www.ucop.edu

August 1, 2017

CHANCELLORS
MEDICAL CENTER CHIEF EXECUTIVE OFFICERS
LAWRENCE BERKELEY NATIONAL LABORATORY DIRECTOR
VICE PRESIDENT–AGRICULTURE AND NATURAL RESOURCES

Dear Colleagues:

Enclosed is the new *Patient Safety Evaluation System* (PSES) *Policy and Procedures.*

The purpose of this policy is to reflect the University's participation in *Patient Safety Organizations* (PSOs) operations pursuant to the *Patient Safety and Quality Improvement Act* (PSQIA), including *California Hospital Patient Safety Organization* (CHPSO), one of the oldest and largest PSOs in the country. CHPSO is a division of the Hospital Quality Institute, affiliated with the California Hospital Association.

The PSQIA was enacted to facilitate and promote the review and analysis of data regarding clinical care and patient safety events in order to help health-care providers to identify, understand, and prevent avoidable injuries and other health and safety hazards. The law shields activities conducted through a provider's "*Patient Safety Evaluation System*" against involuntary disclosure. Among other things, the law and implementing regulations require health-care providers participating in PSOs to develop and maintain policies such as the attached to describe their programs and protect "patient safety work product."

The new Policy was effective as of December 21, 2016, the date the interim policy was approved, and will be published online at http://policy.ucop.edu/.

Yours very truly,

Janet Napolitano
President

Enclosure

cc: Division Leaders
Associate Vice President and Chief Risk Officer Lloyd
Deputy General Counsel Nosowsky
Executive Director Yozgat
Deputy Campus Counsel Sparkman, UCSF
Patient Safety Analyst Kolvan, UCSF

Patient Safety Evaluation System Policy and Procedures

Responsible Officer:	Associate Vice-President & Chief Risk Officer
Responsible Office:	UCOP Office of Risk Services
Issuance Date:	August 1, 2017
Effective Date:	December 21, 2016
Scope:	University Clinical Enterprise

Contact:	Kim Yozgat, UCOP Risk Services
Email:	Kim.Yozgat@ucop.edu
Phone #:	(510) 987-9822

TABLE OF CONTENTS

I. POLICY SUMMARY

The Policy of the University of California is to participate in Patient Safety Activities conducted in accordance with the Patient Safety and Quality Improvement Act of 2005 and its implementing regulations (collectively, the Act). The University of California collects Patient Safety Work Product (PSWP) for the purpose of ultimately reporting that information to a Patient Safety Organization (PSO).

The University entered into a contract with the CHPSO Patient Safety Organization effective January 29, 2013 and may contract with other Patient Safety Organizations to

fully effectuate the Patient Safety Activities and reporting of PSWP, in accordance with the procedures described herein.

PSWP that contains protected health information (PHI) continues to be subject to federal and state health information privacy and security laws and regulations including but not limited to HIPAA and The Confidentiality Of Medical Information Act (CMIA - California Civil Code Section 56.10 et seq). Any use of such PHI shall conform to all laws, regulations, and University Privacy and Security policies.

II. DEFINITIONS

Terms are defined either at first use or in Appendix 1.

A full list of terms and definitions released by the Agency for Healthcare Research and Quality (AHRQ) can be found at Agency for Healthcare Research and Quality Patient Safety Organization Program.

III. POLICY TEXT

A. What Comprises the University's Patient Safety Evaluation System (PSES)?

The PSES includes the collection, management and/or analysis of Patient Safety Concern information recorded in the University Event Reporting System (ERS) for reporting to a PSO. **It includes information documented in the ERS and also deliberation and analysis of a Patient Safety Concern**.

1. A Patient Safety Concern includes:
    - A patient safety event that reached the patient, whether or not there was harm;
    - A near miss or close call - a patient safety event that did not reach the patient; or
    - An unsafe condition - circumstances that increase the probability of a patient safety event.
2. It may also include all activities, communications and information reported or developed by individuals or committees, such as data analyses, Root Cause Analyses, outcome reports and minutes, for the purpose of improving patient safety and/or healthcare quality
    a) Activities involving the actual delivery of patient care and the supporting services directly related thereto; and all original records reflecting the actual delivery of patient care and the supporting services directly relating thereto (e.g., medical records, orders, billing and discharge information);

b) Information or activities which have been specifically de-designated as PSWP (as further described at Sections III.D, below);

c) Information or activities which are not permitted activities or uses of PSWP (e.g., information required to be collected, maintained and reported to any local, state or federal regulatory agency).

B. Creation of PSWP

PSWP is created automatically upon filing an event report in the ERS that involves a Patient Safety Concern. All Patient Safety Concern information is collected and/or developed with the intent to report to the PSO.

1. The University Medical Center, Student Health or Counseling Center or other University facility Risk Manager, Quality or Patient Safety Manager (or his/her designee) ("Authorized Staff") shall review and triage the Event report early in the incident review process, using the criteria set forth in Appendix 2.

