CNA
We can show you more.®

VANTAGEPOINT®

VP 2019 ISSUE 1

Patient Safety Data: A Guide to Preventing Unwanted Disclosures

Quality and safety improvement in healthcare settings depends upon candid discussion of process problems, provider misjudgments, staff miscommunications, adverse events, near misses and other lapses. By sharing information in an atmosphere of openness and accountability, providers and staff can learn from mistakes and make necessary changes.

The professional obligation to track and analyze errors involves creating highly sensitive and potentially compromising reports, analyses, data aggregations and other documents. State and federal law provides some degree of protection against disclosure of findings created and used expressly for quality improvement or evaluative purposes. However, the compiling of safety-related data continues to present significant liability exposures for healthcare organizations and providers in the form of discovery challenges made in the course of litigation.

Did someone forward this newsletter to you? If you would like to receive future issues of *Vantage Point*® by email, please register for a complimentary subscription at **go.cna.com/HCsubscribe**.

In today's legal environment, organizations must be cognizant of the risk of data discoverability, adopting and enforcing measures that encourage the collection and preservation of sensitive information while protecting it from unwanted disclosure. To clarify this legally and procedurally complex topic, this edition of *Vantage Point*® focuses on three major administrative processes that produce patient safety data – peer review, quality assurance and performance improvement (QAPI), and risk management – and examines the protections and limitations pertaining to each. The issue also provides reminders designed to help providers, staff and organizational leaders avoid common legal and regulatory missteps that could weaken defensibility. Finally, it includes a readiness checklist of practical recommendations intended to help readers maximize confidentiality of patient safety and performance-related data.

PEER REVIEW DATA

Peer review is the process whereby physicians and other medical providers assess colleagues' clinical competence and behavior in relation to applicable standards of care and professional conduct. Peer review activities are generally conducted in the following circumstances:

- **When a physician requests medical staff privileges** or changes to existing privileges.
- **For accreditation purposes** following evidence of substandard physician performance, as required by the Joint Commission.
- **To improve quality of care** through random case selection or review and analysis of cases with poor outcomes.

Different institutions conduct the peer review process in widely varying ways.

For peer review to work, participants must be free to discuss incidents and concerns without fear of negative legal repercussions. Healthcare organizations, therefore, must ensure that peer review findings remain confidential and protected from discovery by third parties, as failure to safeguard information may result in participants being named in retaliatory lawsuits. Such unwanted disclosure also may have a chilling effect upon the future involvement of providers in this vital process.

Both state and federal law offer statutory privileges relating to peer review. However, these safeguards are subject to limits in terms of both scope and degree of protection.

State law protection for peer review data. All 50 states, as well as the District of Columbia, have enacted statutes offering various levels of discoverability protection to certain peer review-related records and documents. Some states protect documents *generated by* a peer review committee – e.g., reports, statements, memoranda, proceedings, findings – but do not safeguard records *given to* a committee, such as risk management investigations of adverse incidents. At the other end of the spectrum are states that treat as confidential *all* information considered by a peer review committee in pursuit of its quality assurance mission. State statutes are readily available for online scrutiny. Organizational leaders and providers should periodically review these laws, consulting with legal counsel if questions arise concerning their term and scope.

Even state statutes drafted with the intent of providing a full range of protection for peer review materials often have limitations regarding discovery. As a result, claims of peer review protection may be challenged in state court, a fact that should be kept in mind when drafting documents.

In determining the status of records, courts often focus on the questions of how and why they were created. Peer review-related documents may become discoverable in the event that …

- **Peer review matters are addressed through general hospital procedures,** instead of by a centralized, formal peer review committee.
- **Documents or other communications are shared with parties who should not be privy to the information.** For example, a discussion of case findings at a staff meeting attended by hospital administrators or other non-physicians would likely not be exempt from discovery.
- **Reports are generated outside the peer review process,** such as investigative findings or witness statements compiled by risk managers or human resources administrators.
- **A claim of employment discrimination has been instituted against a hospital by a physician,** or allegations of negligent supervisory or credentialing practices are asserted in relation to the peer review process.
- **A state medical licensing board requests peer review information** for disciplinary purposes.
- **A physician is charged with homicide** associated with criminal negligence, an unusual occurrence.

