LegalNotes

Volume2 Issue2

LegalNotes is a regular online *Aligning Forces for Quality* (AF4Q) publication that provides readers with short, readable summaries of developments in the law that collectively shape the broader legal environment for efforts to improve quality, reduce health care disparities, and improve the transparency of price and quality information.

The Patient Safety and Quality Improvement Act Regulations: Implications for Health Information Access and Exchange

Lara Cartwright-Smith, J.D., M.P.H.
Sara Rosenbaum, J.D.
Christina Sochacki, R.N. (J.D. Cand.)

Introduction

The Patient Safety and Quality Improvement Act (PSQIA) was intended to prompt providers to report patient safety and other health care quality information by using the legal tool known as "privilege" to encourage robust examination of quality and safety without fear that the results of such efforts could be "discovered" by a plaintiff during a liability trial. Whether the Act (as implemented in regulations issued in late 2008) will promote much critical self-analysis, and just as importantly, whether even aggregated and de-identified results of such self-analysis will ever be available to communities, remains to be seen. The implementing regulations appear to give providers – and the patient safety organizations to which they report information – considerable leeway to avoid active engagement in quality improvement while nonetheless claiming a privilege for the information they create.

This **Legal**Notes provides an overview of the Act and implementing regulations and assesses their meaning for AF4Q communities.

Background

Efforts to collect patient safety and quality information have been hampered by providers' fears over the use of information in medical malpractice cases or disciplinary proceedings. In its 2000 report, *To Err is Human*, the Institute of Medicine recommended that, with the exception of the most serious adverse events, the special legal protections afforded to peer review of information related to adverse events should be extended to data used to improve patient safety and quality improvement outside of the peer review process.[1] While peer review privilege is aimed at protecting information about serious errors, the privilege created by the PSQIA reaches beyond these limits to shield information related to quality and safety more generally.

In response to this recommendation as well as considerable evidence of problems in patient safety and health care quality generally, Congress passed the PSQIA in 2005.[2] The Act establishes a new federal privilege covering certain information known under the Act as "patient safety work product (PSWP)."[3] In general, the law shields PSWP from discovery in connection with federal or state judicial or administrative proceedings. The PSQIA is not a federal program; instead, federal law essentially creates a safety zone of confidentiality in order to encourage quality improvement activities. It does so through creation of a legal privilege that applies when the conditions of the law are met.

Legal Barriers, based at The George Washington University School of Public Health and Health Services, provides technical assistance for *Aligning Forces for Quality,* a national initiative of the Robert Wood Johnson Foundation.

The purpose of the PSQIA is to create a nationwide privilege in order to encourage critical, internal self-assessment of patient safety and health care quality matters. Without such a privilege, special reports and studies commissioned by a provider to examine safety and quality problems could be "discoverable;" that is, an injured plaintiff could demand the studies as part of its effort to "discover" information relevant to his or her claim and could use that information in a lawsuit against a provider.

Implementing the Law

The Agency for Healthcare Research and Quality (AHRQ) is the federal agency charged with implementation of the Act. In November 2008, AHRQ issued final regulations interpreting the legislation.[4] The final rule, entitled "Patient Safety and Quality Improvement," establishes a process for designating and creating PSWP and for confidentially reporting such information to Patient Safety Organizations (PSOs).

What information is covered by the privilege?

In order to claim the privilege available under the PSQIA, providers must create PSWP and report it to formally recognized PSOs for aggregation and analysis. The concept of "patient safety work product" encompasses "any data, reports, records, memoranda, analyses, or written or oral statements" that meet one of two criteria:

- The materials "could improve patient safety, health care quality, or health care outcomes" and are gathered by a provider to be reported *and are reported to a PSO* or are developed by a PSO to conduct patient safety activities; or
- The materials "identify or constitute the deliberations or analysis of, or fact of reporting to, a patient safety evaluation system." [6]

The important thing about this definition is that it underscores the deliberate and intentional nature of PSWP as part of a formal quality improvement enterprise. As you will see in the discussion below about actual reporting, however, whether the regulations in fact advance this purpose is open to question.

