MITIGATING RISK IN TELEMEDICINE: Taming Compliance, Security and Governance Challenges

Make the most out of the exciting move to telemedicine by ensuring you are taking the important steps in risk mitigation.
Telemedicine, one of the fastest-growing segments of the healthcare industry, is particularly well-suited for the new reality of today’s value-based care model. Rather than clogging up emergency rooms and already-crowded private practice offices with relatively small health issues, patients increasingly are utilizing a wide range of technology options to consult with, and receive treatment from, physicians and their staffs. That flexibility is changing the rules of the game for providers and patients who want a better healthcare delivery experience and process.

As a result, global investments in telemedicine solutions are surging. Research from Mordor Intelligence pegs telemedicine revenues at more than $66 billion by 2021, a robust 19% compound annual growth rate over a 6-year period.1 Other data indicates that 63% of insured adults have access to virtual care services enabled by technology, such as phone calls, email, Webcam sessions, instant messaging, texts or mobility-based healthcare provider applications.2 Telemedicine has found a home in many use cases, from remote patient monitoring and practitioner collaboration to interactive patient-doctor consultations and improved physician access in rural areas with fewer local doctors.

As a result, telemedicine has delivered numerous benefits from all parties in the healthcare ecosystem. For providers, it allows them to interact with and treat patients with less-dramatic problems faster, giving them additional in-person time for more challenging patient scenarios. For hospitals and practices, it provides an incremental revenue flow, particularly in light of the increased recognition of telemedicine as a reimbursable solution by most states and insurers. And for patients, it allows them to avoid crowded and potentially unhealthy physical spaces like emergency rooms and doctors’ offices in order to be “seen,” diagnosed and treated.

MITIGATING RISK IN TELEMEDICINE:
Taming Compliance, Security and Governance Challenges

1 Global telemedicine market: Growth, trends and forecasts,” Mordor Intelligence, January 2017

2 2016 connected patient report, Salesforce Research/Harris Poll, July 2016
Still, we’re talking about healthcare delivery, which means there are always going to be unique and potentially significant challenges that must be acknowledged, addressed and remediated in telemedicine. The early adopters of telemedicine solutions have blazed the trail for others, and have given us a roadmap for risk mitigation in three major areas:

**Compliance.**

Healthcare is undoubtedly one of the most highly regulated industries in the world—a trend that is likely to continue for some time.

**Security.**

The dramatic economic value of compromised or stolen health records means that healthcare is literally a treasure trove for hackers, and infrastructure realities such as wireless networking and the widespread use of personal mobile devices adds complexity and risk to telemedicine.

**Governance.**

Healthcare organizations place a high value on data governance, in part because of the related compliance and security issues, but also because of the diverse, expanding and ever-changing nature of healthcare data and its many sources.
Regulatory mandates are an increasingly challenging issue for healthcare IT, and this is especially true in telemedicine. That’s because the process of providing secure, private, authorized and documented access to information in electronic, rather than human, interaction is a still-evolving one. As a result, telemedicine activities fall under the purview of a large number of compliance rules and governing bodies, including but certainly not limited to:

- HIPAA
- PCI DSS
- HITECH
- COPPA
- Affordable Care Act
- Department of Health and Human Services
- National Institute of Standards and Technology

There also are large and growing numbers of state and local regulatory bodies that increasingly are participating in regulatory mania, as well as a host of agencies in countries and regions outside the United States.

These and other mandates cover a wide range of requirements for healthcare information, such as Electronic Protected Health Information (E PHI) and Personally Identifiable Information (PII). Of course, there also are important financial issues for compliance mandates that impact providers utilizing telemedicine, including heavy fines for privacy violations and cuts in federal insurance reimbursements for failure to demonstrate Meaningful Use.

One of the hard facts about HIPAA, the centerpiece of all healthcare mandates, is that it is not ever set in stone. In fact, it is a moving target, with regular updates and extensions to the core regulations. So, achieving a state of compliance can be ephemeral, especially for a fast-growing and rapidly evolving segment like telemedicine, where new technical, physical and administrative issues arise all the time.

Take, for instance, the idea of video-based interactions between doctors and patients. This is one of the most-desired capabilities by both sides of the telemedicine equation,
because it allows for physical inspection of the patient and a more personal interaction. But consumer-friendly mobile video applications like Skype and Face Time come with unique regulatory challenges over privacy, audit trails and video file storage security.

Providers that have adopted video applications for telemedicine point out that virtual visits need to be treated in much the same way as in-person visits from a privacy standpoint. For instance, providers should conduct video-based visits in a private area where highly personal information can be conveyed with confidence of, and respect for, patient privacy. These video applications also should have seamless links to electronic medical records (EMRs) in order to ensure the most up-to-date information is accessible to all those authorized to examine a patient’s full history.

For employers offering telemedicine as an employee benefit covered under health insurance, it is important to consider numerous compliance angles above and beyond HIPAA, including COBRA and ERISA. This requires a flexible approach to IT-based telemedicine solutions development and deployment, since many municipal bodies have different approaches to what is and isn’t covered in telemedicine. “While many states are loosening their restrictions on telemedicine, and even requiring insurers to pay for it, some states are headed in the opposite direction,” warned Scott Behrens, an ERISA compliance attorney with Lockton Benefit Group.