   PSWP may also be created by manual completion and delivery to Authorized Staff of any information meeting the description of a Patient Safety Concern and intended to improve patient safety or health care quality. The date of entry into the PSES is the date the Event is delivered or reported to the Authorized Staff.

2. If so designated by Authorized Staff, PSWP may encompass the data collection efforts leading up to making the Event report. The date of entry into the PSWP is the date these activities occur.

3. **PSWP is created when deliberations and analysis (D or A) related to a Patient Safety Concern is conducted**. The date of entry into the PSES is the date these activities occur. **PSWP protections will apply immediately. Deliberations and analysis cannot be de-designated as PSWP. Documents included in this category include but are not limited to**:

   a) Failure Mode Effects Analysis (FMEA)

   b) Root Cause Analysis (RCA) not otherwise reported in the ERS

   c) Data analysis reports & comparative outcomes

   d) Patient Safety Committee minutes

   e) Quality Improvement Committee minutes

4. Once created, PSWP remains PSWP until and unless it is de-designated to no longer be PSWP. Information entered into the University's PSES is promptly evaluated for possible de-designation, as described in Section III.D.

C. Use of PSWP by the University

1. PSWP may be used by the University for a variety of activities, including:

a) Patient Safety Activities.

(1) Patient Safety Activities may be conducted by any individual, committee or body that has assigned responsibility for any such activities. The workforce includes faculty, staff, trainees, volunteers, and contractors who perform work under the direct control of the University. Committees include but are not limited to:

a) Patient Safety Committees

b) Quality Improvement Committees

c) Clinical Performance Improvement Committees

d) Medication Safety Committees

e) Risk Management Committees

f) The Regents Health Services Committee

g) UC Chief Medical Officers/Chief Nursing Officers

h) Center for Healthcare Quality Innovation

i) UCOP Risk Services and/or Committees

j) UCOP Data Management System

k) Audits and Compliances Committee

l) Other Regents committees with jurisdiction

(2) PSWP may also be disclosed to other Affiliates[1] of the University.

(3) PSWP may be disclosed to the University's contractors for the conduct of Patient Safety Activities. Contractors may not further disclose the PSWP.

(4) De-identified PSWP may also be shared with non-University Affiliates to assist them in conduct of Patient Safety Activities, if identifying information is sufficiently removed, as described at Appendix 6.

b) University operations.

Use of PSWP within the University does not constitute a "disclosure" of PSWP. This includes workforce members of the University, as well as members of its health care providers' medical or allied health professional staff. Anyone with a reasonable need to know information to conduct assigned responsibilities or related patient safety activities may be given access to or copies of PSWP, subject to the following limitations.

[1] For purposes of this Policy only, "Affiliate" is defined in the Act as a legally separate provider that is the parent organization of the provider, or is under common ownership, management, or control with the provider, or is owned, managed, or controlled by the provider

(1) Except as otherwise described in these Policy and Procedures, PSWP may not be disclosed outside of the University of California.

a) "Disclosure" means the release, transfer, provision of access to, or divulging in any other manner of PSWP to a legally separate entity or person outside the University of California.

b) PSWP may be shared with outside attorneys, accountants, or other approved consultants as approved by HHS who assist the University in the conduct of the University's business operations. These individuals may not further disclose the PSWP, and any use of the PSWP is subject to Section III.C.3, below.

2. PSWP may not be used or disclosed for purposes prohibited by the Patient Safety Act, including, in particular:

a) PSWP may not be provided in response to any subpoena or other order in any federal, state, local or tribal civil, criminal[2] or administrative proceeding, including but not limited to a disciplinary proceeding against any healthcare provider.

b) PSWP may not be admitted into evidence in any federal, state, local or tribal civil, criminal or administrative proceeding, including but not limited to a disciplinary proceeding against any healthcare provider.

c) PSWP may not be admitted in a professional disciplinary proceeding of a professional disciplinary body established or specifically authorized under State law.

3. Any individual or committee needing to use PSWP for purposes prohibited by the Patient Safety Act may not use the information that is maintained within the PSES for the prohibited purposes, unless:

a) The information can be de-designated and removed from the PSES (see Section III.D, below), or

b) All identified providers authorize the disclosure (see Appendix 7, Paragraph 3), or

c) The identifiable information can be effectively removed (see Appendix 6).

4. Information required for purposes other than reporting to the PSO must be developed through independent investigation outside the PSES. This is generally done by conducting separate interview, record review or evaluations to discover the information as may be needed to accomplish the non-Patient Safety Act purposes.

[2] Exception: PSWP may be disclosed in a criminal proceeding only after a court makes an *in-camera* determination that such PSWP contains evidence of a criminal act, is material to the proceeding and is not reasonably available from any other source.