The statute envisions PSWP as part of a conscious and deliberate quality and safety improvement enterprise. The concept of PSWP thus would appear to demand a clear, purposeful patient safety and quality improvement effort, without which there can be no privilege. Under the statute, therefore, *materials not gathered to be reported to the PSO* and not actually transmitted to a PSO would not qualify for a privilege. *Schlegel v. Kaiser Foundation Health Plan*[7] is the only case to date that interprets the meaning of the Act. In *Schlegel*, the defendant was denied the protection of the PSQIA because its internal reports describing problems with its kidney transplant program were neither created as formal patient safety work product nor reported to a patient safety organization.

Deliberations or analyses related to decisions regarding *whether* to report data to a PSO are also protected. A provider may voluntarily remove the information from the "patient safety evaluation system" if it is not PSWP, or if it is needed for non-protected activities, such as fulfilling external reporting obligations.[8]

The privilege specifically does not apply to medical records, billing and discharge information, or other records kept outside safety reporting systems. Furthermore, providers must comply with any state laws that require reporting of patient safety information. Thus, if a patient safety investigation references medical records, the records themselves do not become part of the work product eligible for protection.

Documents created, maintained, or developed separately from a patient safety evaluation system are excluded from the definition of PSWP.[9] Thus, individual patient medical records, billing and discharge information, and any original patient or provider records are not considered PSWP and are not protected under the Act.[10] Indeed, these documents are not PSWP even if they, or copies of them, are entered into a patient safety evaluation system and/or provided to a PSO. In addition, information collected to comply with external reporting requirements is not PSWP. The regulations identify several examples of information that must be reported and does not merit protection as PSWP, including state incident reporting, adverse drug event information reporting, records for compliance with health oversight agency requirements, reporting physician disciplinary actions to the National Practitioner Data Bank, and disclosures required under Medicare's conditions of participation.[11] Thus, a significant amount of data remains outside the PSWP definition.

How is unreported information protected?

In law, many things end up being other than they seem. Even though the statute protects only information that is "reported to a PSO,"[12] the final rule treats as actually reported information that has not been reported to a PSO but that is documented as being within a provider's patient safety evaluation system for future reporting to a PSO. In this case, the information is to be treated as if it was actually reported even though it has not been reported and may never be reported (there is no time limit on future reporting). As a result, the entire concept of extending a federal privilege as a *quid pro quo* for advancing a quality enterprise – the logic behind the Act – seems to collapse in the face of a rule that allows providers to essentially hold onto – for an indefinite time period – important quality and safety information that should actually be reported to

a PSO. To underscore the fact that the privilege can exist under the rules even if there is no active use of information (or even its receipt) by a PSO, the regulations provide that the privilege begins on the date the information is collected.[13]

The extension of PSWP privilege to any information in a provider's patient safety evaluation system – as opposed to information that actually was reported – was one of the most significant changes in the final rule; the proposed rule would have protected only that information actually reported to a PSO. The U.S. Department of Health and Human Services (HHS) justified this change as efficiency-based; that is, it would reduce the need to maintain duplicate reporting systems while giving providers time to determine if the information is truly PSWP.[14] But the final rule does not explain the contradiction inherent in this justification, since the information must have been created precisely to be reported to begin with under the terms of the statute.

The statute defines patient safety work product as:

> "any data . . . (i) which (I) are assembled or developed by a provider *for reporting* to a patient safety organization and are reported to a patient safety organization; or (II) are developed by a patient safety organization for the conduct of patient safety activities; and which could result in improved patient safety, health care quality, or health care outcomes; or (ii) which identify or constitute the deliberations or analysis of, or identify the fact of reporting to, a patient safety evaluation system."[15] (emphasis added)

The final regulation moved away from the requirement that the information be actually reported after numerous commenters noted that information collected for reporting but not yet reported would be unprotected. Rather than limiting the protection to information actually in use in a PSO system, HHS instead revised the definition to read (new language in italics): "patient safety work product means any data . . . [w]hich are assembled or developed by a provider for reporting to a PSO and are reported to a PSO, *which includes information that is documented as within a patient safety evaluation system for reporting to a PSO, and such documentation includes the date the information entered the patient safety evaluation system*."[16] A patient safety evaluation system is broadly defined as any "collection, management, or analysis of information for reporting to or by a PSO,"[17] and does not need to be documented as a system. Thus a provider could document all quality and outcomes data as collected for reporting and gain protected status for the information, regardless of whether the information has actually been – or ever will be – reported to a PSO.