The bottom line for mitigating compliance risk in telemedicine: Be sure to look for a solution that not only embraces the full spectrum of today’s compliance issues (across all relevant municipal, geographic and regulatory bodies), but also is flexible enough in its design to account for the ever-changing nature of compliance mandates over time. Your solution should also be technology-agnostic in order to protect privacy of data collected from any number of different devices, from traditional desktops and notebooks to smartphones, tablets and even Internet of Things (IoT) equipment such as sensors and RFID-based medical instruments.
Healthcare security is a hotbed of activity, and telemedicine only adds to the mix. The high economic value of healthcare records has spiked cyber attacks; in fact, the average healthcare organization experiences one cyber attack every month, according to leading cyber security researcher and consultant Ponemon Group. In fact, Ponemon noted that 48% of healthcare IT professionals surveyed said their organizations have experienced an incident resulting in the loss or exposure of patient information during the past year.  

Technology, particularly at the endpoint and core infrastructure, is a major issue in locking down security for telemedicine. Since a big attraction of telemedicine—for both providers and patients—is its ability to allow the use personal mobile devices, the security of those devices can be a wild card. That’s because so many personal devices are often unmanaged from a security standpoint; they often lack the most up-to-date security defenses, such as patches or authentication layers.

User training also is a vital aspect of good security hygiene for telemedicine. That goes for doctors, nurses, clinicians, patients and caregivers. This often is covered under healthcare providers’ data governance platforms, but it also is an essential element to best practices for telemedicine security. Simple missteps like providers failing to log out of a video chat session can leave vital patient records at risk. Imagine the field day cyber attackers could have with ransomware demands upon entry into patient records containing highly sensitive and potentially embarrassing medical conditions.

Finally, be sure that your telemedicine solution is designed in accordance with the all-important SANS 20 Critical Security Controls standard, which provides an important benchmark for such requirements as hardware device inventory, software inventory, system configurations, vulnerability assessments, malware defenses, application-layer security and much more.

The bottom line for mitigating security risk in telemedicine: Your telemedicine solutions must be designed from the start with security as a core requirement across the full telemedicine platform. They must require multi-factor authentication to ensure only those truly authorized—and in their relevant roles and identities—be allowed to access patient data. It also must be able to assign proper access to both digital and physical access, such as ensuring only authorized personnel can access secure records facilities or physical equipment. Finally, telemedicine solutions must account for the unique and still-evolving security requirements for IoT components, which are increasingly become a vital part of the healthcare delivery ecosystem.
Governance risk

This is an area often overlooked in healthcare IT—as it is in most other industries. Governance—defined as policies, procedures, plans and practices that ensure high confidence in the accuracy, completeness, timeliness and security of data—covers a wide range of issues. These typically include data retention policies, access authorization, data disposal and archiving, user training, data heritage and data stewardship. All of these are essential to good telemedicine, especially since they also profoundly influence the organization's ability to mitigate risk in compliance and security.

Data governance is also important in telemedicine because it acts as the foundation layer for healthcare analytics, a vitally important requirement for all aspects of modern healthcare—clinical, operational, financial, legal and regulatory.

One of the governance challenges healthcare IT professionals may run into with telemedicine solutions is application ownership and data stewardship. Doctors and other medical practitioners don’t usually think of themselves as IT people, and in fact they prefer staying far away from IT-related tasks that they think take them away from spending time with patients. But medical professionals, like line-of-business users in other industries, typically have valuable insight into workflows, process management and emerging use cases that IT people often lack. Consideration should be given to having doctors, nurses and other medical staff represented on a data governance team to provide input on the architecture and policies for telemedicine solutions.

Having an overarching data governance platform is very important for success in telemedicine because it provides the basis for issues such as data quality, data integrity and a 360-degree view of the patient that are at the heart of good telemedicine solutions.

The bottom line for mitigating governance risk in telemedicine: The best telemedicine solutions will be planned, designed and deployed with an eye toward tight integration with data governance platforms, rather than tweaking them as an afterthought once telemedicine solutions are up and running. As telemedicine grows in utility, adoption and strategic value to the healthcare organization, it will come with seamless connectors to existing data governance platforms, as well as being designed to operate hand-in-glove with governance platforms from the start.
While there are a number of different telemedicine solutions providers, many of them have been designed for specialized aspects of the solution’s uses, such as video-based consultations or allowing patients to have access to their records after being released from primary care.

However, the eVisit telemedicine solution has been designed and widely deployed as a HIPAA-compliant platform that enhances patient engagement, increases provider revenue and streamlines clinical caregiving.

Most importantly, the eVisit software was designed by experts in both healthcare practices and healthcare IT requirements in compliance, security and governance. That allows healthcare organizations to implement a fully compliant telemedicine solution that identifies, blocks and remediates regulatory and cyber risks, while ensuring consistency with enterprise-wide data governance policies.

The eVisit software enables data transfer to leading EMR software; because it is done as a workflow solution rather than as a software integration, it is easier and faster to deploy, limiting the need for expensive and time-consuming programming.

One of the key business benefits of the eVisit platform is its ability to help increase patient flow. For instance, when used to treat minor medical conditions, eVisit can increase volume by as much as 300%, while patients receive high-quality medical care without the time, expense and hassle of traveling to an often-crowded doctor’s office, urgent care facility or emergency room.

eVisit also provides customized staff training, helping users not only to understand how to navigate the application but also to spot opportunities to use eVisit to improve workflow and increase revenue.

Finally, the eVisit team has extensive experience in helping organizations ensure that their telemedicine activities qualify for reimbursements from both public and private healthcare systems.