D. Procedures for PSWP to Be De-Designated and Used for Other Purposes

1. De-designation refers to removing PSWP from the University's PSES so that it may be used for other purposes.
2. All PSWP is presumed to be collected within the PSES and intended to be reportable to the PSO; and that presumption continues unless a decision is made, prior to actual reporting to the PSO, to remove the information from the PSES and de-designate it to be no longer PSWP. However, deliberations and analysis conducted on PSWP cannot be de-designated.
3. Only information not yet reported to the PSO may be de-designated.
4. Only the Authorized Staff may de-designate PSWP.
5. Authorized Staff shall review and triage Event reports early in the incident review process as described in Section III.B.1, above.
6. If PSWP is needed for a purpose not authorized by Section III.C.1, above, it may be de-designated any time prior to reporting to the PSO. Any uncertainty as to whether a use is permitted or not should be referred to a University Risk Manager or University Legal Counsel.
7. To de-designate PSWP, Authorized Staff will document clearly, in the notes of the ERS, which information is to be de-designated, together with the date the de-designation takes effect and the reason for the de-designation.

   PSWP may be wholly or partially de-designated. Unless otherwise indicated, the presumption is that all information relating to a de-designated Patient Safety Concern, that can be, is de-designated[3]. To rebut this presumption and only partially de-designate any information relating to an identified Patient Safety Concern, specifically identify which data or information are to be de-designated.

E. Reporting PSWP to the PSO

1. PSWP that is not marked for deferral or de-designation may be reported on to the PSO at intervals determined by the UCOP Office of Risk Services in coordination with the PSO.
2. Information is reported using the reporting formats provided by CHPSO and/or any other applicable PSO, when the University is participating in other PSO reporting arrangements, in accordance with the reporting parameters of the University/PSO agreement.
3. A delay may be instituted in the PSO reporting process to allow sufficient time to identify those Patient Safety Concerns needing de-designation. Certain urgent Patient Safety Concerns may be reported sooner to the PSO, as determined by the UCOP Office of Risk Services or University Risk Manager.

[3] Documentation that identifies or constitutes the deliberations or analysis of, or identify the fact of reporting pursuant to, a PSES may not be de-designated.

4. Functional reporting: When agreed to within the University/PSO contract, Authorized Staff will inform the PSO regarding what and when patient safety activity information has been collected in its PSES and is being Functionally Reported. The PSO has the authority to access Functionally Reported PSWP at any time without the prior permission of the Provider in order to conduct its Patient Safety Activities.

F. Maintaining Confidentiality of PSWP / Claiming the Privilege.

1. Confidentiality
   a) PSWP is confidential. All access and use must be structured to honor and maintain this confidentiality.
      (1) All communications and activities conducted within appropriate channels of communication and intended to improve safety and quality are permitted.
      (2) Use of PSWP for University business operations (as described at Section III.C.1.b, above) is permitted within appropriate channels of communications.
      (3) Those who access or use PSWP shall be made aware of its confidential nature and will not disclose the information except to others as permitted in (1) and (2), above.
   b) Questions about these parameters should be referred to University Legal Counsel.
   c) Exceptions to confidentiality are described at Section III.F.3, below, and Appendix 7.
2. Privilege
   a) PSWP is "privileged" (i.e., not subject to compulsory discovery or disclosure). Thus, in addition to prohibiting the University from itself using the information for certain purposes (as described at Section III.C.2, above), other persons or entities are likewise prohibited from gaining access to the information via subpoena, court order, administrative order, inspection processes, or the like.
   b) If any governmental agency, or any individual or organization seeks access to or disclosure of PSWP, the University Risk Manager and University Legal Counsel should be contacted immediately so they may assert the PSWP privilege.
   c) All documents containing PSWP should be prominently labeled as "Confidential and Privileged Patient Safety Work Product"[4] to better enable later identification of privileged documents when responding to requests for

[4] University facilities may select other clear text to be used as the label and modify the Policy appropriately—e.g., "PSWP: Confidential and Privileged".

access or disclosure. However, the absence of such a label does not render PSWP non-privileged.

3. Exceptions

   There are a number of exceptions that permit disclosure of PSWP in limited circumstances and subject to specific requirements. These relate to the following – and the specific requirements of each exception are described in Appendix 7:

   a) Criminal proceedings and/or to law enforcement.
   b) Equitable relief actions.
   c) Provider authorization.
   d) Non-identifiable PSWP.
   e) Research.
   f) FDA.
   g) Accrediting Bodies.
   h) Independent Contractor.

4. Disclosures pursuant to any of these exceptions require approval of University Risk Manager and University Legal Counsel, as described in Appendix 7.

G. Required Reporting

PSWP may not be used to satisfy mandated reporting by any federal, state or other governmental agency and should not be provided as the required report. Whenever a Patient Safety Concern is also a serious reportable event or an unusual occurrence that is required to be reported **original** non-PSWP records[5] and/or communications with individuals involved in the event or occurrence may provide the information needed to complete the report. **Any information that is prepared to meet federal, state, or local health reporting requirements is not PSWP. A copy of the report may be treated as PSWP if functionally or electronically reported to the PSO, or treated as Deliberations or Analysis if subsequently reviewed within the PSES**.

