Telemedicine: Avoiding a Risk Management Nightmare

PARKER | SMITH | FEEK

November 2011

By Sharon Hall, VIce President

A recent msnbc.com article, "Is a Doctor Reading your X-Rays? Maybe Not," is certain to have caught the attention of many consumers, raising awareness of the practice of telemedicine and some issues that may influence a correct interpretation and diagnosis. The article provides several in-depth examples of delayed and missed diagnoses that occurred when radiology interpretation was outsourced. The errors are attributed to several factors: inadequate contextual information necessary for teleradiologists to interpret scans; a lack of teamwork between the originating facility and distant site personnel; and disregard for red flags signifying that qualified radiologists had not interpreted the films. How will you respond to patients who question the safety of your facility's use of telemedicine?

While telemedicine can improve care by allowing quick access to specialists, it can also create scenarios for less than optimal care. And so, it is essential for those using telemedicine to employ specific risk strategies to mitigate the increased risks. These include ensuring the adequacy of credentials and care provided by contracted specialists, team communication, and ongoing quality assessment.

A good first step in risk management strategy is familiarity with the new telemedicine rules for hospitals and critical access hospitals issued by the Centers for Medicare and Medicaid Services (CMS) in July 2011. Their revisions to the Conditions of Participation (CoP), while easing some of the burden typically associated with credentialing telemedicine physicians, also require that specific standards be met. Facilities offering telemedicine services may now rely upon the credentialing and privileging decisions of a distant site hospital that participates in Medicare or of a distant site telemedicine entity that enables a hospital using its contracted services to meet all applicable CoP.

The new rules require a written agreement between the hospital seeking telemedicine services and the distant site hospital or entity. Core provisions of the written agreement include:

1. The distant site hospital or entity providing the telemedicine services must be a Medicare participating hospital or meet all applicable CoP including Medicare credentialing standards.
2. The individual distant site practitioner providing the telemedicine services is privileged at the distant site hospital or entity which provides a current list of the distant site physician's privileges at the distant site hospital or entity.
3. The telemedicine physician holds a license issued or recognized by the state in which the hospital whose patients are receiving the telemedicine services is located.
4. The hospital reviews telemedicine services provided to its patients by telemedicine physicians covered under the agreement and provides written feedback to the distant site hospital or entity; addressing at a minimum adverse events and patient complaints resulting from telemedicine services.

While compliance with CMS revisions is a good beginning, it will not take care of all your risk management concerns. Experts have indentified some risk exposures that you should consider as part of an effective risk strategy before updating your telemedicine processes. Some of these include:

1. Reliance on the written agreement may not release the originating hospital from a negligent credentialing allegation if the telemedicine facility is noncompliant with Medicare credentialing standards.
2. Informed consent may not be comprehensive, allowing patient choice to accept or decline telemedicine care.
3. Non-physicians participating in telemedicine services may exceed the scope of their certification or licensure, resulting in unmet standards of care.

4. Peer review protections may not extend to information shared between the originating hospital and remote telemedicine site. The structure of your existing program may need to be revised in order to maintain quality improvement protections for shared data.
5. Does your existing insurance adequately cover exposures inherent to telemedicine, such as errors & omissions of a telemedicine practice, negligent credentialing, privacy breaches, and disruption of telemedicine services due to equipment failure or other reasons?

Despite the additional risks associated with telemedicine, it is possible to develop an effective risk management strategy for those exposures. In their May 2010 RMS newsletter, the Rozovsky Group provides a detailed overview for strategies to mitigate telemedicine risk exposures:

1. Evaluate the credentialing standards of the facility providing the telemedicine practitioner in order to ensure that CMS's CoP are met.
2. Review hospital and/or medical staff bylaws and rules/regulations to ensure that new CMS standards are appropriately incorporated into these documents. In addition, incorporate any state specific licensure requirements.
3. Develop a process to maintain a current list of telemedicine providers and update it regularly.
4. Evaluate the performance of the telemedicine specialists in such areas as meeting credential and compliance standards, and quality of care as determined through peer review.
5. Develop protocols for the scope of practice for non-physician telemedicine providers, e.g. radiology technicians, physician assistants, ARNP's and registered nurses.
6. Review general admission and specialized consent documents for inclusion of patient authorization for services via telemedicine.
7. Educate physicians on essential informed consent elements and audit documentation for inclusion of telemedicine consent in the patient record. Explanations should include how the technology is used and any limitations.
8. Develop guidelines regarding the type of medical information to be shared with distant site practitioners who provide telemedicine interpretation and services, and monitor documentation as part of your performance improvement process.
9. Work with your information system personnel or vendors to evaluate and implement necessary measures to keep electronic health information secure and to ensure compliance with HIPAA privacy and security requirements.
10. Create or review existing telemedicine agreements for compliance with the new standards and modify as needed if you decide to rely on the credentialing of the distant site telemedicine facility. For specific contract subject matter recommendations, refer to the RMS Newsletter.
11. Review insurance provisions of your telemedicine agreement for mutual hold harmless and indemnification provisions, as well as adequate insurance coverage.

Proactive risk, quality, and compliance activities are key to avoiding "bad press" incidents that involve missed or delayed diagnosis using telemedicine services.