COSMOS
Navigate the Compliance Universe

Compliance Today - September 2023

Holly J. Hester (holly.hester@nethealth.com, linkedin.com/in/holly-hester-50554a116/) is Senior Director, Strategic Client Partnerships, at Net Health, Grand Rapids, MI.

Yolunda G. Dockett (ydockett@aadermatology.com, linkedin.com/in/yolunda-dockett-0073a56) is Chief Compliance Officer at Anne Arundel Dermatology, Linthicum Heights, MD.

Incorporating telehealth into your compliance work plan

by Holly J. Hester, PT, DPT, CHC, CHPC; and Yolunda G. Dockett, OTD, MOT, M.Jur., CHC, CHPC

The rapid expansion of telehealth during the COVID-19 pandemic has brought both opportunities and challenges to healthcare providers. Providers have been able to reach patients who were unable to obtain in-person treatment or services and expand the types of services offered. For providers new to telehealth, quickly ramping up a program meant finding a telehealth platform, educating both patients and staff on this new mode of treatment, implementing new processes and procedures, and delivering care in a brand-new way. From a compliance perspective, telehealth brings new risks and focus areas to the forefront, necessitating review and revision of an organization's compliance risk assessment and work plan.

Telehealth regulatory landscape

Telehealth uses electronic information and telecommunications technology to provide care when the patient and provider are not in the same location. There are two main types or categories of telehealth—*synchronous*, live, real-time interaction between the provider and the patient, and *asynchronous*, which involves acquiring data of some type and transmitting it to a provider at a convenient time for assessment offline. State law, licensure/certification requirements, and specific payer regulations must be reviewed before delivering telehealth or other virtual services.

Prior to the COVID-19 public health emergency (PHE), Medicare reimbursed for certain Part B physician and practitioner services provided via telehealth using interactive, two-way audio/video technology when the patient was in a physician's office, hospital, skilled nursing facility, or other specified facility location in a rural setting. The list of provider types who were able to provide and bill telehealth under the Medicare program was limited to only nine; it included physicians, physician assistants, nurse practitioners, clinical social workers, clinical psychologists, and a few others.

Very early in the PHE, the Centers for Medicare & Medicaid Services (CMS) quickly implemented several waivers and flexibilities that allowed Medicare beneficiaries in both rural and urban areas to receive services via telehealth while in their homes. In addition, CMS expanded both the list of covered telehealth services and the list of provider types who can provide and bill telehealth to include all providers eligible to bill the Medicare program to ensure access to all types of covered services for the duration of the PHE.

The Consolidated Appropriations Act of 2023 extended these flexibilities for telehealth services provided under the Medicare program through December 31, 2024.[1] What will happen after 2024 remains to be seen; however,

for the foreseeable future, telehealth will continue as a viable mode of service delivery and one that should be accounted for in an organization's compliance risk assessment and subsequent work plan.

Identifying risks associated with telehealth services

An effective compliance program must be based on the accurate identification and assessment of organizational-specific risks. Risk identification requires looking both internally and externally: What are the risks specific to the entity/organization (internal)? And what are the common industry risks (external)?

Internal risk identification

- Talk to clinicians delivering telehealth within your organization as well as individuals providing support (i.e., IT) or oversight (i.e., operations manager).
- Review internal audit and monitoring activities.
- Have you been audited or investigated by a payer or regulatory agency?
- What are your appeal findings?
- Consider patient satisfaction survey results for telehealth-specific feedback.
- Look at utilization trends. Have you noticed an increase in telehealth-related revenue under a particular payer? Do you have a specific clinician with a higher utilization when compared to company average?
- Identify external risks.
- Review U.S. Department of Health and Human Services Office of Inspector General Work Plan updates and audit reports to understand the agency's focus as it relates to telehealth.
- Stay abreast of applicable regulatory changes, survey guidance, and published targeted probe and educate trends.
- Assess recent enforcement trends, including civil monetary penalties, False Claims Act, and HIPAA violations.
- Track corporate integrity agreements and other settlement agreements applicable to your setting. These agreements can identify risk areas like overutilization, billing and coding, and even retaliation.
- Review headlines and publications specific to the organization's setting/line of business.

Risk classification

Once internal and external organizational risks are identified, they can be categorized or classified into risk areas. Examples of risk areas that apply to telehealth include licensure, practice act/state regulations, payer regulations, human resources (HR), quality of care and patient safety, HIPAA, documentation, and billing and coding. Within each of these general areas, specific risks should be called out on the organization's compliance risk assessment.

Know the licensure requirements and specific regulations for each state the organization does business in. Regulations can vary by discipline, provider type, venue, or practice setting. States and/or regulatory agencies often have differing expectations of supervisory relationships and may dictate specific parameters for delivering

telehealth services. If a nonphysician practitioner renders services, a board-approved, collaborative agreement must be in place for the states where services are delivered.

While some payers follow Medicare guidelines, that is not always the case. It is imperative to know and adhere to payer-specific rules associated with telehealth delivery to ensure compliance and accurate reimbursement.

Don't forget about HR-related risks, such as licensure verification and clinical credentialing. Each telehealth provider must maintain an active and unencumbered license in the states where their patients reside, and they must be credentialed with each payer.

Like in-person services, patient safety and quality of care risks exist with telehealth. Patient emergencies during treatment happen. Ensure policies and procedures are in place to manage in-person and virtual emergencies. Quality of care and positive clinical outcomes remains a top priority—even in telehealth. Not everyone is a candidate for telehealth. Understanding visit appropriateness and ensuring clinicians are qualified and competent to deliver telehealth is essential to providing quality care, patient satisfaction, and decreasing clinical risks.