H. Root Cause Analyses

1. Except as next provided, any RCA conducted by the University is deemed PSWP.

[5] E.g., a patient's medical record, billing, discharge information or other information that is collected, maintained or developed separately from the PSES; as well as information that has been de-designated as PSWP may be provided as part of these reporting requirements.

a) An RCA conducted at the direction of University Legal Counsel[6] in connection with pending or potential litigation is not PSWP unless specifically designated as such.

b) An RCA conducted by a medical staff peer review committee is not PSWP unless specifically designated as such.

c) An RCA that is conducted by any University and specifically designated at the outset as being conducted outside of the PSES is not PSWP.

2. PSWP may be voluntarily disclosed to The Joint Commission, subject to compliance with Appendix 7 (paragraph 7), and (if applicable) Section III.H.1.a, above.

I. Medical Staff Peer Review

1. PSWP may not be used for medical staff disciplinary proceedings.
2. The Act prohibits a provider from taking an adverse "employment action"[7] against an individual if the action would be based upon the fact that the individual, in good faith, reported to the provider with the intention of having the information reported to a patient safety organization, or reported directly to a PSO. This includes, but is not limited to failure to promote, or adverse evaluations or decisions regarding credentialing. This does not, however, preclude bona fide peer review actions that are taken for other reasons.
3. Medical staff or medical peer review activities are not conducted within the PSES. Information copied from these activities may be incorporated into the PSES and designated as PSWP for use in non-medical staff peer review activities, as described in Section III.B.1.a.1, above.
4. Incorporating information into the PSES shall be deemed in furtherance of the responsible medical staff committee's responsibilities with respect to evaluation and improvement of the quality of care rendered in the hospital or for the peer review body, and does not waive any evidentiary protections or privileges associated with that information.

J. University Personnel Actions

1. The Act prohibits a provider from taking an adverse employment action against an individual if the action would be based upon the fact that the individual, in good faith, reported to the provider with the intention of having the information reported to a patient safety organization, or reported directly to a PSO. This includes, but is not limited to loss of employment, failure to promote, or adverse

[6] As used here, Legal Counsel refers to any in-house or outside legal counsel who may be directing the activity with respect to the University, and is not limited to the General Counsel or in-house counsel who are designated responsible for PSO activities.

[7] The definition of "employment action" under the Act is broad enough to encompass all medical staff, even those medical staff not employed by the University.

evaluations or decisions regarding credentialing. This does not, however, preclude bona fide personnel actions that are taken for other reasons.

2. Further, the Act prohibits use of PSWP in litigation. Thus, it is important to assess the possibility that a personnel action may lead to litigation. Any use or release of PSWP in connection with personnel actions must be approved by University Legal Counsel.
3. There are three options for addressing this limitation:
    a) Any report of a Patient Safety Concern clearly involving individual performance or conduct may be held as PSWP within the PSES, and not released to the PSO until a decision has been made not to use the PSWP for a personnel action. The time delay in reporting to a PSO (see Section III.E.3, above) should then be set to include sufficient time for identification of PSWP needed for personnel actions.
    b) Any report of a Patient Safety Concern involving individual performance or conduct that may result in personnel action may be immediately de-designated as PSWP (see Section III.D, above) and removed from the PSES. A copy of the report is then automatically re-entered into the PSES and the copy is deemed PSWP, as of the same date, and may be used for other (non-personnel action) Patient Safety Activities.
    c) Information can be placed into the personnel file that is developed separately from the regular Event reporting and review process.

K. Grievances

In some cases, patient grievances may involve Patient Safety Concerns. When that is the case, all documents (other than the patient's original written grievance and the grievance log), data, evaluations and the like are deemed PSWP.

Information that is reported to the patient or any outside agency must not include PSWP (unless the PSWP is able to be and has been properly de-designated as PSWP [see Section III.D, above].

IV. TRAINING

A. University Medical Center, Student Health or Counseling Center or other University facility Risk Manager and/or Quality or Patient Safety Manager *or his/her designee* shall undergo training to assure sufficient knowledge of the requirements of the Act, these Policies and Procedures and the University's uses of PSWP and conduct of Patient Safety Activities.

B. Other University Personnel

University Medical Center, Student Health or Counseling Center or other University facility Risk Managers and/or Quality or Patient Safety Managers or their designees shall be responsible to conduct or arrange sufficient training of all University

personnel who will be accessing PSWP as to the permitted uses of PSWP and appropriate measures to maintain confidentiality in accordance with these Policies and Procedures.

V. COMPLIANCE / RESPONSIBILITIES

The Chancellor of each University is responsible for assuring compliance with this Policy.

VI. PROCEDURES

Applicable procedures to be followed by the University healthcare entities will be as defined by the respective University of California campuses consistent with this Policy and applicable law and regulations.

