In the never-ending quest to improve healthcare quality and safety and decrease costs, public and private payers and accreditation bodies have raised the bar for healthcare organizations and practitioners by expecting them to comply with specific practice standards and patient outcomes in order to receive enhanced reimbursement and continued accreditation.

Pay-for-performance (P4P) programs and The Joint Commission’s standards for focused and ongoing performance monitoring of practitioners are examples of initiatives generating large amounts of sensitive data that, in the wrong hands or if subject to discovery in a malpractice or similar action, could provide a plaintiff’s attorney with significant documentation and evidence to prove a negligent credentialing claim.

**10 steps to protect sensitive practitioner data**

Changes to healthcare landscape create potential pitfalls for hospitals and medical staff offices

- Patterns of blood and pharmaceutical use
- Length of stay (LOS) patterns
- Morbidity and mortality data
- Use of consultants
- Requests for tests and procedures
- Clinical outcomes

The Joint Commission requires hospitals to adopt and apply one or more criteria and then monitor and measure the results. The accreditor’s expectation is that hospitals will implement remedial measures as soon as they identify any substandard patterns rather than wait to review and remedy practitioner outcomes every two years at reappointment.

**Enhanced efforts to track practitioner data**

P4P programs and OPPE/FPPE standards are only select examples of enhanced efforts, spurred in part by public demand for more transparent results, to identify outcomes and results so that payers and consumers can make better-informed decisions about providers. To monitor compliance efforts and to educate practitioners about how their practices measure up to identified standards, hospitals have designed computerized and other tracking methods that generate individualized and aggregate physician profiling data. For example, some programs look at major diagnoses (e.g., heart failure, cardiac arrhythmia, angina, and percutaneous cardiovascular without acute myocardial infarction) and then evaluate a practitioner’s performance by examining factors such as average LOS, average cost, mortality, complicating factors, outcomes, readmission, number of consultants utilized, and drugs used.

Individual results are compared with those of peers to determine whether the practitioner is performing on par with the peer group or is an outlier in one or more categories. The goal of this profiling exercise, especially as applied to outlier results, is to improve outcomes and modify practices where warranted.
Balancing sensitive data protection with duty to protect patients

Lost in the above-described efforts to improve health-care quality and safety and decrease costs is the fact that hospitals and practitioners are generating increasing amounts of sensitive information about practitioners that a plaintiff could use against the hospital and/or its medical staff practitioners in a negligent credentialing claim.

How? It is a fairly established law that hospitals have a duty to patients to ensure that practitioners are currently competent to exercise the clinical privileges the hospital grants to them. If a hospital grants privileges to an unqualified practitioner—or if the hospital knew (or should have known) that the practitioner was not qualified based on internal or external studies, reports, or peer review analyses but took no action to limit or remove the privileges in question—the hospital may be found independently negligent if the practitioner is found negligent.

In order for a plaintiff to establish a breach of this duty, he or she will request that the hospital provide copies of any and all information obtainable, including but not limited to:

- Bylaws
- OPPE and FPPE procedures
- Physician profiling results
- Use of P4P standards and outcomes
- Peer review studies

For example, if the plaintiff can use this information to establish that the hospital negligently granted privileges to an outlier physician who consistently had high mortality results over the years as evidenced in his or her physician profiling reports, the hospital could be at risk.

What materials are discoverable? Which are not protected by courts?

It is common knowledge that bylaws and policies and procedures documents are discoverable. On the other hand, most states have adopted statutes that protect certain privileged and confidential reports, studies, minutes, and other documentation that fall under the statutory definition of peer review materials. Each state has a different statute and therefore a different standard, in addition to interpretive case law, that sets forth what is and is not discoverable. The problem is that most hospitals must rush to generate profiling and other data to fulfill P4P and accreditation requirements and have not taken into account whether their peer review statutes protect these reports or certain aspects of them.

Moreover, hospitals often create these profiles through the use of software created by third-party vendors that do not distinguish between data that might be privileged and those that are not. Although courts generally recognize the need to protect pure peer review information because of the accepted public policy need to encourage open and frank internal discussions about physician quality and performance, they tend to interpret the statutes strictly. For example, business, financial, risk management, and similar reports prepared for non-peer review purposes are not usually protected if simply run through a peer review committee. On the other hand, reports that are specifically designed for or requested by a designated committee for a statutory peer review purpose stand a much greater chance of being treated as a protected and nondisclosable document in the courts.

10 steps to legally protect sensitive information

So, what is a physician profiling report? It usually contains cumulative and individual results as well as sensitive and generic information. Would a plaintiff love to get his or her hands on this information? Absolutely. Will it be protected? That depends on what steps a hospital has taken to maximize protection under its peer review statutes. The following are some important and practical steps a hospital and medical staff should consider to protect against the discovery of sensitive information that could be used against both parties in a malpractice suit or other action (hospitals can and should use these steps in all instances in which they gather practitioner data—not just in regard to P4P or OPPE/FPPE):

1. List all relevant reports, studies, forms, analyses, profiling data, etc., that a hospital uses in carrying out

> continued on p. 4
10 steps < continued from p. 3

its P4P, quality assurance, peer review, risk management, credentialing, and similar functions.

2. Identify those reports and information or portions thereof that, if accessible to a patient or plaintiff's attorney, could be used to support a malpractice or corporate negligent claim.

3. Identify all applicable state and federal confidentiality statutes, such as peer review, physician-patient, medical record, HIPAA, attorney-client, business record, and others that arguably apply to this data set.

4. Determine the scope of protections afforded under the statutes and applicable case law, and/or the steps needed to at least assert a confidentiality argument, to the list referenced in step 1 in order to make an objective assessment about what data are likely to be protected and what may or will be discoverable.

5. Identify documents, or portions of documents, that remain after completing steps 1–4, and determine the level of sensitivity of the remaining information.

6. If sensitive information remains, consider whether it can be moved to, consolidated with, or reauthorized by a peer review committee (or determine what other steps can be taken) to maximize protection under the applicable statutes.

7. Determine whether the remaining sensitive information can be deidentified or aggregated without minimizing its effectiveness.

8. Adopt bylaws, policies, and procedures that use statutory buzzwords (e.g., “This report is privileged and confidential under the ________ Act because it has been authorized for development and use by the ____ Committee for the purpose of reducing morbidity and mortality and to improve patient care”). This action may be self-serving, but courts have held that not making this internal designation suggests that the hospital did not consider the document confidential.

9. Consult with legal counsel in developing a plan—or at minimum meet with counsel regarding the final review of the plan.

10. Update the plan as forms and the law change.

By following these steps, a hospital and medical staff can better appreciate the manner in which it develops internally P4P and quality assurance information (e.g., information gathered through OPPE/FPPE) and whether there are additional ways to retain the confidentiality of the data to the extent possible. Following the preceding 10 steps likely will result in changes to the way your hospital generates and memorializes sensitive data, as well as modify the way it shares this information. Remember that not all information is protected under the statutes. However, too many hospitals are unnecessarily making a plaintiff's job easier by failing to understand where the confidentiality lines are being drawn.

Editor's note: Michael R. Callahan, an attorney and senior partner in the Healthcare Practice Group at Katten Muchin Rosenman, LLP, in Chicago, IL, can be reached by phone at 312/902-5634 or via e-mail at michael.callahan@kattenlaw.com.