PUBLICATION

A Guide for Telemedicine Service Vendor Contracting: Applying Traditional Contracting Considerations in a New Arena [Ober|Kaler]

October 15, 2015

*Co-authored with Karen Byank Mathura**

While no longer "new," telemedicine, defined by the American Telemedicine Association as the use of medical information exchanged from one site to another via electronic communications to improve a patient's clinical health status,[1] is a rapidly expanding area of medicine. Health-care organizations, physician practice groups and various health-care service providers such as provider staffing companies and nurse call centers are eager to join in this trending mode of delivering medical care. They too want to offer a variety of modalities, including eICU/TeleICU, TelePsych, TeleDerm, ePrescribing and virtual medical offices or urgent care centers, just to name a few. These new and improved methods of clinical service delivery have set the stage for competition among software manufacturers and service vendors (professional and nonprofessional) looking to gain market share by offering the next cutting edge product and sweetening their clients' offers as they go along.

Understandably, providers, employers and health plans may be anxious to jump into this arena of clinical service; however, the parties should take time to carefully negotiate the implementing contractual arrangements. While the same issues and considerations common to many service arrangements must be addressed in the telemedicine context, there are telemedicine-specific issues to consider as well.

Furthermore, telemedicine service providers and their offerings run the gamut and not all telemedicine arrangements look alike. Examples include: (1) a professional telemedicine services agreement between a specialist and a health-care facility, or between a specialist and a primary care physician group for treatment of the facility's or group's patients; (2) direct to consumer arrangements; (3) a software license agreement between a nursing facility and a telemedicine IT platform provider; and (4) a beginning-to-end arrangement under which a telemedicine service company supplies software, hardware and the physician providers to a health-care facility for the facility's provision of telemedicine services to its patients and consumers.

This toolkit was designed to help navigate through all varieties of telemedicine arrangements by discussing standard contractual provisions in a services contract in the context of the telemedicine arena and noting questions the parties should think through and have answers to before signing.

The Services/Parties' Obligations

Ensure the description of the services accurately reflects the intended and accurate scope of the arrangement from all perspectives.

- Start with the easy question. What is the service being provided, and who is providing it? A telemedicine arrangement has two primary service elements: the physician (or other professional)

services and the connectivity service. Ensure the parties know who is bringing each of those to the table. For example, in an arrangement between a hospital and telemedicine service vendor, does the hospital expect to receive professional services similar to those in a typical professional services arrangement? If so, how are they obtaining the connectivity? Or is the expectation that the hospital is receiving a telemedicine service platform that allows its employed physicians to provide telemedicine services?

- Ensure physician availability and coverage requirements are reasonable. When a hospital licenses telemedicine software and equipment only, it must secure the professional service providers to render the telemedicine services. The arrangement may stop before it even starts if physicians are not willing to participate or if they are not appropriately licensed in the relevant states. (See Applicable Law herein.)
- Ensure physicians can meet appropriate licensing and credentialing requirements. Are physicians providing services across state lines? Some states have specific telemedicine licensure requirements. Which party is obligated to ensure compliance with state licensure laws? (See Applicable Law herein.)

  - The Centers for Medicare and Medicaid Services (CMS) has hospital-specific medical staff credentialing requirements.[2]
  - Medicaid requires that all providers practice telemedicine within the scope of their state practice acts. Some states have enacted legislation requiring providers using telemedicine technology across state lines to have a valid state license in the state where the patient is located.
- With regard to professional physician services, who is the "provider of record?" It may seem like a silly question and one to which the answer is clear, but mutual understanding of this point is sometimes taken for granted. For example, if a hospital contracts for the services of a third-party "telemedicine physician practice," does the third-party practice become credentialed as part of the hospital's physician practice and reassign billing rights or does the practice remain independent with its own patient relationships? (See The Patient Relationship herein.)
- Who is given control of marketing and final approval on any promotional materials? This is important from a business perspective but also from a regulatory compliance perspective when federal health-care programs are involved. Consideration must be given to whether compensation is being provided in exchange for the generation of business, and whether such arrangement complies with the federal fraud and abuse laws. (See Compliance herein.)