When assessing HIPAA-related risks, there is an added risk of an impermissible disclosure if the provider's location and/or the patient's location isn't private when telehealth provides treatment. Also, consider security-related risks that exist when using technology to deliver care.

- Is the platform being used HIPAA compliant (a requirement now that the COVID-19 PHE has ended)?
- Will the technology vendor have access to patient data? If so, who specifically will have access?
- Where will the data be stored?
- Does the platform have end-to-end encryption?
- Is a business associate agreement in place?

Perhaps the most easily identified telehealth risks include documentation, and billing and coding. Medical necessity is always required and should be documented, and technical documentation requirements must be met. As with in-person services, ICD–10 and Current Procedural Terminology (CPT) coding must be accurate and supported by documentation in the medical record. In addition, telehealth claims must accurately reflect the appropriate place of service codes and/or modifiers as required by each specific payer. Also, remember that not only is general consent for services required, but you must also ensure specific consent for treatment via telehealth is documented for patients receiving these services.

Creating a telehealth risk mitigation plan

After risks have been ranked and prioritized based on type, likelihood, and impact, internal controls should be evaluated for effectiveness. This process detects gaps and establishes actionable items for your mitigation plan.

- Should a policy and procedure be developed to address telehealth-specific risks? Or are revisions to current policies required to incorporate telehealth?
- Is routine education and training appropriate? Should it be specific to a particular group (i.e., management versus clinicians/providers)? Who is your target audience?
- Is auditing necessary? Or is monitoring more realistic? Will someone "check the checker" (i.e., audit versus monitoring versus education)?

Use the seven elements of a compliance program as a guide when developing a risk mitigation plan.[2] Compliance professionals understand that even the best mitigation strategies result in some level of residual risk. Residual risk is the degree of risk that remains after all controls and mitigation activities are in place. When risk mitigation strategies are insufficient at reducing residual risk to an acceptable level, it indicates that additional measures are in order.

Developing an effective telehealth auditing and monitoring plan

Auditing and monitoring are key elements of all compliance work plans. Auditing is a formalized process that includes a targeted procedure that assesses a specific time period. An audit requires independence and objectivity and is designed to evaluate and improve effectiveness of processes. Audits require preplanning, a sample size, testing, and validation. On the other hand, monitoring is a less formalized approach to detecting areas that may require further scrutiny. Monitoring often includes ongoing procedures typically driven by management teams to validate that established processes are effective.

Specific auditing and monitoring activities should be incorporated into your current work plan to address and mitigate the identified risks associated with telehealth delivery. Simply adding an item or two to existing monitoring processes or slightly expanding the scope of the review may be sufficient to confirm the adequacy (or inadequacy) of the internal controls and ensure the provision of telehealth complies with the law, organizational policies, regulations, and clinical best practices.

- Monitor compliance with licensure and credentialing requirements, including verification that state law and scope of practice allow for telehealth delivery and that supervision requirements are met.
- Perform routine documentation reviews to ensure the medical record reflects medical necessity and supports the coding and billing of the services provided, including those delivered via telehealth. These periodic reviews should also incorporate technical requirements specific to telehealth, such as documentation of informed consent.
- Monitor compliance with payer-specific rules related to CPT coding, modifiers, and place of service codes by reviewing records from different payers and checking that payer policies are met in addition to coding and billing requirements that apply across the board.
- Review telehealth utilization trends, noting who is providing telehealth, to which patient populations, and for which services. Look for outliers and target deeper reviews and analysis as appropriate.
- Confirm evidence of provider training and competency for telehealth delivery, including the use of technology, emergency management, and clinical approach.
- Track and analyze patient satisfaction and grievances. This data gives insight into potential quality of care concerns, visit appropriateness, potential competency issues, and liability risks associated with telehealth.
- Ensure the platform being used to provide telehealth is HIPAA-compliant, and work with your IT team to perform initial and ongoing testing to confirm end-to-end encryption.

Final thoughts

The expansion of telehealth across provider types as both a service delivery model and a reimbursable treatment modality requires compliance professionals to incorporate telehealth into their compliance programs. Identifying, assessing, and prioritizing the risks associated with using technology to provide patient care directs the establishment of mitigation strategies and auditing/monitoring activities to ensure the safe and effective

delivery of telehealth.

Takeaways

- The rapid expansion of telehealth necessitates reviewing and revising of an organization's compliance risk assessment and work plan.
- Identify both internal (organization-specific) and external (industry-related) risks associated with telehealth.
- Categorize or classify telehealth-related risks and call out specific risks on your organization's compliance risk assessment.
- After risks have been ranked and prioritized based on type, likelihood, and impact, internal controls should be evaluated for effectiveness.
- Incorporate specific auditing and monitoring activities into your current compliance work plan to address and mitigate the identified telehealth-associated risks.

1 Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, §§ 4413 and 4151, 136 Stat. 4459 (2022), https://www.congress.gov/117/bills/hr2617/BILLS-117hr2617enr.pdf.
2 Health Care Fraud Prevention and Enforcement Action Team, Office of Inspector General, "The Seven Fundamental Elements of an Effective Compliance Program," accessed June 30, 2023. https://oig.hhs.gov/documents/provider-compliance-training/945/Compliance101tips508.pdf.