Courts also may apply a "balancing test" to ascertain whether a plaintiff should have access to protected peer review data, weighing the trouble and expense of producing peer review documents against the possibility of obtaining this information in some other and potentially simpler manner.

Even state statutes drafted with the intent of providing a full range of protection for peer review materials often have limitations regarding discovery.

Federal protection for reviewers. The federal Health Care Quality Improvement Act of 1986 (HCQIA) applies to the *practice* of peer review, rather than the documents consulted. The HCQIA establishes a qualified immunity for persons who provide information to a professional review body regarding the competence or professional conduct of a physician or other medical provider. (See "Basics of the Health Care Quality Improvement Act" below.) Those protected under HCQIA include investigators, witnesses, fellow professionals and others involved in the peer review process.

The HCQIA was enacted primarily to shield participants in peer review processes from retaliatory lawsuits, thus enabling providers to freely engage in discussions about quality of care. In general, this federal law provides peer review records a narrower range of confidentiality than do state statutes, and does *not* protect peer review records or related materials from discovery and court subpoena if a malpractice claim is filed against the provider under review.

BASICS OF THE HEALTH CARE QUALITY IMPROVEMENT ACT (HCQIA)

HCQIA, enacted by Congress in 1986, protects physicians and other medical and dental providers who conduct peer review activities in good faith. The act has two primary components:

Part A provides immunity for hospitals and reviewers from peer review-related lawsuits brought by physicians and other medical providers. To qualify for immunity under HCQIA, a professional review action must be taken …

- **In the reasonable belief that the action will further the committee's purpose** of enhancing healthcare quality.
- **After the committee has made a reasonable effort to obtain the facts** of the matter under review.
- **After the provider under review has been afforded adequate notice** and fair hearing procedures.
- **In the reasonable belief that the final decision is warranted** after the committee has duly considered the facts and the provider has been given a fair hearing.

Part B establishes the National Practitioner Data Bank (NPDB). The NPDB is a digital repository of reports of medical malpractice payments made and other adverse actions involving healthcare practitioners and suppliers. It is intended to protect healthcare consumers and organizations by disclosing providers' history of care that resulted in patient injury, as well as actions taken by hospitals with respect to staff privileges.

Important Reminders

1. **HCQIA does not protect peer review records from discovery in federal court.** Substantive deliberations concerning possible violations of federal law – such as the Emergency Medical Treatment & Labor Act (EMTALA) – are not protected from disclosure if civil litigation is removed from state to federal court. For this reason, it may be prudent to submit cases involving potential violations of federal law to hospital legal counsel rather than the peer review committee, thus establishing attorney-client privilege.
2. **Materials must be created solely for peer review purposes to enjoy state-based protections, and the peer review process must comply with applicable statutes.** For example, some states require that the peer review committee operate under the aegis of the medical staff, rather than the hospital administrative staff. Other states specify that the committee must consist primarily of physicians in order to qualify for confidentiality privileges.
3. **Documents prepared by an outside reviewer are not necessarily protected against discovery.** If there is no qualified expert on staff, or potential reviewers are deemed to be competitors of the provider under review, an external reviewer may be selected. Consult with legal counsel to clarify confidentiality implications and ensure that outside contractors are impartial, appropriately credentialed and qualified to conduct peer review under relevant state laws.
4. **Reports containing the findings, deliberations and analyses of a peer review committee are confidential, and should not be shared with other committees or hospital departments.** This information should remain in a secure location within the medical staff office. By forwarding a peer review report to the risk management department, for example, an administrator may unwittingly weaken discoverability protections. (Typically, the risk manager will be informed through other channels of any event giving rise to a peer review exercise, such as a patient death in the operating room, and may choose to conduct an independent investigation.)

