THE
NATIONAL LAW REVIEW

Leading Health Care’s Information Age Over the Horizon

Article By Jennifer S. Geetter
Bernadette M. Broccolo
Clare Connor RanalliDale Van Demark
Sandra M. DiVarco
McDermott Will & Emery

Health Law & Managed Care
Health Care Law Reform
Administrative & Regulatory
All Federal

Thursday, March 27, 2014

Technological innovation in health care delivery is happening everywhere: institutional health care providers, informatics and population health organizations, start-up technology companies, physician practices and insurance and managed care companies have all been incubators for products and business methods to graft new information technology to health care delivery systems. These innovations have significantly expanded the ways in which health care is delivered, and can be powerful tools for improving patient access to care, health care delivery efficiency and the quality of care.

While significant delivery system innovation through technology may seem just over the horizon, the rapid proliferation of medical apps and telemedicine services has left regulators struggling to keep up and has introduced technology companies and entrepreneurs to the complex regulatory environment of health care.

Although the diversity of business models for technology-assisted health care delivery is staggering, a few core issues are applicable to just about any effort.

REVENUE MODEL

1. Medicare reimbursement for telemedicine services is subject to geographic and service restrictions, making reimbursement largely unavailable for most of the country. Legislative attempts at liberalization have produced incremental expansion, while large-scale expansion efforts have not yet produced results (though legislation is pending).

2. Many Medicaid programs reimburse for telemedicine encounters pursuant to special programs designed to address specific areas of need such as access. Each program is different, however, making multistate efforts difficult to implement.

3. Populations subject to state-provided health care services, such as prison populations, are increasingly treated through connected health models. Innovative approaches to providing care to these types of populations may be welcomed by federal, state and local governments, and may represent significant markets in their own right.

4. Consumer-focused efforts, such as mobile medical apps, monitoring devices and online-based reservation systems, may have simpler revenue models, but the structures may still require consideration of health regulatory issues, including reimbursement and privacy-based requirements.

5. States are increasingly requiring insurance products to reimburse health care providers for certain types of services provided via telemedicine systems.

PRACTICAL NOTE: While connected health revenue models require research and planning, the evolving reimbursement landscape may open the door to additional sources of revenue. Accordingly, periodic review should be conducted to avoid missing opportunities.

PRACTICAL NOTE: There is little uniformity in the rules for participation among the various reimbursement efforts offered by government agencies and private payors. Nonetheless, participation may provide valuable experience integrating technology in the clinical setting.

PERSONNEL

6. Connected health delivery models can implicate professional licensure rules and regulations as well as credentialing requirements. When the applicable business model is national in scope or when the care provided crosses state borders, licensure can become a complicated issue.

7. While some telemedicine and other technology-assisted programs do not contemplate physician interaction, physician oversight of extenders and other health care service providers may still be required or recommended to ensure quality and safety.

8. National or multi-state programs may implicate state laws prohibiting the practice of medicine by anyone other than licensed professionals or organizations they own and control. Working within the requirements of the so-called “corporate practice of medicine” doctrine is possible, but needs to be addressed during the planning stage.

9. State and federal fraud and abuse laws may be implicated by connected health delivery models that compensate physicians for services and provide them with other benefits, such as access to telemedicine technology. For example, even cash-only business models may implicate fee-splitting prohibitions in some states.

PRACTICAL NOTE: While specific reimbursement programs may impose staffing, licensing or other personnel requirements, best practices are still being developed, and different connected health programs will have their own unique staffing and personnel challenges.

PATIENT RELATIONSHIP

10. Remote encounters between physicians and patients may result in the creation of a physician-patient relationship, which may expose the provider to patient abandonment claims (particularly when multiple physicians are involved in the telemedicine encounter and it is less clear who controls the patient’s care). Steps should be taken to ensure the encounter is limited enough to avoid this eventuality or to ensure the encounter adheres to all appropriate practice requirements and the laws of the state in which the patient is located.

