CHAN Healthcare™
A subsidiary of Crowe Horwath LLP

October 2014

Know Telemedicine's Risks and Considerations

Managing the Risks to Realize the Benefits

By Raj Chaudhary, CGEIT, CRISC, Debbie Gore, CISA, CISSP, Darren Johnson, CIA, and Nancy Van Dyke, CPA, CIA

Smartphones, tablets, laptops, and desktop computers allow people to connect instantly with other users and communicate via voice, video, text, or other Internet-based media. The advent of such devices and the relative ease of their use has led healthcare providers to begin interacting with patients through electronic communication. As this practice becomes more prevalent and effective, the associated risks must be managed more closely.

As defined by the American Telemedicine Association (ATA), telemedicine is the use of medical information exchanged from one site to another via electronic communication to improve a patient's clinical health status.[1] The Centers for Medicare & Medicaid Services (CMS) defines telemedicine as two-way, real-time interactive communication between a patient and a physician or practitioner at a distant site through telecommunications equipment that includes, at a minimum, audiovisual equipment.[2] The common theme of these definitions is that information is exchanged or a service is provided across an electronic medium that does not require participants to be in proximity. Telemedicine includes consulting with patients via video conferences, transmitting images for evaluation, and monitoring patients remotely.

Telemedicine's Drivers and Benefits

Employers, private insurers, patients, and the *Affordable Care Act* (ACA) all are contributing to the telemedicine trend.[3] The ACA requires doctors and hospitals to be more accountable by moving care providers away from the fee-for-service model, with payments based on the volume of services, to a reimbursement model based on the value of care provided. The aim of telemedicine services is to provide cost-effective, high-quality healthcare that keeps patients out of hospitals, where care is more expensive. At a time when healthcare costs are increasing, telemedicine is evolving into a more cost-effective means of providing services.

The emergence of telemedicine practices will improve access to healthcare not only for patients in remote or rural settings but also for patients who desire convenience rather than face-to-face contact with providers. An example of such services is Louisville, Ky.-based KentuckyOne Health, which began its Anywhere Care service in November 2013.[4] Anywhere Care provides statewide access to doctors and nurses via a webcam or telephone 24 hours a day, seven days a week, for a flat $35 fee. The service treats patients with uncomplicated medical conditions. KentuckyOne acknowledges that

the service is not for continual care or patient monitoring. If the patient's scope of care is greater than what can be determined through the telemedicine link, the patient is referred to a local emergency room, doctor, or urgent care center. Thanks to new providers such as KentuckyOne, the trend toward telemedicine services is expected to increase as more hospitals and physicians look for ways to improve patient access and reduce costs to offset decreases in reimbursement.[5]

Types of Telemedicine

New types of technology continue to change the kinds of telemedicine services that can be offered. Currently, telemedicine is classified into three main types: store and forward, remote monitoring, and interactive services. Following is a high-level description of each type:

Store and forward is defined by Medicaid.gov as the transfer of data from one site to another using a camera or similar device that records (stores) an image to send via telecommunication to another site for consultation. This technology typically is used for nonemergent cases. Examples include radiology, cardiology, or dermatology images taken at one site and then forwarded to a specialist for review and interpretation. Store and forward also can include video – such as exam clips – or other data. This technology provides access to specialists the hospital or medical office might not have available on-site and can reduce overhead costs associated with hiring specialists.

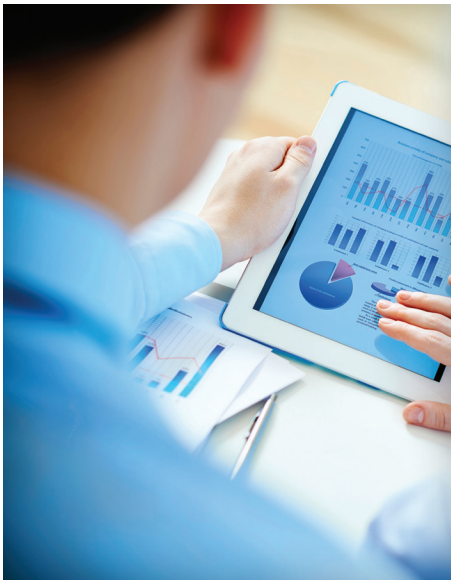
Remote monitoring, aka self-monitoring/testing, enables the physician to remotely monitor the patient's status and typically is used for conditions such as heart disease, diabetes, and asthma. The physician can view data collected without the patient needing to go into the office to have medical staff collect and communicate the data to the physician. This technology is more convenient for the patient and tends to be less costly than in-person clinical visits.