QAPI DATA

Hospitals and providers may be reluctant to share information regarding performance indicators, survey findings, complaints and other sources of QAPI data due to the possibility of legal action if details are discovered by plaintiff attorneys. To promote voluntary reporting by providers and healthcare organizations, the Affordable Care Act requires hospitals with 50 or more beds that partner with state health insurance plans to maintain a patient safety evaluation (PSE) system, which is a formal, internal mechanism designed to review and analyze adverse events. Patient safety organizations (PSOs) are federally designated external bodies (such as the Center for Patient Safety, ECRI Institute PSO and others) designed to help healthcare organizations identify and address risks by creating a secure environment where providers and administrators can collect, analyze and share patient safety data without being subject to legal discovery.

PSO networks help organizations and providers share data with other healthcare professionals, utilizing common reporting formats developed by the Agency for Healthcare Research and Quality (AHRQ). Information reported to a PSO is afforded confidentiality protection under the federal Patient Safety and Quality Improvement Act (PSQIA). The PSQIA helps safeguard providers in hospital and non-hospital settings who report safety-related information to a PSO via their PSE system. (See "Understanding the Patient Safety and Quality Improvement Act (PSQIA)" at right.)

Adverse event reports compiled through a PSE system for later submission to a PSO are protected, as are the analysis and evaluation of those events.

UNDERSTANDING THE PATIENT SAFETY AND QUALITY IMPROVEMENT ACT (PSQIA)

The PSQIA was enacted by Congress in 2005 to improve patient safety and healthcare quality by establishing a voluntary, confidential and non-punitive system for physicians and other healthcare providers who report medical errors and near-miss data to a designated PSO through their internal PSE system, thus encouraging a free flow of vital information and fostering a culture of safety. Prior to the passage of the Act, protection of patient safety data from discovery in a professional liability lawsuit was primarily a function of state law. The PSQIA provides broad confidentiality provisions on the federal level. If stronger protection for patient safety work product is offered at the state level, then the act does not preempt state law.

The PSQIA is complemented by the Patient Safety Rule, which establishes a framework for reporting patient safety information to PSOs for purposes of data aggregation and analysis. Adverse event reports compiled through a PSE system for later submission to a PSO are protected, as are the analysis and evaluation of those events. Prior to submitting an event report to the PSO, providers may change their mind and "unprotect" the event report. This option, known as the *drop out provision*, is intended to provide some flexibility for organizations as they work through their various external obligations. The drop out provision does not apply to information that describes or constitutes the deliberations or analyses of a PSE system in regard to a particular event. However, it would cover, for example, aggregate reports that may be requested by external regulatory bodies. When removing information from the PSE system, it is necessary to date the document or data and label it as "voluntarily removed." Upon removal, the information is no longer protected.

Defining patient safety work product. The PSQIA protects from disclosure patient safety work product (PSWP), which is generally defined as data, reports, records, memoranda, analyses, and written or oral statements that are …

- **Compiled by a provider for the express purpose of being reported to a PSO,** and are so reported.
- **Developed by the PSO** through its mission to improve patient safety and healthcare quality.
- **Included in the fact-reporting process of a PSE system,** or related to a PSE's deliberations or analysis.

Information collected, maintained or developed separately from a PSE system is not considered PSWP. (See the chart below for a listing of information that is and is not protected within the parameters of PSWP privilege.)

Under the PSQIA, patient safety work product is not subject to discovery or disclosure in civil or administrative proceedings. It is also protected against requests under the Freedom of Information Act or professional proceedings by a disciplinary body, such as a state licensing board. However, PSWP may be disclosed …

- **If authorized in writing** by each provider identified in the PSWP.
- **To an accrediting body,** subject to limitations in use and provided all identified providers agree, in writing, to the disclosure.
- **In a criminal proceeding,** as opposed to a civil action.
- **In an action by an employee who asserts retaliation** for reporting PSWP.
- **To a regulatory body** – such as the Food and Drug Administration (FDA) or the U.S. Department of Health and Human Services (HHS) – when authorized by the relevant provider.

In general, information disclosed under these limited permissible circumstances retains some level of confidentiality. For example, if PSWP is disclosed to the FDA for the purpose of evaluating the quality, safety or effectiveness of a healthcare device or product, the data remain privileged and may not later be disclosed in a professional liability lawsuit.

