The NJHA Institute for Quality and Patient Safety
A Federally Certified Patient Safety Organization

NJHA's Institute for Quality and Patient Safety has been designated a "Patient Safety Organization" (PSO) by the U.S. Agency for Healthcare Research and Quality. PSOs partner with healthcare providers to improve healthcare quality through data collection and analysis. The Federal Patient Safety and Quality Improvement Act of 2005, which authorized the certification of PSOs, also affords confidentiality and privilege protections.

Background

In 2005 Congress passed the Patient Safety and Quality Improvement Act of 2005, which established federal privilege and confidentiality for patient safety work product which is reported to a PSO. Up until that point, providers had been reluctant to participate in efforts to pool data and share experiences because of the concern that they would lose confidentiality privileges and the information would become discoverable. This was especially true in New Jersey. In the fall of 2008, the Department of Health and Human Services issued the final rules for this Act, thereby creating Patient Safety Organizations (PSOs). PSOs are intended to encourage providers to share patient safety information and performance improvement data with uniform federal confidentiality and privilege protection so that ultimately, best practices can be identified and patient safety will be improved.

There are many benefits to participating in a PSO:

- Participation in a PSO grants certain federal confidentiality and privilege protections for the information that is submitted to the PSO;
- Healthcare organizations can talk about and work on ways to prevent adverse events in a protected environment;
- PSOs provide a national standardized taxonomy for describing patient safety events, near misses and unsafe conditions;

- PSOs can populate a national repository of reported patient safety data utilizing Common Formats developed by the Agency for Healthcare Research and Quality (AHRQ).

Currently, participation in a PSO is voluntary. However, in at least one state, Missouri, state officials have determined that organizations that want to participate in the state's Medicaid program must participate in a PSO to receive payment for Medicaid beneficiaries. Additionally, in the Affordable Care Act there is language in Section 1311 Affordable Choices of Health Benefit Plans

- (h)(1) Enhancing Patient Safety - Beginning January 1, 2015, a qualified health plan may contract with
  - (A) a hospital with greater than 50 beds only if such hospital
    - (i)utilizes a patient safety evaluation system as described in part C of title IX of the Public Health Service Act.

In the Public Health Service Act, a patient safety evaluation system "means the collection, management, or analysis of information for reporting to or by a patient safety organization."

This brief provides more information about PSOs and their components, including the Patient Safety Evaluation System and the Patient Safety Work Product (PSWP).

> For more information on how your organization can be a member of the NJHA Institute for Quality and Patient Safety's PSO, contact Aline Holmes, senior vice president, clinical affairs at 609-275-4157 or aholmes@njha.com.

What is a Patient Safety Evaluation System (PSES)?

To obtain the federal privilege and confidentiality protection afforded by a PSO, organizations must design a system by which information is collected and analyzed. A PSES is the collection, management or analysis of information for reporting to or by a PSO. It is made up of your already existing quality improvement activities and can be considered as a subset of your existing improvement activities. It is the protected space in which PSWP is assembled or developed for reporting to or from a PSO.

A PSES can include information like outcomes data, near-miss reports, utilization data, infection control, risk management and incident reporting activities and peer review activities (excluding disciplinary actions). In setting up your PSES you will want to define the scope and function of your system, the process owner(s), how information is collected, managed, analyzed and reported, where and how it will be maintained and how information will be transmitted to the PSO.

A PSES defines the processes within an organization for the collection, management and reporting of a PSWP to a PSO. It can be established as a component of an organization's current risk management, patient safety or quality improvement program. Following are steps to guide the development of a PSES within your organization:

- Assign an individual or team to review the Patient Safety & Quality Improvement Act, the Act's Final Rule and current applicable quality, risk, medical staff and safety policies, procedures and practices.
    - This individual/team should be familiar with the organization's safety reporting system, peer review and credentialing processes, HIPAA, risk management and claims activities around reporting and disclosure practices.
- Identify and assess current reporting systems and information flow, ie. how patient safety events are currently identified, reported and managed through risk management/patient safety/quality improvement/customer services/credentialing processes. Also look at how this data is shared and documented – it may be a good idea to flowchart these processes.
- Develop new or amend current applicable policies to identify and define the scope and function of your PSES.
    - Assess data and information currently collected to determine what should and should not be included in the PSES.
    - Address how PSWP and non-PSWP will be managed within the PSES-related policies.
- Determine where and how data and information to be included in the PSES will be maintained, including in what equipment/systems, the physical location and who will have access to it.
    - Store information within the PSES in a secure physical or electronic space designated for the conduct of patient safety activities.
    - Identify individuals who are authorized to report to the PSO within your PSES.
- Define procedures for how your PSES will report data to the PSO. Identify reporting mechanism to be used, who is authorized to have access to the system to enter data and information, who is authorized to determine when data entered into the system is officially "submitted to the PSO," and identify who will be authorized to have access to the system to retrieve and review reports.
- Consider using standard language on all documents submitted to the PSO from your PSES, such as "*This information has been collected within the (name of organization) PSES for the purpose of reporting to the NJHA Institute for Quality & Patient Safety PSO, (date)"*

What is Patient Safety Work Product (PSWP)?