Interactive services are real-time interactions between a patient and a provider. The interaction can include phone conversations, online communication, or home visits. Examples include medical history reviews, physical exams, psychiatric evaluations, and ophthalmology assessments. Like remote monitoring, interactive services are more convenient for the patient and tend to be less costly than in-person clinical visits.

Telemedicine Risk Management

Although telemedicine brings benefits of accessibility to medical services for patients who otherwise would not have access, the method of service delivery also presents unique risks. Identifying these and establishing processes for mitigating them are critical to successful development of a telemedicine program.[6] Significant risk areas include the following:

- **Regulatory.** The originating site (where the patient is located, such as at a residence or medical facility) and the distant site (where the provider performing remote services is located) might not understand federal or state telemedicine regulations or stay current on regulatory changes.



- **Confidentiality.** The exchange of information could occur between unintended parties or other than as designed.
- **Reliability or integrity of technology.** The technology used to facilitate the service of telemedicine could fail while working with the patient.
- **Fraud and abuse.** Data could be used inappropriately or by an unintended party.
- **Legal agreements.** Agreements between the originating site and the distant site might not outline ways to confirm that services meet regulatory and payer requirements.
- **Credentialing.** Medical personnel and sites might not meet regulatory and legal-credentialing specifications for the site locations involved.
- **Liability.** Insurance at the originating site and the distant site might not be set up appropriately to cover all parties, services, and geographic areas.
- **Billing and reimbursement.** Payer requirements might not be well understood.
- **Clinical documentation.** Patient encounters might not be documented completely and accurately in the patient's medical records.
- **Informed consent.** Patients participating in telemedicine encounters might not be aware of and agree to all associated distant medical provider services and limitations.

The sections that follow discuss each of these risk areas and provide strategies for managing the risks.

Regulatory

Significant risks related to regulations include:

- Noncompliance with the following regulations:
  - 42§ 482.12 Medicare conditions of participation (CoP) requirements specifically related to credentialing telemedicine providers
  - The *Health Insurance Portability and Accountability Act* (HIPAA) and the *Health Information Technology for Economic and Clinical Health Act* (HITECH)
  - State licensing laws and medical board requirements
  - State credentialing laws
  - State online prescribing requirements
  - State informed-consent form requirements
  - Face-to-face requirements for establishing the relationship between the patient and the provider
- Policies and procedures might not be updated in a timely manner when telemedicine regulations change.

Risk Management Recommendations

There are varying opinions on state licensing requirements. Therefore, it is critical to obtain the advice of legal counsel in interpreting telemedicine regulations. For example, in June 2014 the American Medical Association adopted a quality of care and patient safety policy recommending that physicians delivering telemedicine services be licensed in the state where the patient receives treatment. The ATA does not

agree that the physicians need to be licensed in the state where the patient receives treatment. Regulations are changing rapidly as technology advances and pressure increases to provide more services at lower costs. Currently, many requirements related to credentialing, licensing, online prescribing, medical boards, informed consent, and face-to-face meetings vary by state and at times conflict with federal regulations. In addition, precedents related to liability insurance claims have not been set yet. Healthcare providers should work closely with legal counsel to address regulatory risks as they continue to emerge.

Confidentiality

Significant risks related to confidentiality include:

- Access to patient data might not be secured adequately, allowing unauthorized individuals to access information.
- Processes to authenticate users might not be effective, resulting in treatment of an imposter or an imposter performing services on behalf of another provider.
- Noncompliance with federal or state regulations, privacy legislation, or HIPAA might occur.
- Clinicians or other relevant staff might use technology to access and use patient data inappropriately.

Risk Management Recommendations

Existing internal policies and procedures to protect the confidentiality, privacy, and security of patient data at hospitals – to comply with HIPAA and/or HITECH – can provide a strong foundation for the privacy of telemedicine practices. One difference is that the originating site must understand and agree with practices followed by the distant site and any third-party vendors and software. It is important to work with legal counsel and the facility's HIPAA privacy and security officers to review any agreements and processes for telemedicine vendors and third-party providers.

Reliability or Integrity of Technology

Significant risks related to reliability include:

- Equipment might not be maintained, resulting in equipment failures while working with a patient.
- Technology failure might occur during critical moments of data exchange.
- Information corruption or transmission of incorrect information during the exchange might occur.
- Data might be transmitted to an individual or location other than the intended party.
- Data might be transmitted through insecure methods, allowing outside parties to access and use the data inappropriately.
- Site/system support might not be available to keep the site/system available during hours of operation.
- Third-party vendors, software, and services might not execute matters in compliance with the contract.

Many existing fraud and abuse processes cover risks associated with telemedicine.

Risk Management Recommendations

Management of technological risks heavily depends on the vendor or internal employees who administer and oversee these operations. With rapid technological changes available for telemedicine, having policies and processes outlining the permitted technology and providing an approval process for new technology can reduce some of this risk. Another significant consideration is the implementation of adequate controls to limit access to systems and information to authorized individuals. Strong controls reduce the risk of imposters intercepting the transmission and using the data. Again, if a third party is responsible for administration of the communication and electronic connectivity process, then legal counsel, security officers, and other informed members of management should review all contracts to verify that all aspects of the agreement and services are defined clearly.

Fraud and Abuse

Significant risks related to fraud and abuse include:

- An individual other than the approved, designated person might obtain access to patient information.
- An individual could use another patient's identity or photo to obtain free services.
- Patients might engage multiple physicians to obtain illegal quantities of medication.
- Services never provided might be billed.
- Anti-kickback violations might occur, in which the site and/or the practitioner knowingly and willfully offer, pay, solicit, or receive remuneration to induce referrals of items or services reimbursable by any federal health program.
- A physician might refer Medicare beneficiaries to entities in which the physician has a financial interest, in violation of the *Stark Law* (Stark).
- Tax law violations might occur if telemedicine services are provided internationally.

Risk Management Recommendations

Many existing fraud and abuse processes cover risks associated with telemedicine. Areas of heightened focus should include adequately securing data during transmission and verifying that data is received from an authorized source. It also is important to review the participating physician's relationships and outside interests to confirm that distant-site providers do not have conflicts of interest that violate Stark or the *Anti-Kickback Statute*.

Legal Agreements

Significant risks related to legal agreements include:

- Telemedicine services received could differ from what has been agreed upon by the originating site and the distant site.
- Agreements might not clearly identify the scope of services and diagnoses that will be provided.
- Agreements might not specify provider competency requirements such as licensure, quality of care, or the peer review process.

Risk Management Recommendations

At a minimum, telemedicine agreements should include language to outline:

- Who will be responsible for credentialing the providers at the distant site
- The state credentialing laws and licensing requirements for telemedicine services of the originating site and the distant site
- Whether the distant site is certified for Medicare and meets all CoP, if applicable
- Whether the agreements comply with the Medicare CoP
- What documentation must be retained by each party, where the documentation will be stored, and how the documentation will be stored

Credentialing

Significant risks related to credentialing include:

- The distant-site medical provider engaging in telemedicine services might not be certified for Medicare or meet all CoP standards.
- The provider performing remote services might not be credentialed and licensed in accordance with state and federal regulations.
- The provider might not have sufficient training and knowledge to perform the services.
- Medical staff might not operate under bylaws approved by the governing body.
- Medical staff peer review and quality processes might not be established and completed.
- State laws related to credentialing might not recognize the originating site or the distant site.

Risk Management Recommendations

An understanding of credentialing requirements for the originating site and the distant site is critical to limit liability and receive reimbursement. These laws vary by state and at times might conflict with federal requirements and other state laws. CMS relaxed credentialing requirements in July 2011, allowing facilities that offer telemedicine services to rely on the credentialing and privileging decisions of a distant-site hospital that participates in Medicare. In addition to meeting credentialing requirements, the originating hospital should obtain updated lists of credentialed physicians, review the quality of care and peer review processes for distant providers, and communicate any deficiencies to the distant site.

Liability

Significant risks related to liability include:

- Liability insurance might not cover telemedicine processes, services, or geographic areas.
- Peer review protections might not extend to information shared between the originating site and the distant site.
- Liability insurance might not cover the originating site or the distant site.

Risk Management Recommendations

Telemedicine might not be included in existing liability insurance policies. It is important to review existing policies to identify whether telemedicine services are included and make any needed changes to limit liability. Examples of items that might not be included are negligent credentialing, errors and omissions, privacy breaches, and disruptions of service during equipment failures. Hold-harmless clauses also should be reviewed to verify that coverage suffices. Healthcare providers should work with legal counsel and risk management to confirm that liability policies have appropriate language and coverage.

Billing and Reimbursement

Significant risks related to billing and reimbursement include:

- Reimbursable telemedicine services vary by state and payer.
- Payer requirements and definitions might not be understood by the originating site.
- There might be a lack of clarity in what the distant site and the originating site can bill, resulting in either both billing for the same service or nobody billing for the service.