VII. RELATED INFORMATION

- Patient Safety and Quality Improvement Act of 2005 and its implementing regulations. – link: https://www.pso.ahrq.gov/legislation/act
- Patient Safety Rule – link: https://www.pso.ahrq.gov/legislation/rule
- Patient Safety and Quality Improvement Act of 2005 - HHS Guidance Regarding Patient Safety Work Product and Providers' External Obligations (*May 2016*) - link: https://www.pso.ahrq.gov/legislation/HHS-guidance

VIII. FREQUENTLY ASKED QUESTIONS

AHRQ FAQs -link: https://www.pso.ahrq.gov/faq.

IX. REVISION HISTORY

August 1, 2017: This is a new policy, which has been remediated to meet Web Content Accessibility Guidelines (WCAG) 2.0.

X. APPENDICES

Appendix 1

Definitions

CHPSO: CHPSO Patient Safety Organization (see additional definition of PSO, below).

Copy: The Patient Safety Rule refers to the term "copy" in two ways in the definition of patient safety work product. First, when information meets all of the applicable requirements for protection as patient safety work product, any copy of the PSWP is also protected. Second, if information is not eligible for protection as PSWP (e.g., it is from the medical record or a report sent to regulatory authorities); the provider can still send a copy of the information to its PSO. While the copy held by the PSO or by the provider's PSES is protected, that protection does not apply to the original information that exists elsewhere (e.g., the medical record or the copy held by the regulator).

De-Designated: Pertains to the Drop-Out Provision. The Patient Safety Rule provides a limited opportunity for a provider to remove patient safety work protections from information that the provider entered into its patient safety evaluation system (PSES) for reporting to a PSO. The drop-out provision can be used for any reason, provided the information that the provider had placed in its PSES has not been reported to a PSO and the provider documents the action and its date. Upon removal, the information is no longer protected. The drop-out provision cannot be used if the information has been reported to a PSO and it does not apply to information that describes or constitutes the deliberations or analyses of a PSES.

Deliberations or Analyses (D or A): as a means of creating PSWP includes, but are not limited to, all verbal discussions, dialogues and other forms of communication, electronic or otherwise, as well as documents, reports, studies and all other forms of work product relating to identified patient safety activities which are conducted within a licensed health care provider’s patient safety evaluation system (PSES) for the purpose of improving patient safety and the quality of health care services. D or A also includes communications and work product regarding the development of a PSES, and whether such information constitutes PSWP or whether or not to report PSWP to a PSO. Communications and work product which are identified as D or A automatically become PSWP and need not be reported to a PSO in order to qualify as PSWP.

Event Reporting System (ERS): The University’s system for work force reporting of Events.

Event: An unanticipated occurrence or set of circumstances that caused or could cause harm to patient personnel (staff member, employee, volunteer) or visitor, and that is not consistent with the routine care of a particular patient and/or the routine operation of the facility. Not all Events are Patient Safety Events (see definition below).

Functional Reporting: Is the method by which the Provider identifies to a PSO the category of patient safety activity information, as described in its patient safety evaluation system ("PSES"), which is not actually reported to a PSO but which becomes

available to and accessible by the PSO in order for the PSO to perform its Patient Safety Activities as described in the Agreement and related policies and procedures.

Near Miss: A Patient Safety Event that did not reach a patient. For example: discovery of a dispensing error by a nurse as part of the process of administering the medication to a patient (which if not discovered would have become a Patient Safety Incident); or discovery of a mislabeled specimen in a laboratory (which if not discovered might subsequently have resulted in a Patient Safety Incident).

Patient Safety Activities: Activities carried out on behalf of University health care providers and/or the contracting PSO that involve Patient Safety Concerns, and are intended to improve patient safety and quality of health care delivery, including but not limited to:

- Collection and analysis of PSWP;
- Development and dissemination of information with respect to improving patient safety – such as recommendations, protocols, or information about best practices;
- Using PSWP to encourage a culture of safety and provide feedback and assistance to minimize patient risk;
- Maintaining and securing PSWP confidentiality;
- Using qualified staff; and
- Other activities related to operation of the PSES and dissemination of information to PSES participants.

Patient Safety Concern: A Patient Safety Event or an Unsafe Condition.

- Incident—a patient safety event that reached the patient, whether or not there was harm;
- Near miss or close call—a patient safety event that did not reach the patient; or
- Unsafe condition—circumstances that increase the probability of a patient safety event.

Patient Safety Evaluation System (PSES): The collection, management or analysis of information for reporting to a PSO.

Patient Safety Event: An Event that happens to or involves a patient, including Patient Safety Incidents and Near Misses:

Patient Safety Incident: A Patient Safety Event that reached a patient, and either resulted in no harm (no harm incident) or harm (harm incident). The concept “reached a patient” encompasses any action by a healthcare practitioner or worker or healthcare circumstance that exposes a patient to harm. For example: if a nurse gives a patient an incorrect medication to take and the patient recognizes it as such and refuses to take it, a Patient Safety Incident has occurred.