PSOs and the peer review process. Participating in a PSO offers organizations an additional measure of security when conducting peer review activities, permitting reviewers to designate patient records – as well as case review findings, letters of inquiry and other documents – as federally protected PSWP. Classifying peer review activities and materials as PSWP can be especially helpful in states where protection against legal discovery has been weakened either by statute or through case law.

What Constitutes Patient Safety Work Product (PSWP)?

PSWP:	NOT PSWP:
Information reported by a provider to a PSO, and which has been collected expressly for this purpose. Such information may include ... - Reports - Oral and written statements - Records - Memoranda - Data - Root cause analyses and deliberations	Information collected outside the PSE system, compiled from (rather than reported to) the system or gathered for another reason. Such information may include ... - Patient healthcare information records - Discharge records - Inspection or survey reports - Provider records - Corporate records maintained for federal or state regulatory purposes - Billing records

Source: "How to Structure Health Care Systems, Clinically Integrated Networks and Other Affiliated Providers in Order to Benefit from Patient Safety Act Protections." (See "Quick Links" on page 11 for full citation.)

Important Reminders

1. **QAPI data must be collected within a PSE context to secure protection as PSWP.** Otherwise, state-mandated safety and quality regulations may nullify confidentiality protections. For example, if incident or medication error reports are collected pursuant to state regulations and *also* for the purpose of reporting to a PSO, attempts to label them as PSWP may face legal challenge. Such materials are known as "dual-purpose" documents. (See "Relevant Case Law: Dual-purpose Documents and PSO Confidentiality Protections" at right.)
2. **QAPI-related analyses and other deliberations must be conducted within the structure of a PSE system** in order to qualify for PSWP status and related privileges. For example, if a root cause analysis is performed to determine the reason for an error, but the findings are not reported to the PSO, the information may be discoverable unless protected by state law.
3. **Written statements must be dated** to qualify for PSWP designation.
4. **Various types of licensed healthcare providers and facilities may contract with a PSO,** and also may work with more than one PSO. Hospitals, physicians, emergency medical services, ambulatory centers, aging services organizations and pharmacies may establish a PSE system to collect patient safety-related documents, data and evaluations.
5. **Providers that participate in QAPI activities cannot submit all of their data to a PSO merely for the purpose of obtaining a blanket PSWP privilege.** The data must meet the three criteria listed on page 5 in order to qualify for the privilege.
6. **PSWP should not be disclosed to the Centers for Medicare & Medicaid Services and state or other surveyors.** However, they typically do enjoy access to the following materials:
   - **All original documents** that are not labeled as PSWP, such as patient, billing and discharge records.
   - **Staff interviews** relating to clinical care and processes.
   - **Incident reports** that serve a dual purpose.
   - **Information about the process for reporting adverse events and patient safety issues** to a PSE system for evaluation.
   - **Action plans or corrective actions** taken as a result of an evaluation.

For a sample flowchart designed to help organizations establish a PSO, share information and maximize available protections, see "Working With a PSO: One Approach" from the AHRQ. For additional resources, see PSO Resources and Toolkit from the Center for Patient Safety.

RISK MANAGEMENT DATA

Determining whether data regarding adverse patient events, near-misses or unsafe conditions are protected against discovery in a malpractice lawsuit can be a challenge. Often, risk management information relating to medical errors and adverse occurrences is collected both for purposes of reporting to a PSO and also in the ordinary course of business, e.g., for reasons relating to reimbursement, accreditation or regulatory compliance. Incident reports, occurrence screens, investigative findings and associated analyses are common examples of data collected or scrutinized for dual purposes. Not surprisingly, these documents frequently are the subject of legal disputes focusing on whether they qualify as PSWP under the Patient Safety Rule, or instead constitute potentially discoverable state-mandated reports. (See the box below for a listing of some of the relevant case law.)