Under the Act, PSWP is any data, reports, records, memoranda, analyses (such as root cause analyses, clinical practice protocols, evaluation of staff or equipment, etc.) or written or oral statements that

- Could improve patient safety, health care quality or health care outcomes;
- Could be used to understand patient safety events and prevent them from recurring, including recommendations to prevent future events;
- Are assembled or developed by a provider for reporting to a PSO and are reported to a PSO; or
- Identify or constitute the deliberations or analysis of, or identify the fact of reporting pursuant to, a PSES.

While the PSO law does not require that a provider document what encompasses its PSWP, AHRQ strongly recommends that a policy be written to define the extent of an organization's PSES to reduce the risk of successful legal challenge.

PSWP is **not** initial source information, e.g. medical records, billing and discharge information or any other original patient or provider information. HHS has ruled that copies of such information as an incident report can be provided to a PSO with legal protections in place, but the original incident report used for internal quality assurance or risk management purposes is not protected by the federal protections offered under the PSQIA. However the PSO cannot be forced to release the copy of the incident report it holds as part of the PSWP. PSWP can be shared within your workforce, medical staff and attorneys, but this should be covered in the documentation of your PSES, and everyone should have signed confidentiality agreements. PSWP can be shared with your attorney, but cannot be used in litigation once it is submitted to the PSO.

Additionally, any data collected for external reporting, such as relates to the N. J. Patient Safety Act, the NPDB, FDA, etc. is not considered patient safety work product and would not receive additional federal protections. In those situations, to avoid conflicting compliance risks a provider needs to ensure that the external reporting (for ex. to the NJDHSS) is done prior to submitting that event and associated data to the PSO. For that reason, PSWP can "live" in the PSES until for a long time and still have protection while the investigation is going on. Intent to submit is the minimum threshold for protection under PSQIA, and the Final Rule implementing the PSO program does not specify how much time a provider has to make this final determination before information must be submitted to the PSO. AHRQ has warned, however, that information left indefinitely in a PSES with no submission to a PSO could be vulnerable to a court challenge, with plaintiff's attorneys arguing that there was never any good faith intent to submit to the PSO and therefore should not receive the protection provided for. It would be wise, in developing your PSES that you determine, and document, your own time frames for this final determination. Other data related to reporting to entities such as licensing boards for medical professionals, reporting to the National Practitioner Data Bank of practitioner disciplinary actions and disclosure of particular providers or suppliers required by the Medicare program's conditions of participation are also not PSWP.

Finally, HHS has allowed that PSWP that exists in your PSES can be "released" or removed back into your QI activities by your facility at any time before submitting to the PSO. A copy of the information can still be submitted to the PSO, but the health facility will not receive the federal protections. However, the PSO will receive the protections and therefore will not and cannot disclose/release the information. In a situation where PSWP has been submitted to the PSO and subsequently there is determined to be a need to report the incident externally, the PSQIA allows providers to create a new version of the information needed for external reporting after the original document was submitted. Since the original source documents are not protected, a facility could use those records, interviews, etc., and "recreate" the incident to meet an external requirement. For example, an adverse event occurs, routine investigation is completed, there is no requirement for external reporting and the event is submitted to the PSO. Subsequently, the facility receives a notice of complaint and wants to use the PSWP reported to the PSO to defend the facility – the PSO cannot release that PSWP, however, the facility can use

the original medical record and identify witnesses to obtain current statements, thereby recreating what was submitted to the PSO.

Following are steps to define and manage your PSWP:

- Identify and assess what patient safety-related documents, data and information are currently developed by the organization. These may include safety and quality reports, either verbal or written, committee minutes, notes, checklists, transcripts, recordings and peer review documents, incident reports, RCAs. They also include any discussions or documentation used for quality and patient safety improvement.
- Determine how these documents and discussions are being used, documented and maintained within your organization. Consider:
    - Who is collecting, reviewing and maintaining the data and information;
    - How, where and when the information is being filed;
    - How the information is being maintained;
    - Whether the information is for activities that would not allow the information to be defined as PSWP.

