

Seventh Floor
1501 M Street, NW
Washington, DC 20005-1700
Phone: (202) 466-6550 Fax: (202) 785-1756

MEMORANDUM

To: Clients and Friends
From: Rebecca Burke
Date: May 8, 2009
Re: Patient Safety Organizations: Risks and Opportunities

PATIENT SAFETY ORGANIZATIONS: RISKS AND OPPORTUNITIES

The Patient Safety and Quality Improvement Act of 2005 (the Act), enacted in the wake of the landmark Institute of Medicine report on medical errors, creates both risks and opportunities for health care providers. The Act, which amends the Public Health Service Act, provides for the formation of new organizations, known as patient safety organizations (PSOs), whose purpose is to collect from reporting health care providers, including physicians, information on patient safety events and provide analysis and feedback to the reporting providers on effective strategies to improve patient safety. 42 U.S.C. §§ 299b-21 – 299b-26. Once a PSO is certified by the Agency for Healthcare Research and Quality (AHRQ), “patient safety work product” (PSWP) reported to it is considered both privileged and confidential. The AHRQ recently issued final PSO regulations which took effect January 19, 2009. 73 Fed. Reg. 70732 et seq. As of this date, 58 PSOs have been certified by the agency.

Although PSOs can be useful tools for providers seeking to understand and minimize risks and hazards in the delivery of patient care, PSO operations are not without risk and their success is entirely dependent on the ability of the PSO and reporting providers to keep this highly sensitive information from unauthorized or inappropriate disclosure.

Who Can Become a PSO?

Generally, any public or private entity that meets the AHRQ criteria can be listed as a PSO. However, there are certain entities that are prohibited from establishing PSOs, including health insurers, regulatory agencies or their agents, licensure and accreditation agencies and entities that administer a governmental patient safety reporting system to which health care providers are required to report by law.

Provider organizations, including regional hospital associations or national physician specialty organizations, may wish to establish PSOs to encourage the reporting of patient safety events and provide a mechanism by which providers can learn from their mistakes. In addition, reporting registries may also be interested in expanding the scope of their activities to include becoming a PSO.

Requirements of PSOs

In order to qualify as a PSO an entity must meet a number of requirements including:

- Have written policies in place to perform eight specific patient safety activities;
- Maintain procedures to preserve confidentiality of PSWP;
- Provide security measures with respect to PSWP;
- Utilize qualified staff;
- Provide feedback to participants in a patient safety evaluation system;
- Have at least two bona fide contracts with different providers ; and
- Collect data from providers in a standardized manner.

Additional requirements apply if the PSO is a component of another organization, i.e. a unit or division of another legal entity or an entity that is owned or controlled by another legally separate parent organization. Component organizations must maintain PSWP separately from the rest of the parent organization and meet a number of requirements designed to maintain the PSO operations separate from those of the parent organization and prevent unauthorized access by the parent. In addition, no conflicts of interest must exist between the component PSO and its parent organization.

Termination of PSO Operations

AHRQ certification of a PSO lasts three years after which it may be renewed. If a PSO does not seek renewal, its status will automatically expire. In addition, a PSO can decide to voluntarily relinquish its certification. A PSO that does not comply with the PSO regulations may have its certification revoked. If a PSO's certification is revoked or voluntarily relinquished (including a decision not to renew), the PSO is required to either transfer PSWP to another PSO, with approval of the source, or return the data to the provider who submitted it. If returning the data is not practicable, the PSWP must be destroyed. 42 C.F.R. § 3.108.

Privilege and Confidentiality Protections

The Act states that PSWP is “privileged” and (subject to certain exceptions) cannot be (1) subject to subpoena or discovery or admitted as evidence in any Federal, State or local judicial proceeding; (2) admitted in a State professional disciplinary proceeding; or (3) obtained from the government through a Freedom of Information Act request. The Act specifically provides that it supersedes any less stringent state or local laws.

The Act also provides that PSWP is “confidential” and (again, subject to certain exceptions) cannot be disclosed. Further, since most entities reporting to PSOs will be “covered entities” under the HIPAA Privacy Rule, to the extent that PSWP includes protected health information (PHI), disclosure is also subject to the HIPAA restrictions. For this purpose, the Act provides that disclosure of PHI as part of PSWP to a PSO is considered “health care operations” and thus an authorized disclosure under HIPAA. Further, a PSO would be considered a “business associate” of the covered entity and subject to the business associate requirements of the HIPAA Privacy Rule.

Confidentiality and privilege protections also apply to redisclosure. Thus, if PSWP is disclosed, either permissibly or impermissibly, the protections continue to apply and would limit redisclosure of the information. Non-identifiable PSWP can, however, be disclosed. Non-identifiable PSWP is PSWP from which specific identifiers have been removed, as set forth in the PSO regulations.

Exceptions to both the privilege and confidentiality protections include:

- Disclosure for use in criminal proceedings if the court has made an *in camera* determination that the PSWP contains evidence of a criminal act, and the information is material and not otherwise available;
- Disclosure in connection with retaliatory employment actions brought against an individual who reports information to a PSO, to the extent necessary to permit equitable relief, subject to a protective order;
- Disclosure where authorized in writing by each provider identified in the work product; and
- Disclosure to the Secretary in the context of an investigation to determine compliance or enforcement of the Act of the HIPAA Privacy Rule.