Patient Safety Organization (PSO): An entity certified by the Secretary of Health and Human Services pursuant to 42 U.S.C. 299B-24, and with which the University has contracted, on behalf of each University health care provider, for the delivery of PSWP

and the conduct of Patient Safety Activities. The University has contracted with CHPSO for these purposes, and in the future may elect to contract with other PSOs, as well. Any such election will be accompanied by an Appendix to these Policy and Procedures clarifying any unique requirements applicable to interactions with other PSOs. Except as otherwise so documented, references in these Policy and Procedures to PSO shall mean CHPSO and any other PSOs with which the University has contracted.

Patient Safety Work Product (PSWP):

- 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.
- Patient Safety Work Product must not be disclosed, except in very specific circumstances and subject to very specific restrictions as specified in Appendix 7 "Exceptions to Non-Disclosure Requirements"
- When analysis and deliberations are conducted in the PSES, PSWP protections will apply immediately; the drop-out provision does not apply

Unsafe Condition: Any circumstance that increases the probability of a patient safety event; includes a defective or deficient input to or environment of a care process that increases the risk of an unsafe act, care process failure or error, or patient safety event. An unsafe condition does not necessarily involve an identifiable patient. For example, an out-of-date medicine on a shelf represents an unsafe condition. It might be given to a patient, but the identity of such patient is unknown at the time of discovery. The attempt to administer the out-of-date medicine to a patient would either represent a near miss (if not administered) or an incident (if administered).

Appendix 2

Triaging Patient Safety Concerns

The University Risk Manager or his/her designee is responsible to review Event reports and determine if they involve Patient Safety Concerns. Those involving Patient Safety Concerns are further assessed and handled as follows:

	Event	**Disposition**
1.	❑ Does or may involve performance of a member of the medical or allied health professional staff.	• The report involves a member of the medical staff, any and all peer review activities are to be the result of an independent review. • The original event report is PSWP which may be used for non-medical staff peer review Patient Safety Activities.
2.	❑ Does or may involve performance of other hospital personnel.	• Any and all personnel actions must be the result of an independent review. • The original event report is PSWP which may be used for non-personnel Patient Safety activities.
3.	❑ Does or may involve potential lawsuit.	• Retain as PSWP (unless also involves 1 or 2 above – in which case handle per applicable disposition instructions noted for those matters), subject to further investigation and evaluation. • PSWP should not be reported to the PSO until UCOP Office of Risk Services, in consultation with University Legal Counsel, determines it is not needed as evidence in litigation. (If not yet reported to the PSO, some PSWP may be de-designated*, copied, and the copy returned to the PSES as PSWP and reported to the PSO; and the original used as needed as evidence in litigation.)

Appendix 3

Information for Law Enforcement Officials
About Permitted Uses and Disclosure of Patient Safety Work Product

To: *[insert name of law enforcement official and agency to whom PSWP is given]*
The information you have requested is protected by federal law (the Patient Safety and Quality Improvement Act of 2005, 42 U.S.C. 299b-21 et. seq., and 42 C.F.R. Part 3, §§ 3.10 et. seq.) as Patient Safety Work Product. These provisions permit your access to this information only in the following circumstances and subject to the following conditions:

42 CFR 3.206(b)(10) Disclosure to law enforcement.

(i) Disclosure of patient safety work product to an appropriate law enforcement authority relating 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.

(ii) Law enforcement personnel receiving patient safety work product pursuant to paragraph (b)(10)(i) of this section only may disclose that patient safety work product to other law enforcement authorities as needed for law enforcement activities related to the event that gave rise to the disclosure under paragraph (b)(10)(i) of this section.

By your signature below, you confirm that your request for access to this information is consistent with the above-cited federal law, and that you will maintain confidentiality of the information as required by federal law.

Date:_____ Signature:_____

Retain signed original for University files; a copy of this document should be provided to the law enforcement official who obtains a copy of the PSWP.

Appendix 4

Provider Authorization to Disclose PSWP

Name of Provider_____

The above-named provider hereby authorizes disclosure to:

_____

[insert name of individual or entity to which PSWP may be disclosed]

of the following Patient Safety Work Product information:

_____

[insert description and purpose of the information to be disclosed]

_____

_____

_____

Signature:_____ Date:_____

For University Use:

Information was disclosed pursuant to this authorization on: *[list below all dates upon which disclosure was made]*

Date	*Signature of [Designated Person] releasing information*
_____	_____
_____	_____
_____	_____

This authorization is to be delivered to the University Risk Manager and retained for 6 years from the date of the last disclosure made pursuant to this authorization.

Appendix 5

Information for State & Federal Regulators (or others seeking compulsory access to PSWP)

The information you have requested is protected by federal law (the Patient Safety and Quality Improvement Act of 2005, 42 U.S.C. 299b-21 et. seq., and 42 C.F.R. Part 3, §§ 3.10 et. seq.) as Patient Safety Work Product. Identifiable Patient Safety Work Product may not be disclosed outside of this facility.