- Determine what documentation can and cannot be considered PSWP, and how each type of documentation will be managed and separated within your PSES.
        - Not considered PSWP – original source documents such as patient's medical record, billing and discharge information and any other original patient or provider record; mandated reports for compliance with federal, state or accreditation requirements.
        - May be considered PSWP – data reports, records, memoranda, deliberations, analysis, written or oral statements and other information collected, maintained, developed or assembled by the organization for the purpose of reporting to a PSO.
            - Other documents developed for the purpose of analysis, review, quality improvement, risk management and patient safety improvement;
            - A *copy* of information included on mandated reports;
            - Analyses, deliberations and recommendations for improvements to be made related to events resulting in a mandated report.

On occasion, it may be necessary to remove PSWP from your PSES. PSWP that has not been reported to the PSO may be removed from your PSES.

- As an example, an event is entered into the PSES and is defined as PSWP
    - Results in a peer review process which requires a report to be sent to professional licensing board.
- Such a report would need to be removed from your PSES and reported as required. The reports themselves cannot be submitted as PSWP to a PSO and receive the protections. However, the following data elements contained within your PSES reporting system may be reported to the PSO as PSWP and could be eligible for the privilege and confidentiality protections afforded PSWP: facts of the event and analyses, deliberations and recommended improvement resulting from the event.

- In developing a process to remove PSWP from your PSES prior to submission to the PSO, consider maintaining a log of PSWP that is removed from the PSES, including the date of removal and a statement that the provider no longer intends to report the information to a PSO; and identifying which personnel are authorized to remove PSWP from the PSES.

A Case Study to Demonstrate How All of This Works

1. A 75-year-old patient admitted with shortness of breath gets up in the middle of the night to go to the bathroom, slips and falls, hitting his head, suffering an intracerebral bleed which leaves him comatose.

- Nurse manager notifies the risk manager and completes an incident report.
- Risk manager and nurse reviewer do an initial investigation: (PSES)
  - Review the medical record (not PSWP)
  - Gather facts from staff about what happened (not PSWP)
  - Risk manager and nurse reviewer have discussion, take notes on their deliberations (PSWP)
- Risk manager determines if this event requires reporting to the NJDHSS Patient Safety Reporting Initiative.
  - In this example, it does, so risk manager proceeds with reporting as required by the Patient Safety Initiative (http://www.state.nj.us/health/ps/report.shtml)
  - Any notes, minutes, documents prepared during the course of the investigation and not required to be submitted to NJDHSS are considered PSWP and can be submitted to the PSO.

2. The same patient falls, sustaining multiple bumps and bruises, but no serious injury.

- Nurse manager notifies the risk manager and completes an incident report
- Risk manager and nurse reviewer do an initial investigation: (PSES)
  - Review the medical record (not PSWP)
  - Gather facts from staff about what happened (not PSWP)
  - Risk manager and nurse reviewer have discussion, take notes on their deliberations (PSWP)
- Risk manager determines this event does not require reporting to the NJDHSS Patient Safety Reporting Initiative.
- Risk manager schedules a meeting with all involved physicians and staff (PSES) to complete a root cause analysis (RCA) (PSWP)
- The team convenes to complete the RCA – this team is part of your PSES.
  - Create a "staging" area, either electronic or physical, where all documentation related to this incident is considered PSWP and is housed within your PSES (the intent to submit exists, but there is still opportunity to remove it); this is important because once you submit to the PSO, the information cannot be viewed or used outside of your facility.
  - The completed RCA is PSWP, as the intent is to submit to the PSO.

- The next day, the risk manager and the administrator meet with the facility's general counsel and determine:
    - That there is a strong likelihood that a liability suit will be filed against the facility by the family
    - That there may be a complaint filed with NJDHSS by the family
    - That it is in the best interest of the facility to show the results of the RCA to the state and perhaps to the family of the patient.
- The risk manager can then go into the PSES and remove the RCA. This moves the RCA from the PSES into the facility's quality improvement activities. The RCA is no longer protected by the federal Patient Safety Improvement Act.
- The risk manager completes the in-depth investigation (PSWP) and attaches it to the reported event in the PSES. The RCA (no longer PSWP) is reviewed by the facility's fall committee (part of PSES) and in its review a decision is made to hire a falls consultant to assess current practices and make recommendations. The committee minutes are PSWP.
- Weeks later, the falls consultant (PSES) performs an evaluation and produces a report with recommendations (PSWP). The falls committee reviews the consultant's report and creates an action plan to implement the recommendations (minutes and action plan are PSWP and can be entered into the PSES). The action steps taken by the falls team eventually result in changes in the falls assessment form (not PSWP) and changes in policies (not PSWP).
- Once the risk manager determines that the work is complete, she can submit it to the PSO. The risk manager could decide to send a *copy* of the RCA to the PSO with the rest of the PSWP related to this event, in which case the word "copy" should be added to the top of the RCA. As a copy, the RCA is not PSWP and will not receive the federal protections; however, the PSO will receive the federal protections, and therefore will not and cannot disclose/release the information.