Furthermore, the law creates no affirmative obligation on the part of PSOs to actually *do* something with the information they receive as a condition of maintaining the federal privilege for the materials. That is, a PSO could simply be a repository for such materials and need not demonstrate actual quality and safety activities with the materials in order to keep the federal privilege in place.

What are PSO responsibilities and what kinds of entities can become a PSO?

PSOs are intended to provide two essential services, both of which underscore the concept of an active quality enterprise. The first is gathering information on errors and health care outcomes from a number of patients in a variety of settings and in a uniform format in order to detect patterns of risk and harm. The second is providing the results of their analyses to providers in order to help improve quality and safety. Although the data shared with PSOs will remain confidential, information from the PSO network will be used to analyze national and regional statistics, including trends and patterns of health care errors, and this general information will then be made public in annual quality reports issued by AHRQ.

AHRQ oversees the PSO certification and listing process, while the HHS Office of Civil Rights (OCR) is responsible for compliance with the confidentiality provisions. Any individually identifiable patient information reported to PSOs is subject to the privacy and security standards of the Health Insurance Portability and Accountability Act (HIPPA).

Generally, any private or public entity may become a PSO if it is certified by HHS, which requires demonstration of 15 basic requirements, discussed below.[18] If the entity is a component of another organization, additional requirements apply to ensure that the component PSO is adequately separated from the parent organization with respect to patient safety work product.[19] Thus, a hospital or other provider may develop a component organization to be certified as a PSO if that organization meets the requirements for certification.

To avoid conflicts of interest that could arise, certain entities are excluded from becoming PSOs, such as an agent of an entity that oversees or enforces health care statutes or regulations, a health insurer, health care accreditation or licensing entity, or an entity that manages or operates a mandatory patient safety reporting system. However, a PSO may be a component of one of these excluded entities or may enter into limited collaboration with the excluded entity.[20]

What are the requirements for initial and continued listing of a PSO?

The period of listing of PSOs is three years, unless revoked or relinquished by the Secretary. After three years, the listing will automatically expire unless the PSO renews its certification.[21] Entities that seek initial or continued listing must demonstrate compliance with 15 requirements,[22] which include eight mandatory patient safety activities[23] and seven additional criteria for certification as a PSO.[24] The actual undertaking and completion of patient safety and quality improvement activities is not a requirement; instead, the PSO need demonstrate only that it is making an effort to do so. Similarly, a PSO does not need to collect and analyze data from its entire network, meaning that if certain network members hold data back, the fact that the data analysis covers less than the full network would not disqualify the PSO. PSOs that are components of another organization must make three additional certifications relating to their ability to maintain separate, confidential PSWP and avoid conflicts of interest.[25] Further requirements exist for PSOs that are components of excluded entities.[26]

The final rule does not require component organizations to keep separate information systems from their parent organizations, nor does it preclude the use of shared staff, as was suggested in the proposed rule. However, it does require component PSOs to maintain PSWP separately from the rest of the parent organization, to ensure that members of its workforce do not make unauthorized disclosures to the rest of the parent organization, and to prevent conflicts of interest with the parent organization. The component organization may give the parent organization access to PSWP upon written agreement that access will be granted only for the purpose of enabling individuals or units with access to assist the PSO in its patient safety activities. Access is also conditioned on the existence of appropriate security measures to prevent unauthorized disclosures.

There is no requirement for documentation supporting the attestations made in the PSO certification process, but OCR may conduct unannounced spot checks of listed PSOs or investigate PSOs in response to complaints. Successful applicants are listed publicly for the duration of their listing.

As of February 2, 2010, there are 78 listed PSOs in 29 states and the District of Columbia.[27]

SEVEN PSO CRITERIA

1. PSO's primary activity is to conduct activities designed to improve patient safety and the quality of health care delivery.
2. PSO has appropriately qualified staff (either directly or through contract), including licensed or certified medical professionals.
3. PSO collects PSWP in a standardized manner that permits valid comparisons of similar cases among similar providers.
4. PSO uses PSWP to provide direct feedback and assistance to providers to minimize patient risk.
5. PSO has at least two bona fide contracts with providers to receive and review PSWP (within 24-months of its initial listing and in every subsequent 24-month reporting period).
6. PSO fully discloses to the Secretary any relationships with contracting providers.
7. PSO is not an excluded entity.