The Patient Relationship

Ensure the parties understand who has the patient relationship and how and when the relationship is formed. Although this is dictated by state law, generally speaking, it is presumed that any act of diagnosing or recommending treatment is the practice of medicine in the state where the patient is located for the purposes of medical licensure and the protection of public health, regardless of whether it is accomplished in the physical presence of a patient or through electronic media.

- Discuss the various stages of patient interaction within the telemedicine system and when the patient relationship attaches. For example, is there an initial intake form or are survey questions presented? Could the completion of the form be viewed as creating a patient relationship and, therefore, trigger a physician's professional obligations? How are patients informed of any risks in using the particular telemedicine service? How do patients provide informed consent? Telemedicine-specific informed consent documents are unique because not only do they speak to the risks, benefits and alternatives of the proposed treatment or procedure, but they also must address the risks of the cyber aspect of the telemedicine consultation or evaluation.

- Are patients reminded of their freedom to choose any provider? If a facility or other provider has entered into an exclusive arrangement with a telemedicine service provider, are the patients reminded of their continued right to choose any provider for their medical needs?

Billing

Make sure to capture the full scope of the parties' billing obligations and consider all applicable compliance obligations.

- Is there billing—either self-pay patient or third-party—involved in the arrangement?
- Ensure the parties understand which party's credentials are used in the billing. (See The Services/Parties' Obligations herein.)
- If one party is billing for the other, is the nonbilling party comfortable with the billing party's procedures, security and representations? If the billing entity is a nonparty does the provider of record have privity and recourse against that billing entity for errors?
- Will Medicaid or Medicare be billed? If so, does the arrangement meet the requirements of anti-kickback and Stark laws? (See Compensation herein.)
- Are all payor credentialing requirements met? Which party is responsible to ensure this—the provider of record, the billing party or another billing entity?

Compensation

Ensure the compensation terms are accurate and transparent.

- What compensation is exchanged pursuant to the arrangement? Ensure that all aspects of the compensation and the method by which it is paid are addressed in the agreements. For example, not only should the software license fee be specified, but also fees for maintenance, service, training and implementation. How are the physicians paid for their services? By the hour? By the service?
- Analyze the compensation arrangements with sensitivity toward federal fraud and abuse requirements. While federal health-care program payment is limited and may not currently apply to the arrangement, most likely it is only a matter of time before that changes. Discussions regarding new telemedicine HCPS codes are consistently found in Medicare fee schedule issuances. Moreover, while a telemedicine arrangement may not involve federal health-care program business, other arrangements between the parties may and a noncompliant telemedicine agreement could potentially call those other arrangements into question. For example, is a hospital providing above fair market value compensation for a specialist's telemedicine consult in the hopes that the specialist will increase referrals under its other professional services agreement with the hospital? Accordingly, structuring compensation terms in compliance with these laws would be prudent. Compensation cannot reward or induce referrals for federal health-care program business or vary with the volume or value of that business.
- To date, Medicare will reimburse for telemedicine services only for Medicare patients that present for treatment at a spoke hospital that is located in a health professional shortage area or in a county outside of a metropolitan statistical area. Medicare does have current procedural terminology (CPT) codes for remote monitoring, and yet it will not currently reimburse for telemedicine services delivered into the home. Pursuant to their contractual arrangements, some commercial health plans may pay for telemedicine related services while others will not. Accordingly, all of these payor policies must be analyzed in determining the arrangement's financial viability

Information Technology

Ensure that all IT obligations are fully negotiated, covered by the parties and specified in the agreement, so that the arrangement complies with all applicable rules and regulations.

