Telehealth and the Risk Management Practices You Need to Consider

VGM Insurance SERVICES

800.362.3363 | info@vgminsurance.com

The demand for reliable, accessible, and affordable health care services has never been greater, and the challenge of meeting it has forced the entire health care industry to reconsider its service model. Telehealth, defined as the remote delivery of health care services over the internet or other telecommunications infrastructure, has opened the door for providers to supply their patients with cheaper, more efficient and more personalized care, regardless of where they reside.

As the need for quality care continues to grow across the nation, telehealth promises to empower consumers with more information and control over their health care decisions than ever before, while presenting providers with an ever-expanding menu of options for where and how they can treat their patients. These new options bring new opportunities, but they also carry new risks. If you're currently offering telehealth services or are considering it as an option for the future, you'll want to be proactive in identifying and mitigating the potential risks to protect your patients and your business.

Documentation, Privacy and Compliance

As with all patient encounters, any provider-patient interaction using telehealth technology should be documented in the patient's health record. In addition, patient and provider access to this documentation should comply with existing regulations and institutional policies for privacy and security of health information.

Take care to address these items as you think about your documentation, privacy and compliance measures:

- The health record should include documentation of all patient-related electronic communications, including informed consent, as well as therapeutic modalities to be used, clinical evaluations and instructions related to telehealth technology
- Documentation should also include all clinicians involved in the telehealth visits
- Informed consent should include full disclosure of the following:
    - » The names and credentials of telehealth staff and providers
    - » Explanation of the patient's right to stop or refuse treatment by telehealth
    - » The technology that will be used
    - » Privacy and security risks as well as measures taken to reduce the risk
    - » Technology specific risks such as service interruption and poor transmission quality
    - » Instructions for alternative care in case of an emergency or technology malfunction
    - » Diagnosis/injury to be treated
    - » The scope of service defined for each type of telehealth service provided
    - » Potential risks involved in therapy
    - » Reasonable expectation of the results of therapy/care
    - » Differences between telehealth and traditional care
    - » Complete and full understanding by the patient of all information disclosed

Staff Training

It's imperative that all providers and staff who participate in telehealth services, or care for patients who may receive telehealth services, receive telehealth training either at hire or initiation of telehealth services, as well as periodically thereafter. Consider the following when implementing a telehealth training program:

- Education and training should include role-specific, direct and supportive patient care, including how to perform any adjunct tasks such as responsibility for documentation and informed consent
- Education on each type of telehealth modality that might be encountered, as well as how to troubleshoot problems with the technology and/or how to obtain technical assistance
- Develop role-specific telehealth competencies and use them to evaluate providers and staff periodically
- Include telehealth expectations in job descriptions and annual performance evaluations
- Ensure all staff and providers who participate in telehealth services have received telehealth specific healthcare privacy and security training

Legal/Regulatory

It's extremely important to understand the telehealth laws in your own state and in the state of every patient that you're treating. You'll want to rely on solid legal counsel as you make decisions regarding your telehealth practice, while also consulting with your business insurance provider to protect yourself from liability.

While educating yourself about the regulations surrounding telehealth, it's important to:

- Incorporate telehealth into the Notice of Privacy Practices
- Ensure that your telehealth services and processes comply with both federal and state laws and guidelines
- Ensure that all providers that are to participate in telehealth services are properly licensed and/or credentialed as required in all applicable states
- Ensure that rules related to privacy and confidentiality are upheld by both patients and providers when protected health information (PHI) is transmitted electronically

Technology and Data Security

Telehealth requires clear communication in real-time between you, your patients, and other medical professionals. Low-grade equipment can cause miscommunication or even misdiagnosis, resulting in poor patient outcomes and dangerous liability risks. It also tends to malfunction more frequently, which can be disruptive and expensive to deal with on a regular basis.

As PHI continues to be a valuable commodity on the digital black market, it's also vital to establish strict data security measures. Don't make the mistake of assuming your business is too small or obscure to attract the attention of hackers.

As you make your equipment and software selections, be sure to:

- Ensure that equipment used for telehealth purposes has high quality audio and visual capabilities, up to date operating systems, and the ability to be secured against malware

- Develop backup plans and downtime policies and procedures. Provisions for communication and documentation during service interruptions should be developed and tested
- Consider telehealth capabilities in all hazard disaster planning, particularly for surge (a markedly increased volume of patients) management
- Develop and implement technical standards to ensure the security, capacity and reliability of data transmission. These standards should specifically address interoperability of systems, verification of receipt of data and results and technical support
- Implement data control measures to ensure that patient information is stored and transmitted in a confidential manner through the creation of a Virtual Private Network (VPN), use of encryption technology and/or file anonymization software. Encryption measures also should extend to stored data on portable devices or removable media, as theft and loss of laptops, tablets, smartphones and USB flash drives are a leading source of data breaches
- Establish authentication measures to enable only authorized users to enter the system and access patient and company data. This can include two-factor authentication, biometric scans, voice pattern samples, etc.
- Protect your systems and devices by ensuring that firewalls and antivirus software are kept up to date and that scans are run regularly to detect malicious programs and activity

Patient Safety

Treating patients virtually can create additional patient safety risks, particularly when treatment modalities involve movement, such as physical therapy. It's important to be aware of these risks and take extra precautions to protect your patients.

As you plan each treatment session, consider these best practices:

- Ensure each movement involved in therapy is clearly demonstrated. The provider should ask the patient for their confirmation and understanding before the patient attempts the movement themselves
- All patients, but specifically those who are mobility challenged, should be instructed to incorporate safety measures such as sitting, holding onto a chair while standing or other recommendations to lessen the likelihood of a balance issue or fall that could result in an injury
- The provider should maintain supervision of the patient at all times while the patient performs any movements involved in therapy
- There should be an emergency plan in place for all providers should there be a fall or injury, including:
  - » Instructions to the patient
  - » Call 911
  - » Follow up procedure for post-acute medical care

Moving Forward with Telehealth

As telehealth continues to grow in scope and popularity, healthcare providers need to stay current on new technologies and procedures, while also managing the new risks that come along with these opportunities for enhanced patient experience and care.

For more information about how you can manage the risks associated with telehealth in your business and to ensure you have adequate coverage, reach out to your VGM Insurance Services Account Manager or contact us today at info@vgminsurance.com or 800-362-3363.