THE
NATIONAL LAW REVIEW

Digital Medicine: Health Care Providers' Side of the Story

Thursday, August 2, 2018

Health care technology, particularly digital medicine, promises great new capabilities that will improve outcomes and reduce overall costs and time constraints. Digital medicine encompasses a broad-range of technologies, from technologies used to record, retain, and manipulate health data (i.e., Electronic Health Records aka., EHRs) and thereby make it more useable and amenable to analysis; to actual tools in clinical care (i.e., medical imaging, wearable sensors) that can measure physiological parameters or patient activity and facilitate clinical care and decision-making.

Drinker Biddle

Article By Krissa L. Webb
Svetlana Lyapustina, Ph.D.
Drinker Biddle & Reath LLPDBR on Data

Communications, Media & Internet
Health Law & Managed Care
All Federal

The problem is that health care providers (operating on narrow margins and focused on individual patient care) may not be best situated for making costly and complex technology acquisitions, or for maintaining and securing complex information systems and technology. As new technology is introduced, and as cybersecurity risks proliferate with broader adoption, health care providers are stretched thin to keep pace with these new opportunities and risks. So how does a health care provider adapt to this environment?

The Pros and Cons

Real evidence is growing that digitalization may lighten a health care provider's burden on the whole. For example, a 2016 report to U.S. Congress noted studies indicating that telehealth and remote-monitoring tools have the potential to improve access and outcomes. Also, a 2014 survey of U.S. nurses indicated that EHR systems aided in record management and error reduction and freed up time to interact with patients. Similarly, newer technologies were viewed as reducing the health care providers' immediate workload in studies conducted in 2003-2009 in Brazil and the Netherlands. Accordingly, there is good reason to believe technology will continue to bring valuable efficiencies and improvements to health care and to encourage its proliferation. However, actual cost-savings borne out of health care technology remains elusive for health care providers and, in fact, medical technology is considered one of the main drivers of increased costs in health care.

Improvements in technology come with additional front-end and ongoing costs—in both time and financial resources. Keeping up with the latest in health care information technology is complex, continuous, expensive, and tedious for providers who are every day faced with more pressing issues of patient care. Such issues include:

• Ongoing training on proper and legally compliant use of new technologies.
• Remaining informed of new and evolving regulatory and legal requirements issued by government agencies and implementing enterprise compliance programs.
• Remaining abreast of industry best-practices and recommendations from professional societies.
• Re-envisioning health care provider schedules and work flows to ensure time to review and react to alerts and notifications streaming in from connected patient devices.
• Training patients on relevant digital tools and ensuring adequate patient-support resources.
• New infrastructure investments (e.g., physical space, physical equipment, power and connectivity, data storage facilities).
• Expansion in workforce to add personnel with technology, privacy, and security expertise.
• Managing software and hardware upgrades, while ensuring data integrity and usability.
• Maintaining ongoing security measures, patches, software upgrades, auditing, and other measures necessary to protect against rapidly changing security vulnerabilities.

Furthermore, even efforts to update aging technology is fraught with complication when old and new systems co-exist, presenting additional challenges and vulnerabilities, as explained in an American Hospital Association (AHA) letter to the U.S. House Energy and Commerce Committee assessing cybersecurity risks.

Meanwhile, to date, payors have been slow to adapt measures to support the added costs associated with the foregoing advancements. This is most acutely seen in the slow adoption of reimbursement models built for supporting the costs of remote medical care. Specifically, in the U.S., Medicaid reimbursement for telehealth services has been slow to roll out state by state, as has reimbursement by Medicare and commercial payors, although some progress is expected soon. Similar issues have been experienced in Europe.

To its credit, the federal government has created incentive programs to encourage and facilitate implementation of certain health technology (i.e., electronic health records). It has also opened the door for additional cost-saving collaborative efforts between health care providers by creating, and continuing to consider, safe harbors that permit provider risk and resource sharing without fear of committing health care fraud. Unfortunately, these types of solutions lag behind the needs of the market. The urgency of finding a solution is underscored by a recent finding that less than half of health care providers have a budget for cybersecurity, and many have concerns over liability and other barriers.

Ideas for improving cost/benefit ratio

To address these barriers to technology adoption, health care provider associations, including the American Hospital Association and the American Society of Cataract and Refractive Surgery, have called on regulators and technology manufacturers to support more efficient adoption of new technology. Likewise, medical device manufacturer associations, such as AdvaMed and MITA, are also recognizing their need to share responsibilities and expenses. Pointing in the same direction, the proposed updates to the framework for cybersecurity issued by the U.S. National Institute for Standards and Technology (NIST) expand the target audience of those responsible for implementing cybersecurity. And for its part, the FDA promises to engage the whole "ecosystem," including federal partners, manufacturers, payors, patients, and health care providers, as the agency is building the National Evaluation System for health Technology (NEST). The hope is that these measures will strengthen the connected digital health environment overall, so that health care providers responsible for transmitting and storing sensitive data on those networks will be less vulnerable at all times.

In the end, to build successful and sustainable transformations in health care, each such transformation will likely require an innovative solution.

Source URL: https://www.natlawreview.com/article/digital-medicine-health-care-providers-side-story