Telehealth and Telemedicine: Clinical and Regulatory Issues

Somesh Nigam, PhD

Editor's Note: This is the second in a series of articles by Dr. Nigam on the use of digital information and communication technologies, commonly referred to as telehealth and telemedicine. In this article the author discusses clinical practice issues and the challenges of regulation and security of digital health information facing society today.

The incorporation of teleconsults as one of the services offered by insurance companies is growing. Oscar Insurance Corporation based in New York, for example, positions teleconsults as a central part of their marketing strategy. The company provides a doctor-on-call service over the phone at any time. In addition, it offers a mobile application that enables its customers to view and manage their health history, including doctor visits, prescriptions, and lab work.

From a regulatory perspective, three issues will influence the ultimate utility and success of doctor-on-call and other telemedicine services. These include the patient-doctor relationship, data security, and data sharing.

Maintaining the Patient-Doctor Relationship

When used properly, telemedicine has the potential to enhance the patient-physician relationship through increased opportunities to communicate and improved access by both parties. But there is the risk that by eliminating, or at least minimizing, common face-to-face consultations, telemedicine may disrupt some of the traditional principles that govern the physician-patient relationship. In 2014, Dr. Robert Wah, President of the American Medical Association, asserted, "We always look to have the best possible information to take the best possible care of our patients. And we feel that face-to-face interactions are a rich source of that information. It's hard to come to that level of information through other modalities." Dr. Wah acknowledges that exceptions include emergencies and physician cross-coverage. “But those are the outliers."

From a regulatory perspective, mandates should focus on ensuring integration of health data and information with all healthcare professionals who are providing care. At the same time, telemedicine must never exert long-term intermediation on the durable patient-physician relationship.

Quality of Decision Support and Predictive Clinical Algorithms

One area that has not garnered sufficient attention from regulators or providers is around the quality and effectiveness of decision support tools and predictive algorithms that are beginning to flood the marketplace. If powered by a high level of positive predictive value (PPV), these tools have the potential to serve as early warning systems (e.g., who is going to be hospitalized or who is going to become a diabetic) and “force multipliers” for providers (e.g., what is the best course of action for my particular patient based on the best published evidence and outcomes in thousands of similar patients). In this regard predictive algorithms can serve as a “super diagnostic” tool for providers that can help optimal and timely allocation of scarce resources.

On the contrary, dependence on a less effective decision support tool can cause expensive medical resources to be directed towards less effective therapy or on patients who may not be the best targets. At worst, poorer algorithms (just like lower quality providers) can miss out on serious developing conditions or complications.

In this regard it is important to note that highly effective predictive models of the future will need to be powered by large volumes of anonymized patient-level longitudinal data (both claims and EHR based) and enormous computing power—exactly the kind of assets IBM has been developing and accumulating with Watson suite supercomputing, machine learning based predictive technologies, data derived from their recent acquisitions of Explorys and Truven and partnerships with premier centers of excellence such as Cleveland Clinic in Ohio and the he University of Texas MD Anderson Cancer Center, in Houston, Texas.

Only time will tell how soon this vision is accomplished. However there is a lot of excitement about IBM Watson's role in the emerging market for population health management and clinical decision support that is expected to grow to over $20B by 2020.

Security

As telemedicine and data collection and monitoring become ubiquitous, stakeholders have good reason to insist on assurance that their data are secure. Among all of America's critical infrastructures, the healthcare sector is the most targeted by persistent attacks from malicious hackers intent on exploiting the vulnerabilities of insecure and antiquated networks in order to obtain patient health records. And the problem is growing, with eight of the ten largest hacks into any type of healthcare provider occurring in 2015, according to the US Department of Health and Human Services (Table 1).

For example, in March 2015, Excellus Blue Cross Blue Shield discovered a breach and notified affected individuals that the attackers may have gained access to personal information from as many as 10 million individuals, including name, date of birth, Social Security number, mailing address, telephone number, member identification number, financial account information, and claims information. The number of affected individuals even included members of other Blue Cross Blue Shield plans who sought treatment at a facility located in the Excellus service area.