EIGHT PATIENT SAFETY ACTIVITIES

PSOs must have policies and procedures in place to:

1. Make efforts to improve patient safety and the quality of health care delivery.
2. Collect and analyze PSWP.
3. Develop and disseminate information to improve patient safety, such as recommendations, protocols, or information regarding best practices.
4. Utilize PSWP to encourage a culture of safety and to provide feedback and assistance to minimize patient risk effectively.
5. Maintain procedures to preserve the confidentiality of PSWP.
6. Provide appropriate security measures to preserve confidentiality of PSWP.
7. Utilize qualified staff.
8. Operate a patient safety evaluation system (the collection, management or analysis of patient safety information) and provide feedback.

When may patient safety work product be disclosed?

PSWP is privileged, which means it cannot be subpoenaed or offered into evidence in legal proceedings, including medical liability cases or professional disciplinary proceedings.[28] PSWP is also exempt from the Freedom of Information Act or similar federal or state public records laws. However, providers must continue to comply with federal, state and local reporting laws. There are many circumstances in which PSWP will not be considered confidential and therefore, may be disclosed (see text box).[29] The regulations also contain a safe harbor provision under which the disclosure

of PSWP to someone other than a PSO will not be considered a violation of the regulation if the PSWP does not either assess an identifiable provider's quality of care or pertain to actions or failures to act by an identifiable provider.[30]

The regulations' protections extend back not only to the time of actual reporting to a PSO but also to the time of collection within a patient safety evaluation system where the intent was to report to a PSO. These protections reach back to the time of enactment of the PSQIA in 2005, even though the final regulations took effect January 19, 2009.[31] Violations of the disclosure regulations could result in civil fines up to $10,000 for each violation.[32]

Nonidentifiable PSWP is exempt from both the privilege and confidentiality requirements, but de-identified information clearly is less useful for purposes[33] of information transparency. Under the regulations, the concept of "identifiable" refers to the identity of the provider or reporter of the patient safety information, not the identity of the patient. (Patient privacy continues to be protected by the privacy and security regulations under HIPAA, as discussed below.) PSWP is nonidentifiable with respect to a provider or reporter if: 1) a person with appropriate statistical knowledge determines that there is only a very small risk that the provider or reporter could be identified from the information; or 2) an extensive list of identifiers is removed from the information, including all names and identifying numbers of providers and associated individuals or organizations, all geographic subdivisions smaller than a state, including zip codes, all elements of dates related to a patient safety event except years, and other unique characteristics; and 3) the person or PSO making the disclosure has no knowledge that the information could be used to identify the particular provider or reporter. Limited information may be retained to aggregate data for research, such as the first three digits in zip codes (as long as there are more than 20,000 people in the combined geographic area) and the year. Thus, although some nonidentifiable data would be exempt from privilege and confidentiality regulations, such as safety trends over large areas, PSWP cannot be published for the purpose of comparing provider performance.

To simplify the aggregation and analysis of PSWP, AHRQ published clinical definitions and technical requirements for the uniform collection and reporting of patient safety data, called the "Common Formats."[34] The first version of the Common Formats focuses on inpatient hospital reporting, but future versions will apply to other settings, including nursing homes, ambulatory surgery centers and physician offices. De-identified information sent to the network of patient safety databases (to be created and maintained by the Secretary) using the Common Formats will be used for AHRQ's annual National Healthcare Quality Report. Although the use of the Common Formats is currently voluntary, the regulations require PSOs to collect information in a standardized manner that permits valid comparisons, which should encourage the use of the Common Formats.