RELEVANT CASE LAW: DUAL-PURPOSE DOCUMENTS AND PSO CONFIDENTIALITY PROTECTIONS

Healthcare organizations and risk managers should periodically consult legal counsel to remain apprised of changes in the treatment and status of risk management and quality documents, as well as the types of challenges plaintiff attorneys are raising to asserted confidentiality privileges. While a comprehensive review of applicable case law is beyond the scope of this article, the following cases, among others, are germane:

- *Carron v. Newport Hospital*, R.I., No. 15-C.A. No. NC 2013-0479.
- *Illinois Department of Financial and Professional Regulation (IDFPR) v. Walgreen Company*, 2012 IL App (2d) 110452, No. 2-11-0452 (May 29, 2012).
- *Charles v. Southern Baptist Hospital*, Case No. 1D15-0109 (Oct. 28, 2015).
- *Johnson v. Cook County*, No. 15 C 741, 2015 WL 5144365 at *1 (N.D. Ill. Aug. 31, 2015).
- *Tibbs v. Bunnell*, 448 S.W.3d 796, 801 (2014).

Attorney-client work product privilege. Risk management reviews triggered by a patient's intent to sue are typically protected by the attorney-client work product privilege, which protects materials created by risk managers on behalf of a lawyer in anticipation of litigation. But the privilege is not absolute. For example, state law may exempt error reports generated in the ordinary course of business from this protection. In addition, the attorney-client work product privilege may not apply if a plaintiff demonstrates a need for certain information and is unable to obtain it elsewhere without undue hardship. In that event, the facts of the incident can be discovered, but the thoughts, opinions and litigation theories of the attorney generally remain protected.

Incident reports. Many states do not view incident reports as PSWP because they are not generated solely for patient safety and quality care purposes, but rather are created in the ordinary course of business or in response to state regulatory requirements. In addition, courts have found that Congress did not intend for state-mandated incident documentation – such as reports or occurrence screens – to acquire a federal confidentiality privilege merely because they have been entered in a PSE system by a healthcare provider or relabeled as quality control or patient safety reports. The test is whether a document originated in a QAPI committee or was prepared solely for the purpose of being submitted to a PSO.

Similarly, many states do not extend the peer review privilege to incident reports because they are not documents generated exclusively through the actions of a peer review committee. In granting peer review confidentiality privilege, courts typically focus on determining whether a document reflects a proceeding, report, minutes or other communication that is "of or originating in" a peer review committee.

Federal guidance. As the case law on treatment of dual-purpose documents is unsettled, the HHS has issued guidance for PSOs and providers designed to clarify the type of information that qualifies as PSWP. The guidance explains that the "intent of the system established by the Patient Safety Quality Improvement Act is to protect the *additional information created through voluntary patient safety activities*, not to protect records created through providers' mandatory information collection activities" (81 Fed. Reg. 32655, 32655, emphasis added). Thus, dual-purpose records do not count as PSWP and are not protected from discovery under the PSQIA.

Important Reminders

1. **Conflict over the PSQIA privilege and confidentiality protections is likely to continue on a state-by-state basis,** in the absence of binding federal authority or precedent. Given that HHS has narrowly defined the PSWP privilege, organizations and providers should be wary of relying on federal confidentiality protection for any data assembled or developed for purposes other than, or in addition to, reporting to a PSE system.
2. **Peer review and QAPI activities should focus on physician education and patient safety, independent of legal consequences.** Risk managers should not risk compromising quality and safety efforts by asking medical staff peer review or quality control committees to conduct risk management reviews aimed primarily at reducing potential data discoverability.
3. **Clearly label risk management-related documents and reports as such, in order to assert protection under the attorney-client work product privilege.** Incident report forms should be used only to report what happened and when. If a patient sustains a serious injury and litigation is anticipated, do *not* utilize a standard incident report form for further inquiry and analysis. If additional investigation is necessary, it should take the form of a separate report, stored and secured like other quality control-related documentation and shared only with legal counsel. Do not staple incident reports to investigative documents or folders, a practice that may affect confidentiality.

Peer review, quality assurance and risk management programs all depend upon access to data that may have liability implications. These critical activities can function efficiently only if concerns about legal discovery by plaintiff attorneys and other third parties are appropriately addressed. The relevant confidentiality privileges are varied and complex, with many connected to the operations of internal PSE systems and multi-provider PSOs. To minimize the likelihood of potentially damaging disclosures, healthcare leaders should become conversant with basic confidentiality concepts and consult routinely with legal counsel about evolving state statutes, federal regulations and guidelines, and judicial rulings.