There are a number of other exceptions that apply only to the confidentiality protections. They permit:

- Disclosure to a contractor or a provider or PSO for patient safety activities;
- Disclosure among affiliated providers;
- Disclosure by a PSO to another PSO or another provider on the condition that the information is de-identified;
- Disclosure to the FDA by entities required to report to the FDA;
- Voluntary disclosure to an accrediting body subject to certain conditions;

- Disclosure for business operations such as to attorneys or accountants; and
- Disclosure to law enforcement if it relates to commission of a crime or if an individual “reasonably believes” a crime has been committed.

Providers and PSOs may, by contract, agree to stricter confidentiality provisions. Such provisions will not be enforced by the Federal government, however.

Enforcement of Confidentiality and Privilege Protections

The privilege protections that apply to PSWP are not enforced by the federal government. Rather, the Act specifically leaves enforcement to the judicial system through individual litigation in local, state and federal courts and administrative bodies. Thus, it will be the responsibility of a reporting provider or PSO to defend the privilege in court against parties seeking access.

In contrast, the confidentiality protections of the Act, which include the imposition of civil monetary penalties of up to \$10,000 per violation, are enforceable by HHS. That agency has formally transferred its enforcement authority to the HHS Office of Civil Rights. This authority includes the right to investigate complaints of a breach of confidentiality and to conduct its own compliance reviews. Civil monetary penalties can be imposed against an entity when there is a “knowing or reckless” violation of confidentiality and an agent’s acts can be attributed to its principal. The law provides that if CMPs are imposed under the PSO Act, they will not also be imposed under the HIPAA Privacy Rule for the same conduct.

Risks Associated with PSO Operations

Possibly the greatest risk to both reporting providers and PSOs is unauthorized disclosure of PSWP resulting from a security breach. Although PSOs are required, as a condition of AHRQ listing, to meet stringent security requirements with respect PSWP in both electronic and other media, cases of unauthorized disclosure or breaches of security could still occur. PSOs are required to provide notification to providers if the PSWP they submitted to the PSO was subject to an unauthorized disclosure or security breach. 42 C.F.R. § 3.102 (b). This is required regardless of whether the data was secured or unsecured. Thus, the notice requirement applicable under the PSO Act is more stringent than that under HIPAA as enacted in the ARRA which only requires notice of a security breach for “unsecured” PHI. It is also possible that state law will impose even more stringent notification procedures.

The PSO regulations provide that PSWP continues to maintain its privileged and confidential status in the event of a security breach or unauthorized disclosure. 42 C.F.R. § 3.208. Thus it would continue to be inadmissible and not subject to discovery in judicial or disciplinary proceedings. However, once PSWP security has been breached, it may be difficult to control the damage despite regulatory protections.

Reporting providers incur similar risks if they do not maintain PSWP in a secure environment. A hospital, for example, could be subject to civil monetary penalties if one of its employees discloses confidential PSWP without authorization.

Additional risks can result from authorized disclosure pursuant to the numerous exceptions in the law. While an authorized disclosure may not be a violation of the PSO Act, a provider whose PSWP is disclosed through a legal exception could still be disadvantaged or harmed. Moreover, with respect to the privilege protection, a reporting provider may have to rely on a PSO to enforce the privilege in a judicial or other proceeding. There is nothing in the regulations which requires a PSO to notify a provider that its PSWP is being released under any of the exceptions to either the privilege or confidentiality provisions. Thus, a PSO could make an authorized disclosure of a provider's PSWP without having to inform the provider and without the provider having an opportunity to object or intervene.

Risk Mitigation Strategies

Providers

Some provider risks may be addressed through contracts with the PSO. For example, the contract could require that PSWP be maintained, to the extent feasible, in a "secured" form as defined by HHS guidance issue to be issued under the HIPAA Privacy Act and the ARRA security breach notification provisions.

Authorized disclosures permitted under the regulations could be limited by contract, to the extent legally permissible. In addition, the contract could require the PSO to notify the reporting provider of any requests it receives for release of a provider's PSWP, for example in the context of a criminal or whistleblower suit. Providers could also include indemnification provisions in the event they are held liable for an unauthorized disclosure that is due to the PSOs negligence.

Providers may also want to obtain an assurance from a PSO that it will legally defend against requests from outside parties for disclosure of PSWP if that disclosure would appear to violate privilege and confidentiality protections. Finally, they should ensure that the PSO has adequate liability insurance that covers security breaches related to PSWP.

PSOs

PSOs can manage risk by employing, to the maximum extent feasible, technology and methodologies that render PSWP unusable or unreadable to unauthorized individuals. However, since these methods are not infallible, PSOs should make sure they have adequate liability insurance which would cover this type of breach in the event that they are held liable. PSOs may also, through contract, seek to obtain waivers or limitations on liability from reporting providers in the event of a breach

perhaps in return for a commitment to undertake certain notification and mitigation strategies.

Summary

If PSOs are to make a meaningful contribution to patient safety and reduction of medical errors, reporting providers must feel confident that PSWP will not be subject to security breaches. As recent events reported in the media demonstrate, security breaches of confidential electronic health information are not uncommon and, according to some, cannot be entirely prevented. With PSOs the risk is heightened since PSWP contains not only HIPAA protected PHI, but highly sensitive information about health care facilities and professionals which, if released, could cause significant damage to reputation and standing in the community. Therefore, PSOs and providers submitting PSWP must carefully assess and take steps to mitigate risks associated with such breaches.

If you have questions about PSOs or this memorandum please contact Rebecca Burke, Esq., 202-872-6751 or Rebecca.burke@ppsv.com