- Privacy and security in telemedicine are generally governed by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and national standards for privacy and security regarding electronic health-care transactions. Additional areas of legislation that could impact hospitals and physician practice groups involved with telemedicine include the Red Flag Rules, the Federal Trade Commission's Disposal Rule and state privacy and data breach laws.
- Make sure it is clear who is providing the infrastructure and connectivity for the telemedicine communications. For example, does the arrangement only cover the software? Or is the IT connectivity and equipment included in the vendor's offering as well? If not, a hospital must seek a vendor that, not only provides such connections and equipment, but also one whose connections and equipment are compatible with the software. In that case, the hospital must know the questions to ask of the vendor to determine such compatibility. (See The Services/Parties' Obligations herein.)
- If the third-party software vendor is providing connectivity, does the vendor remain responsible for the software's functionality, or is the arrangement strictly a third-party license with limited service and support?
- In addition to the purchase of the software and hardware, have software hosting, maintenance and training services been considered? Who is responsible? Who is included in the population of physicians and providers who receive training, hardware and use of the software? Ensure that the provision of any training, software or hardware to referral sources complies with applicable fraud and abuse laws. (See Compensation herein.)
- What is the scope of use of unsolicited text messaging, and does it comply with the recent FCC declaratory ruling limiting such communications?[3]
- Who will be held responsible in case of a cybersecurity breach? Are the indemnification provisions adequate? What type of insurance limits are required and are they sufficient and in fact in place? A robust telemedicine practice should strongly consider the purchase of cyber liability insurance coverage. (See Insurance herein.)

Compliance Representations

The practice of telemedicine implicates regulations issued by a wide spectrum of government regulatory agencies. Key governing bodies of telemedicine include the Food and Drug Administration (FDA), CMS, the Joint Commission, state licensing boards, practice-specific professional associations and the Federation of State Medical Boards.[4]

In addition, as discussed above, there are state-based telemedicine rules, regulations and licensure requirements which may include the need for physicians to apply for and obtain a state-specific telemedicine license. Corporate practice of medicine and fee-splitting prohibitions are key. To the extent a non-professional telemedicine service vendor has an affiliated physician practice, or in any way could be viewed as providing the professional service or sharing in the revenue from such services, these must be considered.

State law on e-prescribing also must be considered in that there may be limitations on what types of prescriptions (e.g., controlled substances) can be prescribed via a video or telephonic consultation.

As previously suggested, it is prudent to craft arrangements in accordance with the federal fraud and abuse laws. Generally speaking compliance with both the antikickback statute and Stark law requires a written and signed agreement setting forth the service provided and compensation in advance, and such compensation must not vary with the volume or value of any referrals or business generated between the parties. (See Compensation herein.) "Mini-Stark" and "mini-kickback" laws on the state level should be considered as well.

Confidentiality

Fully assess any risks to confidentiality and assign responsibility among the parties to address those risks.

- Each party should perform its own risk assessment and should not rely on the other party's assessment. This is necessary from both a HIPAA and risk management perspective.
- Ensure patients still receive the appropriate information regarding their privacy rights, e.g., Notice of Privacy Practices, Authorizations.
- Ensure all parties are clear on where patient information is stored and who is responsible for health information management functions (e.g., disclosures, accountings and storage of health information).
- To the extent a non-HIPAA Covered Entity is involved in the arrangement with access to protected health information (PHI), a Business Associate Agreement will most likely be necessary.

Indemnification

Consider various potential claims situations when negotiating indemnification obligations. For example, in a soup-to-nuts model, referenced above, there is potential for malpractice claims, HIPAA claims, fraud and abuse claims, commercial business claims and cyber liability claims. Management should consider transferring the risk by purchasing applicable insurance coverage and ensuring protections are sufficient with the indemnification and limitation-of-liability/damages provisions. This is a way to ensure that the parties' verbal agreement is reflected in the language of the policy and contract agreements.

Limitation of Damages

For the above reasons and others, parties should ensure any cap on damages take into account the unique aspects of telemedicine. In the context of a telemedicine arrangement, electronic patient information is used, accessed, disclosed, created and maintained on a much more frequent basis than in a standard-services arrangement. The greater the availability of information, the greater the potential for the inappropriate use of that information that could constitute a HIPAA breach.