Risk Management Recommendations

Reimbursement requirements vary by state and payer and continue to evolve. For example, Medicaid reimbursement varies significantly, and no two states are alike. The situation is similar for commercial payers. Understanding billing requirements for telemedicine and communicating what can be billed by both the originating site and the distant site is imperative. Billing also should be addressed in contracts between the originating site and the distant site.

Clinical Documentation

Significant risks related to clinical documentation include:

- Care provided to the patient might not be documented completely and accurately.
- The patient's medical encounters might not be documented in a single electronic health record.
- Documentation by the attending physician might not exist.

Risk Management Recommendations

Establishing clear standards about who will be responsible for documenting the patient encounter, what documentation is required, the time frame for completing documentation, where information will be stored, and how long the documentation will be retained reduces the possibility of incorrect diagnosis and delays in treatment. Documentation should include the mode of service delivery, sites that were linked, attendees' names, and any technical difficulties that affected the clinician's ability to carry out the consultation. Processes should be implemented to routinely monitor compliance with documentation requirements.

CHAN Healthcare™

A subsidiary of Crowe Horwath LLP

Informed Consent

Significant risks related to obtaining the patient's informed consent include:

- The patient might not be aware of telemedicine's benefits and risks.
- The patient might not be able to make informed decisions about information received during a telemedicine visit.

Risk Management Recommendations

Patient informed consents should be comprehensive and make patients aware of telemedicine's benefits and risks, such as delays due to equipment failures and security breaches. Providers should be aware of informed-consent requirements. These informed consents should be reviewed with the patient prior to providing services and sharing information with third parties that might be engaged in the patient care process. Patients also should be briefed and provided access to the notice of privacy practices in accordance with HIPAA privacy rules.

Telemedicine's Evolution

Telemedicine might become an option for some medical providers to achieve financial goals while remaining cost-effective in an era of decreasing reimbursement rates. Telemedicine use and offerings will change rapidly over the next few years as a method to offer cost-effective and efficient services to the increasing number of patients who will have healthcare as a result of the ACA. Successful telemedicine programs will rely on managing risks and monitoring state and federal regulatory changes.

www.chanllc.com

www.crowehorwath.com

Contact Information

Raj Chaudhary is a principal with Crowe Horwath LLP in the Chicago office. He can be reached at 312.899.7008 or raj.chaudhary@crowehorwath.com.

Debbie Gore is with CHAN Healthcare, a subsidiary of Crowe Horwath LLP, and can be reached at dgore@chanllc.com.

Darren Johnson is with CHAN and can be reached at dtjohnson@chanllc.com.

Nancy Van Dyke is with CHAN and can be reached at nvandyke@chanllc.com.

---

1 "What Is Telemedicine?" American Telemedicine Association, http://www.americantelemed.org/learn/what-is-telemedicine#

2 "Telemedicine," Medicaid.gov, http://www.medicaid.gov/Medicaid-CHIP-Program-Information/By-Topics/Delivery-Systems/Telemedicine.html

3 Bruce Japsen, "Obamacare, Doctor Shortage to Spur $2 Billion Telehealth Market," Forbes, Dec. 22, 2013, http://www.forbes.com/sites/brucejapsen/2013/12/22/obamacare-doctor-shortage-to-spur-2-billion-telehealth-market

4 Andis Robeznieks, "KentuckyOne to Offer 24/7 Telemedicine Service," Modern Healthcare, Sept. 20, 2013, http://www.modernhealthcare.com/article/20130920/NEWS/309209948/?template=printpicart

5 Chris Mazzolini, "Telemedicine's Next Big Leap," Medical Economics, Oct. 25, 2013, http://medicaleconomics.modernmedicine.com/medical-economics/news/telemedicines-next-big-leap

6 Sharon Hall, "Telemedicine: Avoiding a Risk Management Nightmare," Parker, Smith & Feek Inc., November 2011, http://www.psfinc.com/press/telemedicine-avoiding-a-risk-management-nightmare; and Paul Hildebrand, "Telemedicine Risk Management: A Practical Guide for Understanding and Mitigating Patient Safety Risk and Malpractice Exposure," TeamHealth, http://www.teamhealth.com/~/media/Files/Helpful%20Tools/White%20Paper%20Telemedicine.ashx

7 Dan Bowman, "AMA Telemedicine Policy Emphasizes In-State Licensure, In-Person Visits," FierceHealthIT, June 12, 2014, http://www.fiercehealthit.com/story/ama-telemedicine-policy-emphasizes-state-licensure-person-visits/2014-06-12