Katten

Keeping information peer-review protected in the digital age

Used with permission from Medical Staff Briefing

"User would like to recall their last email."

Although this option exists in most email programs, let's face it—once something is sent electronically, you cannot physically take it back. You are at the mercy of the recipient, hoping they will respect your wishes and delete the email without looking at it.

Let's say the recipient is a plaintiff's attorney who has requested you send over any relevant information related to a malpractice case against a physician on your medical staff. Because the file is electronic, you send it without first looking through its contents. You realize you have accidentally sent over peer-review protected information that you are not required to send to the plaintiff attorney. You ask the attorney to not look at the information you sent in error. But if that information is what the attorney needs to win their case, they most likely are going to look at it.

"The success of a negligent credentialing or malpractice claim often depends on the availability of documents that the plaintiff's attorneys can use to their advantage," says Todd Sagin in his book *Negligent Credentialing: Strategies for Reducing Hospital Risk* (HCPro, 2016). "Keeping documents out of the hands of opposing counsel can prevent these individuals from finding fault with the language or alleging noncompliance with the contents."

This is just one issue MSPs need to keep in mind as more of their work becomes electronic.

Determining what is 'peer-review' protected

There are many positive reasons to convert to a paperless medical staff services department. It can allow for practitioners to be credentialed faster, for privileging forms to be more standardized, for MSPs to work more efficiently, to break down silos between departments, and for practitioners to fill out less paperwork. However, every new innovation comes with challenges, and MSPs should know what these challenges are and how to overcome them.

Going back to the previously mentioned point, with an electronic file, MSPs need to avoid the temptation to automatically attach and send information without first reviewing what they are sending.

"A lot of diligence has to be paid over these files," says **Michael Callahan**, senior counsel at Katten Muchin Rosenman, LLP, in Chicago. "Review files to make sure you didn't inadvertently include peer-review protected information."

Although MSPs do not directly receive a subpoena for practitioner files, legal counsel usually relies on the MSP to pull together the information. Callahan advises setting up a system of checks and balances before handing anything over.

Some medical staff services departments stamp credentials files and their contents with an indication that they are peer review material and protected from discovery to the extent allowed under the law. This leaves no question about whether the institution considers particular material to fall under the legal protection of peer review.

"Peer-review protected" or "privileged information" is a way of saying that the information in question is deemed nondiscoverable in legal proceedings. The degree to which credentials files can be protected from discovery in legal proceedings varies by state. However, at a base level, almost every state has laws that protect peer review information, including credentialing information.

"These laws are premised on the concept that patients are best served when physicians can have candid conversations about quality and performance that will not be subject to public scrutiny," writes Sagin.

Examples of credentialing information that is often peer-review protected includes:

- Credentialing, quality, and other identified peer review meeting minutes that reflect deliberations on individual applicants for appointment and reappointment
- Minutes, reports, and analyses related to disruptive/impaired practitioners
- References and specific recommendations from a professional peer or body of peers, such as a peer review committee
- Internal and external peer review reports and analyses requested by a medical staff peer review committee

Examples of information that is often *not* peer-review protected includes:

- Delineation of privileges templates
- Application forms
- Policies and procedures related to credentialing
- Medical staff bylaws

According to Callahan, every medical staff has to define what it considers privileged information. Understanding specific state statutes regarding privileged information is key. For example, in Illinois, hospitals are included in peer review statutes, but physician groups are not.

Medical staffs must also understand the difference between what is privileged information under state law and what is privileged under the federal Patient Safety Act (which allows for the creation of Patient Safety Organizations [PSO]). Privilege protections granted by the Patient Safety Act are far broader than most state statutes both in terms of what healthcare facilities and entities can claim for protections as well as the scope of protected patient safety and peer review activities.

"You almost have to have three different files," says Callahan. "One with privileged information under state law, one with privileged information under the Patient Safety Act, and one with privileged information under both.

"Therefore, MSPs should find out if the hospital and health system are in a PSO," continues Callahan. "If so, they need to review its patient safety evaluation system policy, which will describe what information is privileged."

MSPs should review files on a regular basis to see if any information needs to be moved into or out of a file. "A good time to do this—at the least—is at reappointment," says Callahan.

Losing peer-review protection

Make sure to handle files confidentially to ensure that the privilege of nondiscoverability is not unintentionally waived. Consider, for example, a report from an external peer review. A judge could say that the report is not privileged from discovery if a credentials committee discusses the findings at a meeting, and someone in attendance later shares details from the report with a practitioner who is not on the committee.

Callahan gives the example of an unexpected death at a hospital, which will most likely trigger peer review and a root cause analysis (RCA). "Let's say the RCA is conducted right away before the peer review committee says, 'Let's conduct an RCA.' In Illinois, for example, the RCA would not be peer-review protected under its state statute but could be protected under the Patient Safety Act if participating in a PSO."

Callahan points out that MSPs also need to know how case law interpretation of state and federal privilege statutes can affect what is and is not protected. Therefore, MSPs should consult in-house and/or outside counsel because it will affect what information can and should be included in a non-privileged credentials file versus a privileged file.

How your files are stored can also be an issue. Keep in mind that a court may regard information kept outside of the formal medical staff quality, peer review, or credentials file as discoverable. It is harder to claim peer review privilege for documents that are kept in disparate locations. Electronic files will likely be easier to label appropriately. Medical staff leaders should be instructed to forward all peer review findings, documentation, and correspondence to the medical staff office for placement in an individual's peer review file or for attachment to the minutes of the peer review committee. To see a sample policy on confidentiality of files housed in the medical staff services department, click here.

Just as it is easy to send too much information to the wrong people, it is also easy to send too little information to the right people. MSPs must ensure they are giving complete files to department chairs, the credentials committee, the medical executive committee (MEC), etc.

"Let's say an important adverse patient issue did not get to the MEC, and they are making a reappointment decision on a physician. And then the physician makes a subsequent patient injury, and a negligent credentialing suit is brought. The plaintiff wants access to all files."

If the plaintiff attorney is able to see that the MEC reviewed an incomplete file and made a credentialing decision based off of incomplete information, this can help them prove negligent credentialing or malpractice by the organization.

Callahan says some questions MSPs should keep in mind as they embrace electronic files include:

- Is privileged information kept in two places?
- Is the information kept in a paper file and an electronic file? Is it complete in both places?
- Do you keep a paper file as a backup of an electronic file?
- Are the files complete and up to date?
- If transferring paper files to an electronic file, is all of the information being transferred?

Who can view files

All files should be password protected, and the hospital should keep track of who has access to the files.

Physicians may ask to see their own peer review/credentials files. "In order to create a constructive, collegial atmosphere around peer review activities, it is valuable to provide this opportunity," writes Sagin.

However, there may be pieces of information in the physician's file that they should not have access to. For example, some complaints or references may be submitted to the hospital on the premise that they will not be shared with the physician in question. Medical staffs should decide what can be viewed by a practitioner who wishes to access their own credentials file. Consider adopting a policy that specifies the conditions under which the file will be made available. This includes where the viewing can take place. For example, many hospitals only allow the file to be viewed in the medical staff services department and with a medical staff leader or office personnel present to ensure that no alterations are made to the records.

An advantage to allowing practitioners to review their files is that they may pick up on errors in the credentials file that can be corrected. If not caught, such errors might be problematic should the file become discoverable in a negligent credentialing claim.