Any questions about access to this information should be directed to University Legal Counsel, attention: *[insert contact information]*

Appendix 6

Removing Direct Identifiers[8] and Rendering Information as Non-identifiable

A. Removal of Direct Identifiers versus Non-Identifiable PSWP

1. By removing direct identifiers of patients and caregivers, certain disclosures of some information that would otherwise be deemed PSWP may be disclosed to other PSOs (i.e., other than the PSO to whom the University has reported the information), or to other providers, including non-affiliated providers – for Patient Safety Activities. The requirements for removing patient and caregiver direct identifiers are less rigorous than the requirements for rendering "non-identifiable PSWP," and since they are less rigorous, there is a corresponding limitation on how the information may be used (i.e., only for Patient Safety Activities).
    a. The requirements for removing patient and caregiver direct identifiers are set out in this Appendix 6 (Section B).
    b. The University Risk Manager may release information pursuant to this Appendix 6, after confirming that all direct identifiers have been sufficiently removed.
    c. The University Risk Manager may authorize others to disclose information pursuant to this Appendix 6, provided appropriate training and procedures are in place to assure proper identifier management.
2. Non-identifiable PSWP, on the other hand, is PSWP that has been sufficiently scrubbed of all meaningful identifiers to permit disclosure without restrictions on use.
    a. The requirements for non-identification are therefore more rigorous, as described in this Appendix 6 (Section C).
    b. The University Risk Manager is authorized to disclose information pursuant to this Appendix 6. The University Risk Manager must document, in writing, that all of the factors listed in Appendix 6 (Section C) have been considered and determined satisfied.
    c. The University Risk Manager may authorize others to disclose information pursuant to this Appendix 6, provided appropriate training and procedures are in place to assure proper identifier management.

[8] The Act refers to removing direct identifiers as "anonymization", which is confusingly similar, though not identical to "non-identification". For the sake of clarity, this Policy uses the phrase "removal of direct identifiers" in lieu of "anonymization".

B. Removing Direct Identifiers on PSWP is accomplished by removing all of 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:

1. Names
2. Postal address information, other than town or city, State, and zip code (i.e., town or city, State, and/or zip code may be disclosed)
3. Telephone numbers
4. Fax numbers
5. Electronic mail addresses
6. Social security numbers or taxpayer identification numbers
7. Provider or practitioner credentialing or DEA numbers
8. National provider identification number
9. Certificate/license numbers
10. Web Universal Resource Locators (URLs)
11. Internet Protocol (IP) address numbers
12. Biometric identifiers, including finger and voice prints; and
13. Full face photographic images and any comparable images; and
14. With respect to any individually identifiable health information in such PSWP all direct identifiers required to develop a limited data set under HIPAA in accordance with applicable policy. Note, however, that since a data use agreement is not used, the resulting PSWP does not meet the HIPAA definition of “limited data set.”

C. Rendering Information as Non-IdentifiablePSWP is deemed non-identifiable with respect to any particular provider – and hence may be disclosed – if:An “appropriately knowledgeable person” determines that the risk is “very small” that the information could be used alone, or in combination with other reasonably available information, by an anticipated recipient to identify either a provider or a reporter. To be such an appropriately knowledgeable person, one must have knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable. This determination must be documented, including documentation of the methods and results of the analysis that led to the determination.

2. **Alternatively**, PSWP may be rendered non-identifiable if all of the following identifiers have been removed with respect to any identifiable provider or reporter, or any affiliated organizations, corporate parents, subsidiaries, practice partners, employers, members of the workforce, and household members of the provider or reporter:

a. All of the identifiers listed in Appendix 6, Section B, 1 through 13, above, plus

b. Geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code and equivalent geocodes (except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census, the geographic using formed by combining all zip codes with the same three digits contains more than 20,000 people).

c. All elements of dates (except year) for dates directly related to a patient safety incident or event; and

d. Any other unique identifying number, characteristic, or code except as permitted for re-identification (see Section C 3, below); and

e. The person authorizing the disclosure has no actual knowledge that the information could be used, alone or in combination with other information that is reasonably available to the intended recipient, to identify the particular provider or reporter.

3. With respect to non-identifiable information about providers, it is permissible to assign a code or other means of record identification to allow information made non-identifiable to be re-identified by the disclosing provider, PSO, or responsible person, if:

   a. The code or other means of record identification is not derived from or related to information about the provider or reporter and is not otherwise capable of being translated so as to identify the provider or reporter; and

   b. The provider, PSO or responsible person does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

4. With respect to any particular patient, PSWP is deemed non-identifiable only if the individually identifiable health information is de-identified in accordance with the HIPAA Privacy Rule. De-identification of individually identifiable health information must be conducted in accordance with University policy.