11. While remote encounters with physicians can create a physician-patient relationship for purposes of physician liability, it may be insufficient to allow for the valid writing of prescriptions. Some states allow this while others do not.

12. Standard practices around patient consent may not be sufficient if the patient encounter is remote. Consideration should be given to both state law requirements and the provider’s assessment of the likelihood of confusion or misunderstanding given the nature of the encounter.

PRACTICAL NOTE: The physician-patient relationship is evolving along with the development of connected health delivery options and models. Clear communication with patients is imperative to ensure the appropriate relationship is established and confusion is avoided.

PRIVACY

13. Connected health delivery models implicate state privacy and informed consent laws, federal requirements under the Health Insurance Portability and accountability act of 1996, and other laws related to preserving the integrity and safeguarding the privacy and security of patient health information. If the program extends across state lines, multiple state privacy laws may apply.

14. The accumulation of patient health information resulting from the use of communication technologies (e.g., remote monitoring devices and store-and-forward applications) presents special storage and management compliance challenges as the information may be in different formats (e.g. , video, images, text) and be accessible by multiple professionals from different organizations.

15. The delivery of health care services using consumer and web-based technologies (e.g., smart phones, mobile applications, laptops) is evolving rapidly and resulting in the utilization by practitioners of multiple devices—and in some instances their own. So-called “bring-your-own device” policies and the associated activities present special information security and privacy issues.

16. As more community hospitals enter into telemedicine arrangements with tertiary hospitals for specialty

consults, and information is shared between facilities to facilitate credentialing and privileging decisions, it will be important to implement strategies to safeguard the privacy and security of physician peer review and patient information.

PRACTICAL NOTE: The multiplicity of privacy and data security concerns creates a complex and daunting set of compliance planning considerations. In addition, data breaches continue to be headline-grabbing events, and connected health delivery models increase risk because, at their core, they are designed to create a freer flow of information. Accordingly, it is imperative to conduct thorough privacy and security reviews of all connected health programs, and to adopt and implement appropriate compliance policies.

EQUIPMENT

17. As health care technology plays an increasing role in every stage of clinical encounters, the possibility that equipment failure or malfunction will negatively impact clinical outcomes and patient safety also increases. Frequent monitoring of the performance and the use of the equipment is critical.

18. As technology companies develop and market devices for health-related applications, they may become subject to oversight by the U.S. Food and Drug Administration (FDA). Some states also regulate technologies used in the treatment of patients. For providers, FDA oversight can offer comfort with respect to the application of the regulated technology in a clinical setting. For many technology companies, however, FDA oversight may be new and the corresponding compliance requirements difficult to quickly and adequately address.

PRACTICAL NOTE: Technology standardization, maintenance best practices and interoperability of connected health technology are all evolving challenges. Active monitoring and periodic review of FDA guidance, liability standards and industry best practices are highly recommended.

RISK MITIGATION

19. As connected health delivery models continue to develop, expect standards of care, whether local or national, to evolve. As this occurs, standards for liability will also evolve, although more slowly, absent specific legislation.

20. The use of technology in the delivery of health care raises potential risks and exposure arising from inappropriate or incorrect use, incompatibility, malfunction or obsolescence of technology. On the other hand, providers may be liable for patient harm that results from the failure to use available technologies.

21. Malpractice liability insurance policies do not necessarily cover telemedicine services, and some policies only cover claims related to medical services provided to patients in the state where the carrier agreed to cover the provider.

PRACTICAL NOTE: A connected health program should be implemented with the understanding that risk may not be as understandable as it may be in other settings.

PRACTICAL NOTE: To limit the risk of liability when technology is involved in the delivery of health care, policies and protocols should be implemented to prevent transmission errors that could interrupt remote communications and to ensure proper use of the technology.

Source URL: https://www.natlawreview.com/article/leading-health-care-s-information-age-over-horizon