For example, hackers accessing 206 hospitals' electronic information recently caused a breach of medical records for 4.5 million patients across 23 states. Even more impressive, the health-care industry accounted for 42 percent of major data breaches reported in 2014, according to the Identity Theft Resource Center.[5]

A typical limitation-of-damages provision limits liability to three times the amount payable pursuant to the contract. Using the 4.5 million patient breach as an example, consider whether this amount of damages would be enough to address a mass PHI breach.

Credit monitoring expenses and the costs of notifying those with compromised data rise each year. The 2015 Verizon Data Breach Investigations Report outlined that a cyber breach can cost anywhere from $0.58 to $201 per record. With health-care-specific breaches, the estimated costs could be as high as $316 per breached record. When a physician practice or hospital is dealing with potentially thousands of patients' records, the procurement of appropriate insurance limits and a capped limitation of damages are necessities.

Insurance, Cyber Liability Insurance

Do the parties' current coverage policies address all potentials risks presented by the telemedicine arrangement? A well-prepared and insulated telemedicine provider generally has insurance policies providing coverage for professional and general liability, property and cyber liability. Cyber liability incidents within the health-care industry increased to approximately 17 percent in 2014. Traditional commercial general liability policies may exclude electronic data from coverage, and property policies may limit coverage for computer viruses. A crime-coverage policy will likely not cover the theft of credit card numbers because these numbers are not considered tangible property.

"Cyber risk" is an evolving phrase that has come to express the risks associated with storage and use of data, website content and function, email practices, privacy policies, Internet transactions and much more. Health-care organizations, joined by the government and educational institutions, are the three largest industry segments to face this rising risk.

As the marketplace for insuring cyber risks becomes more diverse, specific coverage for this evolving area of risk should be reviewed. Some specifics that a cyber liability policy could cover include: privacy liability coverage, network security liability, Internet media liability, cyber extortion, digital asset loss, business interruption, data breach fund, notification costs and public relations fees. Cyber insurance policies are becoming more important to a company's preparedness plan, with the adoption rate more than doubling over the last year from 10 percent in 2013 to 26 percent in 2014.[6]

Applicable Law

Consider whether the standard applicable law provision applies in this situation. There is a potential for multiple states' involvement because of the differing locations of the patients and physicians. Carefully analyze the advantages and disadvantages of the laws proposed to apply to any disputes that may arise, or consider keeping the governing law silent and let the specifics of a potential conflict dictate applicable law.

Ability to Modify Because of Changes in the Law

Flexibility in modifying the agreement to ensure legal compliance is a must as telemedicine is a constantly growing area. For example, as telemedicine gains momentum at the developmental and political levels, the FDA will gain at least some degree of monitoring control over a small portion of health-related apps, which will no doubt include additional regulations and guidance. Currently, a government-led task force including the FDA, the National Institutes of Health and the Department of Health and Human Services is crafting an action plan so that by 2017, mobile health (m-health) solutions will routinely be available as part of the best practices for national medical care and treatment.

Conclusion

Telemedicine is an exciting area which started out as a value-added service or a subset of health care but has quickly become its own industry. To be successful, parties have to carefully negotiate and implement their telemedicine service arrangements to ensure they are compliant, provide protection and deliver services in the manner the parties intended. While this process involves many of the same general issues presented by the majority of health-care service agreements, telemedicine arrangements come with their own specific set of considerations.

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

2 42 C.F.R. §482.12.

3 In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, WC Docket No. 07-135 (FCC July 10, 2015), available at https://www.fcc.gov/document/tcpa-omnibus-declaratory-ruling-and-order.

4 Federation of State Medical Boards, Telemedicine Policies Board by Board Overview.

5 2015 Second Annual Data Breach Industry Forecast, available at http://www.experian.com/databreach.

6 "Is Your Company Ready for a Big Data Breach?" Ponemon Institute, September 2014, available at http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf.