Healthcare providers implement virtual care systems to meet consumer demand

VIRTUAL CARE CONTROLS AUDITS

Five areas to consider in the design of virtual care system audits

By James Kidwell, JD, CISA, and Molly Murphy, CIA, CRISC, CRMA, CFE, CRCR

The consumerization of healthcare and advances in medical, communications and computing technology are bringing more care delivery options to patients and providers than ever. In addition to the typical visit to a doctor's office or hospital, patients now have online, phone and videoconference care options. Patients can have remote visits from the convenience of home, and providers are able to conference-in professionals from other locations.

As healthcare providers implement virtual care systems to meet consumer demand, the operational, financial, legal, compliance and technology risks should be considered before and after implementation. You must utilize the full portfolio of internal audit expertise to provide management assurance regarding the adequacy of internal controls in this emerging and strategically important area.

State licenses

While technology has created opportunities for providers to treat patients beyond typical geographic boundaries, state legal requirements need to be considered. For instance,

> Providers must be credentialed and privileged for each facility and state where patients are physically located.

healthcare providers are licensed to practice medicine in a specific jurisdiction. Laws addressing telehealth or virtual medicine are not yet established nationally, and they can differ between states.

Organizations that provide patient care across state lines should be aware of the state telehealth laws, practice acts, licensing requirements and standards of care for each state in which they plan to render services.

Credentials and privileges

Provider credentialing and privileging is the process an organization uses to confirm provider qualifications and to authorize the provider to deliver specific services. Providers who perform services in multiple locations must be credentialed and privileged for each facility and state where patients are physically located. This plays an important role in patient safety, quality of care and reimbursement, whether the service is performed in an in-person or virtual environment.

Patient treatment limitations

The virtual medicine environment lends itself to specific challenges from a provider and patient relationship standpoint. Organizations should disclose limitations and have a mechanism in place for patient acknowledgment of treatments that may need to be accomplished in a traditional setting, such as symptoms related to heart attack and diabetes complications.

Adequate training

The training required for medical personnel in the virtual environment involves new procedures such as verifying the patient's identity and location as well as understanding the types of service that can be performed virtually as opposed to in-person. Organizations should consider adequacy of periodic, specialized training for providers and staff to ensure they are cognizant of requirements.

Technology risk

Virtual care applications and services rely heavily on IT infrastructure assets, often involving cloud-based computing environments. In addition to the usual cloud vendor relationship risks and concerns, virtual care sessions must meet HIPAA privacy and security requirements.

When entering into relationships with virtual care vendors, healthcare organizations need to consider due diligence responsibilities. These include obtaining business associate agreements, evaluating third-party IT software development security standards, and establishing a cloud service provider/vendor due diligence program based on globally accepted audit and security frameworks. Strong controls such as encrypted sessions, isolated networks and security event detection and prevention should be employed to safeguard virtual care protected health information.

An important virtual care risk area that cannot be overlooked is resilience. Like any web-based service, such as email, online banking or social media, virtual care services must be always available. Healthcare organizations need to understand the resilience capabilities of their virtual care systems and the performance record related to system availability, disaster recovery and business continuity.

Controls and processes specifically relevant to virtual care resiliency include:

1. Availability and reliability of applications, equipment and infrastructure (e.g., system audio and video need to be clear and uninterrupted for the provider and patient to have a successful encounter)
2. Patient service recovery, including call backs and charge refunds, resulting from system unavailability and dropped sessions
3. Adequacy of technical support, for times when assistance is needed to navigate the system or to troubleshoot a system problem

4. Change management controls to reduce the likelihood of system outages due to unplanned hardware or software changes
5. Adequacy of disaster recovery (DR) and business continuity (BC) plans, strategies and procedures, including guidance to ensure the integrity of backed-up or replicated data and the testing and revision of DR/BC procedures
6. Periodic assessment of potential threats, including:
   - Identification of potential disruption of system operations
   - Identification of critical processes and resources for reliable service delivery
   - Evaluation of equipment performance standards
   - Verification of system audio and visual performance quality

Conclusion

The risks discussed do not encompass all of the issues and concerns, nor are they entirely unique to virtual care. However, as an internal auditor, you should consider virtual care risks and controls differently from the traditional patient/physician single geographic location care delivery model. Virtual care services, technology and potential use opportunities continue to evolve. Healthcare internal audit professionals have an excellent opportunity to partner with management to identify unmitigated risks in virtual care solutions that are operational, as well as potential control gaps in virtual care projects that are not yet implemented. DI

James Kidwell is a Senior Information Systems Auditor for Carolinas HealthCare System. He designs and performs audits of information technology internal controls, HIPAA security program reviews and IT risk advisory consultations. James has extensive technical and management experience in higher education, telecommunications, and healthcare internal audit. You can contact him at (704) 512-4773 or James.Kidwell@carolinashealthcare.org.

Molly Murphy is a Senior Internal Auditor for Carolinas HealthCare System. She has over 15 years internal audit and consulting experience in retail, commercial real estate, manufacturing, insurance, and home health. She is the past President and Board Member of the Charlotte IIA Chapter and serves on the Association of Certified Fraud Examiners Advisory Council. You can contact her at (704) 512-4837 or Molly.Murphy@carolinashealthcare.org.