Already this year, hackers infiltrated the computer systems of two Southern California hospitals with ransomware—malware that restricts access to a computer system and demands that the user pay a ransom to remove the restriction.

Clearly, passwords are antiquated. New strategies are needed to meet the challenge of electronic medical record interoperability between payers and providers. One option known as blockchain technology was first used for Bitcoin transactions. Elsewhere on the *TMT* website, contributor Peter Nichol proposes that blockchains may also be used

to securely manage electronic medical records.

Electronic Medical Record Regulations

Today, we silo health information. This must change to permit free exchange of data, with the patient acting as the gatekeeper. Clarifications in EMR/EHR (electronic medical record/electronic health records) that detail the manner in which healthcare providers qualify for Medicare and Medicaid EMR regulation pertaining to the meaning full use of these databases are needed. To this end, CMS.gov (Centers for Medicare and Medicaid Services) has released the 2016 program requirements that eligible professionals, eligible hospitals, and critical access hospitals must meet in order to participate in Medicare and Medicaid EHR Incentive Programs.

There is also a need to modify and update HIPPA (Health Insurance Portability and Accountability Act) regulations and allay skepticism over the reliability of technology and potential devastation resulting from compromised patient information. These concerns can be addressed through a combination of legal, technical, and administrative security measures combined with assurance that ultimately patients control their data and may opt out if they feel it is in their best interest.

One approach to empower consumers' ability to control their records—and ultimately their healthcare—is Blue Button (Figure 1), which was initiated in 2010 by the Markle Foundation—a charitable organization concerned with technology, healthcare, and national security.

Blue Button enables consumers to securely access their personal health data online, including claims and personal health information maintained by doctors, hospitals, health plans, and others. Patients can access and download their health data without using special software. They may also share data with trusted individuals, including other physicians and family members.

Several federal agencies, including the Departments of Defense, Health and Human

Services, and Veterans Affairs have implemented this capability for their beneficiaries. There are also pledges of support from numerous health plans across the United States. In the future these data, with patient permission, may also be used in a disaggregated form to further medical research.

Conclusion

Today, the healthcare industry is in the process of responding to increasing consumer demands for convenient and affordable alternatives to traditional healthcare. Surely, telehealth will continue to permeate healthcare at all levels as a natural extension of team care. However, our ability to successfully navigate significant regulatory issues will determine the extent to which hospitals, health systems, and other providers can offer specific telehealth services and meet the primary goal of improved societal healthcare.

Tags: clinical, electronic medical record, EMR, HIPPA, issues, Medicaid, Medicare, Nigam, regulatory, regulatory, security, sharing, telehealth, telemedicine, Watson Suite

Somesh Nigam, PHD, is Vice President Information & Data Governance and Health Informatics at IBM.

Table 1.

Company	Individuals Affected (m)	Date of Breach	Type of Breach	Location of Breach
Anthem	78.8	Mar-15	Hacking/IT incident	Network server
Premera Blue Cross	11	Mar-15	Hacking/IT incident	Network server
Excellus Health Plan	10	Sep-15	Hacking/IT incident	Network server
Science Applications Int'l Corp.	4.9	Nov-11	Loss	Other

Community Health Systems Professional Services Corp.	4.5	Aug-14	Theft	Network server
UCLA Health	4.5	Jul-15	Hacking/IT incident	Network server
Advocate Health and Hospitals Corp./ Advocate Media Group	4	Aug-13	Theft	Desktop computer
Medical Informatics Engineering	3.9	Jul-15	Hacking/IT incident	Electronic medical record, Network server
Xerox State Healthcare	2	Sep-14	Unauthorized access/disclosure	Desktop computer, email, laptop
IBM	1.9	Apr-11	Unknown	Other

Source: US Department of Health and Human Services

Figure 1. Blue Button is a symbol for patients to view online and download personal health records.