HIPAA privacy and security rules continue to apply

Under the regulations, confidentiality and privilege protections only apply to information produced by PSOs and do not alter or affect HIPAA's requirements for protecting patient information. Providers must still comply with HIPPA, state reporting requirements and more protective state confidentiality laws. However, the Act specifies that for purposes of applying the HIPAA privacy rule, PSOs will be treated as "business associates" of providers, and their patient safety activities will be deemed to be "health care operations." Therefore, providers will not be required to obtain patient authorizations to disclose PSWP containing protected health information to PSOs.[35] The act also applies the

EXCEPTIONS TO CONFIDENTIALITY OF PSWP

1. Disclosure in criminal proceedings after judge determines that PSWP:
   a. contains evidence of a criminal act;
   b. is material to the proceeding; and
   c. is not reasonably available from another source.
2. Disclosure to permit equitable relief for someone who suffered an adverse employment action because of reporting to a PSO.
3. Disclosure authorized by identified providers.
4. Disclosure for patient safety activities:
   a. between a provider and PSO;
   b. to a contractor of a provider or PSO;
   c. among affiliated providers; or
   d. another PSO or provider for patient safety activities if identifying information removed.
5. Disclosure of nonidentifiable PSWP.
6. Disclosure for sanctioned research if permitted by HIPAA.
7. Disclosure to FDA.
8. Voluntary disclosure to an accrediting body if provider consents, with no further disclosures or retaliation against provider.
9. Disclosure for business operations.
10. Disclosure to law enforcement for necessary criminal law investigation.

HIPAA definition of individually identifiable health information to "identifiable PSWP" under the Act.

Implications for *Aligning Forces for Quality*

The fundamental purpose of the PSQIA was to encourage active self-examination on matters of quality and safety, and to encourage providers to share the results of their efforts through patient safety organizations capable of supporting a community-wide quality undertaking. Whether the law will achieve these results is open to question, and even if results are achieved, it is not clear that communities will ever be able to actively engage with providers around their quality improvement efforts. The law, as implemented by regulations, contains two crucial limitations. First, providers can designate information as PSWP even though they never report it to a PSO or use it. Second, a PSO is not required to generate actual quality improvement and safety output (such as aggregated safety reports or feedback to providers) to remain a designated PSO. In other words, the privilege extends to PSWP even if nothing is done with the information and the information is never transmitted.

While the PSQIA does not appear likely to produce visible changes in active quality engagement in exchange for a legal privilege, it is possible that AF4Q communities may benefit if providers elect to move forward with patient safety initiatives. Ideally, the existence of a legal privilege will encourage providers to report quality information they might otherwise conceal out of fear of liability, and the Act could offer a forum for greater sharing of patient safety and quality information among providers. The question is whether providers are willing to voluntarily reveal to other providers in their communities, with whom they may compete, information that could be extremely damaging if made public through a security breach. If each provider in a community creates a PSO, this of course defeats the purpose of having providers engage in collective exchange of information that may shed light on safety and quality. Furthermore, because the law provides for the reporting and sharing of information to take place out of public view, its value cannot be assessed, nor can it serve as the basis for quality comparisons between providers or for conditioning payment on quality of care.

In addition, the broad definition of PSWP and the protection it enjoys may encourage providers to report all quality information to PSOs instead of to other quality improvement programs that are able to generate public information. To the extent that *Aligning Forces for Quality* projects involve collecting quality data from providers, the providers may be less willing or able to provide that information when they can shield any negative information from public view in a PSO. Organizations that want to publicly report quality information as well as reporting to a PSO will face an additional administrative burden since, in order to continue to report data including the provider's identity to a group other than the PSO, the organization would have to maintain a system for collecting those data entirely separate from the patient safety evaluation system. There is also the potential for confusion among organizations that believe they cannot disclose quality information to organizations other than PSOs under any circumstances.

This law does not entirely shut down the exchange of information. Billing information and original medical records are not considered PSWP, so information can be culled from those sources and disclosed (subject to HIPAA, the terms of data use agreements and any other restrictions) and identifiable PSWP can also be disclosed if authorized by all identified providers. However, the PSQIA and implementing regulations certainly complicate efforts to publicly disclose patient safety and quality information and provide an easy mechanism for shielding such information, which is likely to hinder public reporting efforts.

[1] *To Err is Human: Building a Safer Health System.* Committee on Quality of Health Care in America, Institute of Medicine (Washington, DC): National Academies Press, 2000.

[2] Patient Safety and Quality Improvement Act of 2005, Public Law 109-41, 42 U.S.C. 299b-21 et seq.

[3] 42 U.S.C. § 299b-22(a)(2).