Appendix 7

Exceptions to Non-disclosure Requirements

Criminal Proceedings, Equitable Relief, Provider Authorization, Non-Identifiable PSWP, Research, FDA, Accrediting Bodies

1. Criminal Proceedings and Law Enforcement
    a. Criminal Proceedings - While as a general matter, PSWP is not subject to disclosure, even in criminal proceedings, there is a process whereby a court may review *in camera* (i.e., in the judge's chambers) the circumstances and determine that the PSWP contains evidence of a criminal act, is material to the proceeding, and is not reasonably available from other sources. University Legal Counsel must be apprised of any request for PSWP pursuant to this exception, and will be responsible to coordinate any disclosures directed by the court.
    b. Law Enforcement - PSWP may be disclosed to appropriate law enforcement authorities relating to a Patient Safety Concern that either constitutes the commission of a crime, or for which the disclosing person reasonably believes constitutes the commission of a crime, if the PSWP is reasonably believed to be necessary for criminal law enforcement purposes.
        (1) The law enforcement officials shall be apprised of the controlling regulation (42 CFR Part 3, section 3.206(b)(10)) that the information is PSWP, and that the information may only be disclosed to other law enforcement authorities as needed for law enforcement activities related to the Patient Safety Concern at issue. Attached as Appendix 3 to these Policies and Procedures is a written statement, Notification of PSO Act Limitations on Use of Information, to be provided to law enforcement apprising them of these responsibilities.
        (2) University Legal Counsel shall approve all disclosures to law enforcement officials pursuant to this section.
2. Equitable Relief – Individuals who are seeking equitable relief (e.g., an injunction) associated with a claim that they have been the subject of an adverse employment action relating to their having reported information to a provider or a PSO may have a right to access and use PSWP to pursue that equitable relief. University Legal Counsel must be apprised of any request for PSWP pursuant to this exception, and will be responsible to coordinate any disclosures directed by the court or administrative tribunal.
3. Provider Authorization – PSWP may be disclosed for specified purposes pursuant to written authorization of all identified providers. Any such written authorization must:
    a. Be signed by the identified provider.

b. Contain sufficient detail to inform fairly the identified provider of the nature and scope of the disclosure that he/she is authorizing.

c. Be retained by the disclosing entity for 6 years from the date of the last disclosure made pursuant to the authorization.

See Appendix 4 of the Policies and Procedures for the Authorization Form to be used for this purpose. Authorization pursuant to any other form must be approved, in writing, by University Legal Counsel.

4. Non-identifiable PSWP may be disclosed without restriction. See Appendix 6 of the Policies and Procedures for description of non-identifiable PSWP.

5. Disclosure of identifiable PSWP may be disclosed to an Independent Contractor as required for patient safety activities.

6. Research – PSWP may be disclosed to persons carrying out research, evaluation or demonstration projects that have been authorized, funded, certified or otherwise sanctioned by the Secretary of Health and Human Services. Disclosure pursuant to this exception must be approved, in writing, by a responsible Institutional Review Board and University Legal Counsel.

7. FDA – PSWP may be disclosed to the Food and Drug Administration (FDA) and entities required to report to the FDA. This exception relates to FDA oversight of FDA-regulated products or activities. Disclosure pursuant to this exception must be approved by a University Legal Counsel.

8. Accrediting Bodies – PSWP may be disclosed to The Joint Commission (TJC) or other body responsible for accreditation of a University health care provider, if all individually identified providers agree[9] to the disclosure, or all identifiers described at Appendix 6, Section C of the Policies and Procedures have been removed.

   a. Once authorization has been obtained, or identifiers have been removed, the following persons are authorized to release information to an accrediting body:

      (1) The University Risk Manager.

      (2) The Hospital's CEO.

      (3) The Chief of Staff, with respect to any member of the medical staff or any Allied Health Professional for whom the medical staff has oversight or credentialing responsibility.

[9] Note: the provisions of this exception are not as rigorous as those above with respect to "authorized" disclosures (see Paragraph 3, above). Therefore, it may be possible to disclose information to accrediting bodies so long as a general "agreement" is obtained and documented, or there is otherwise a reasonable anonymization of the information. A general agreement could, for example, be obtained as part of the provider credentialing process, by including an acknowledged agreement to release of identifiable information to the responsible accrediting body.

9. PSWP may be disclosed to the Secretary of Health and Human Services if needed to investigate or determine compliance with the Act or with the HIPAA Privacy Rule, or to make or support decisions with respect to listing of a PSO. Disclosures pursuant to this section shall be coordinated by University Legal Counsel.

   Note: There is no provision in the Act for disclosure of PSWP to other regulatory agencies. If a regulatory agency (other than one described above) requests access to PSWP, it must be declined, with reference to the confidentiality requirements of the Act. Only information that is non-identifiable, as described at Appendix 6, Section C of the Policies and Procedures may be provided to regulatory agencies. See Appendix 5 for a statement, Information for Regulatory Agencies Regarding Access to Patient Safety Work Product that can be used to assist in this communication. In the event the regulatory agency challenges this position, the matter shall be immediately referred to University Legal Counsel for resolution.