Recommendations: Optimizing Protection of Patient Safety Data

RECOMMENDATION	PRESENT YES/NO	COMMENTS
PEER REVIEW		
1. **Issue a written quality plan prefaced by the statement that the purpose of quality improvement and peer review activities is to enhance care and patient outcomes.** The governing board-approved plan also should emphasize the confidentiality of quality improvement/peer review findings.		
2. **Draft detailed policies and procedures that define the scope of peer review activities** and describe their intended purpose as furthering patient safety and quality improvement goals.		
3. **Designate in writing who is involved in the peer review process,** and share privileged information only with these specified individuals.		
4. **Require that peer review committee members sign a** confidentiality agreement prohibiting improper disclosure.		
5. **Map out how data flow through the peer review process,** including how information is communicated to and used by the committee, and how documents are stored and secured.		
6. **Stamp the word *Privileged* on protected peer-review documents,** along with any state-mandated legal language.		
7. **Ensure that discussions and data sharing stay within the peer review framework,** thus maximizing protection of documents and preserving participants' statutory immunity.		
8. **Provide new committee members with an overview of peer review protections** and offer regular refresher training.		
9. **Describe in writing how medical staff corrective action plans and impaired practitioner protocols coordinate with the peer review process,** in order to maintain consistency of documentation and help preserve legal protections.		
10. **Working with legal counsel, develop a formal fair hearing and due process mechanism.** Ensure that the process complies with organizational bylaws and satisfies requirements contained within the Health Care Quality Improvement Act of 1986 relating to peer review.		
11. **Adopt a medical staff bylaw prohibiting staff from disclosing any information obtained through the peer review committee,** unless compelled to do so by law.		
12. **Document compliance with the reporting requirements of the National Practitioner Data Bank and state medical board,** as plaintiffs may challenge protections if relevant facts regarding errors and disciplinary measures are not fully disclosed to these bodies.		
13. **Consult legal counsel immediately if members of the peer review committee deviate from medical staff bylaws or operating policies,** as such actions may compromise the discoverability of reviews and investigative findings.		

RECOMMENDATION	PRESENT YES/NO	COMMENTS
QUALITY ASSURANCE AND PERFORMANCE IMPROVEMENT		
1. Record the following relevant dates:		
▪ When the organization contracts with a patient safety organization (PSO).		
▪ When the PSO is certified and recertified.		
▪ When the organization and PSO create a patient safety evaluation (PSE) system.		
2. **Maintain supporting documentation** of these actions and dates.		
3. **Create an organizational chart for the PSE system** and describe its policies and procedures in writing. (See "Documenting Your Organization's Patient Safety Evaluation System [PSES]," from UHC Safety Intelligence®.)		
4. **Carefully review quality assurance and performance improvement (QAPI) policies and procedures** to ensure that information collected by the organizational PSE system is identified and labeled as such, and that patient safety work product (PSWP) is clearly defined and protected.		
5. **Educate providers about the nature and limits of PSWP,** including what information is eligible for protection and when these protections do and do not apply. (See Patient Safety Rule 3.20.)		
6. **Clearly identify PSWP within the PSE system,** in order to prevent unauthorized disclosure.		
7. **Delineate in writing how and when PSWP is collected,** as well as how it is reported to the PSO.		
8. **Identify potential PSWP that is used for dual purposes** and thus may be subject to mandatory state reporting, such as incident, medication error and adverse occurrence reports.		
9. **Determine if other legal protections apply to dual-purpose PSWP,** such as attorney-client privilege, anticipation of litigation or regulatory requirements.		
10. **Develop a protocol for retention of PSWP** that addresses, but is not limited to, the following issues:		
▪ Length of information storage.		
▪ Methods of securing stored data.		
▪ Means of separating information to be reported to the PSO from material to be removed from the PSE system under the "drop out provision."		
▪ Criteria for removing PSWP from the system and associated documentation practices.		
11. **Maintain a digital or written record of all PSWP submitted to the PSO,** including dates of submission.		
12. **Establish a formal process for evaluating and managing requests for PSWP** from outside organizations and individuals.		
13. **Annually review the written policies and procedures related to PSO activities and the PSE system,** and be prepared to produce up-to-date protocols in the event of litigation.		