[4] Patient Safety and Quality Improvement, Final Rule, 73 Fed. Reg. 70732 et seq. (Nov. 21, 2008) (to be codified at 42 C.F.R. § 3.10 et seq.).

[5] Hansen, Dave. "Rules aim for better patient safety through confidential error report." *American Medical News*, March 10, 2008, *http://www.ama-assn.org/amednews/2008/03/10/gvl10310.htm* (accessed March 1, 2010).

[6] 42 C.F.R. § 3.20 (2009).

[7] 2008 WL 4570619, E.D.Cal., October 14, 2008 (unreported).

[8] 72 Fed. Reg. 70741-70742 (Nov. 21, 2008).

[9] 42 C.F.R. § 3.20 (2009).

[10] 73 Fed. Reg. 70740 (Nov. 21, 2008).

[11] 72 Fed. Reg. 70742-70743 (Nov. 21, 2008).

[12] 42 U.S.C. § 299b-21(7)(A)(i)(I).

[13] 42 C.F.R. § 3.20 (2009) (definition of patient safety work product).

[14] HHS explained its reasoning for the change: "The alternative is a system that encourages providers to indiscriminately report information to PSOs in a race for protection, resulting in PSOs receiving large volumes of unimportant information. By offering providers the ability to examine patient safety event reports in the patient safety evaluation system without requiring that all such information be immediately reported to a PSO and by providing a means to remove such information from the patient safety evaluation system and end its status as patient safety work product, the final rule permits providers to maximize organizational and system efficiencies and lessens the need to maintain duplicate information for different needs." HHS went on to acknowledge that an issue of concern was that "because information may be protected back to the time of collection, providers are no longer required to promptly report information to a PSO to ensure protection. Although we believe this is an unavoidable result of the modification, we believe the likely impact may be rare because providers are likely to engage PSOs for their expertise which requires such reporting." 73 Fed. Reg. 70741-70742.

[15] 119 Stat. 424, § 921(7), 42 U.S.C. § 299b–21(7) (2005).

[16] 42 C.F.R. § 3.20 (2009).

[17] 42 C.F.R. § 3.20 (2009); 119 Stat. 424, § 921(6), 42 U.S.C. § 299b–21(6) (2005).

[18] 42 C.F.R. § 3.102(a) (2009).

[19] 42 C.F.R. § 3.102(c) (2009). The component PSO must certify that it will maintain patient safety work product separately from the rest of the parent organization, that none of its staff make unauthorized disclosures of patient safety work product to the rest of the parent organization, and that the pursuit of the mission of the component PSO will not create a conflict of interest with the rest of the parent organization.

[20] 42 C.F.R. § 3.102(c)(4) (2009).

[21] 42 C.F.R. § 3.104(e) (2009).

[22] 42 C.F.R. § 3.102(b) (2009).

[23] 42 C.F.R. § 3.102(b)(1)(i) (incorporating by reference the definition of patient safety activities in 42 C.F.R. § 3.20) (2009).

[24] 42 C.F.R. § 3.102(b)(2)(i) (2009).

[25] Restrictions include the requirements that PSOs: 1) maintain PSWP separate from the parent organization and establish security measures to maintain the confidentiality of PSWP; 2) not make an unauthorized disclosure of PSWP to the rest of the organization; and 3) assure that the pursuit of its mission will not create a conflict of interest with the rest of the parent organization. 42 C.F.R. § 3.102(c)(1)-(3) (2009).

[26] 42 C.F.R. § 3.102(c)(4) (2009).

[27] Agency for Healthcare Research and Quality, "Listed Patient Safety Organizations," *http://www.pso.ahrq.gov/listing/psolist.htm* (accessed March 1, 2010).

[28] 42 C.F.R. § 3.204 (2009).

[29] 42 C.F.R. § 3.206 (2009).

[30] 42 C.F.R. § 3.206(c) (2009).

[31] 73 Fed. Reg. 70741-42 (Nov. 21, 2008).

[32] 42 C.F.R. § 3.404 (2009).

[33] 42 C.F.R. § 3.204(b)(4) and 3.206(b)(5) (2009).

[34] 74 Fed. Reg. 45457-45458 (Sept. 2, 2009).

[35] 73 Fed. Reg. 70732 (Nov. 21, 2008).