RECOMMENDATION	PRESENT YES/NO	COMMENTS
RISK MANAGEMENT		
1. **In written policy, define what constitutes a reportable incident** and communicate this definition to providers.		
2. **Formalize the incident reporting process,** specifying ...		
- Proper technique and time frame for reporting incidents.		
- Individuals authorized to report incidents.		
- Committees and individuals authorized to receive and review incident reports.		
- Guidelines for reporting incidents to the governing board, legal counsel and insurers.		
3. **Draft formal investigative protocols** that reflect regulatory requirements and offer guidance regarding the following issues:		
- Obtaining witness statements.		
- Managing post-incident personnel issues, including referral to other committees for additional follow-up.		
- Reporting to licensing bodies and other external entities.		
4. **Utilize separate forms** for incident reporting and post-incident investigative efforts.		
5. **Develop written protocols for performance improvement activities,** such as witness interviews and root cause analyses.		
6. **Instruct committee members about the difference between risk management and QAPI data,** ensuring that they understand the purpose of both, as well as the degree of protection granted to work product in each category.		
7. **Using standard training modules,** teach staff how to minimize discoverability when preparing incident reports, witness statements, event timelines and other risk management documents.		
8. **Explain to staff and providers what should and should not be included in the clinical record,** e.g., not to indicate a completed incident report, which could lead to discovery requests in the event of a legal action.		
9. **Clearly mark investigative and risk-related documents as protected,** e.g., "Privileged and confidential: attorney-client work product as defined and protected by [*insert statute name and number*]." Consult legal counsel for appropriate language.		
10. **Minimize to the extent possible "mixed-use" situations,** in which fact-finding investigative reports are shared with peer or quality review committees.		
11. **Establish a risk management review committee separate from the medical staff peer review process.** For each committee, select physicians who are familiar with relevant confidentiality laws to conduct clinical care reviews.		

QUICK LINKS

- Callahan, M. "How to Structure Health Care Systems, Clinically Integrated Networks and Other Affiliated Providers in Order to Benefit from Patient Safety Act Protections." Katten Muchin Rosenman LLP, presented in association with UHC Safety Intelligence, November 19, 2015.
- Frequently Asked Questions About Patient Safety Organization Services, from the QA to QI Patient Safety Organization, October 19, 2016.
- Lin, S. and Dru, K. "Patient Safety Work Product Privilege: Does It Still Exist?" *HLB Health Law & Policy Blog*, posted August 5, 2016.
- Patient Safety and Quality Improvement Act of 2005-HHS Guidance Regarding Patient Safety Work Product and Providers' External Obligations, a rule by the Agency for Healthcare Research and Quality (AHRQ), May 24, 2016.
- Patient Safety Organization (PSO) Program, from the AHRQ. (See Frequently Asked Questions, Compliance Self-Assessment Guide and Resources.)

CNA Risk Control Services

ONGOING SUPPORT FOR YOUR RISK MANAGEMENT PROGRAM

CNA provides a broad array of resources to help hospitals and healthcare organizations remain current on the latest risk management insights and trends. Bulletins, worksheets and archived webinars, as well as past issues of this newsletter, are available at **www.cna.com/riskcontrol**.

Your SORCE® for Education

CNA's School of Risk Control Excellence (SORCE®) offers complimentary educational programs that feature industry-leading loss prevention, loss reduction and risk transfer techniques. Classes are led by experienced CNA Risk Control consultants.

SORCE® *On Demand* offers instant access to our library of risk control courses whenever the need arises. These online courses utilize proven adult-learning principles, providing an interactive learning experience that addresses current regulatory requirements and liability exposures.

Allied Vendor Program

CNA has identified companies offering services that may strengthen a hospital's or healthcare organization's risk management program and help it effectively manage the unexpected. Our allied vendors assist our policyholders in developing critical programs and procedures that will help create a safer, more secure environment.

When it comes to understanding the risks faced by hospitals and healthcare organizations… **we can show you more.®**

CNA

For more information, please call us at 866-262-0540 or visit www.cna.com/healthcare.