Telehealth Risks During COVID-19 and Beyond

Authors: Sarah A. Cole, CPA, Partner, Crowe
Kimberly R. Cusson, CCS, CPC, Crowe
Candice M. Moschell, CISSP, Crowe

Contents:

Expansion of telehealth increases risks

The COVID-19 pandemic has resulted in a remarkable expansion of telehealth services in hospitals and physician practices across the U.S., allowing patients to receive certain services from their home through a phone or video call. Expansion of services now allows providers to deliver care remotely to patients who may be high risk. The services expanded include office visits, mental health counseling, and preventive health screenings. As a result of the COVID-19 public health emergency, the Centers for Medicare & Medicaid Services issued policy changes related to telehealth, including temporarily expanding access to and coverage of telehealth services and easing certain restrictions.[1] Many private insurers followed suit.

An April 2020 McKinsey & Company survey found that 46% of consumers were using telehealth to replace in-person healthcare visits canceled due to the pandemic. This is a significant increase over 2019, when only 11% of patients used telehealth services.[2] The 2020 rapid rise of telehealth was a necessary solution to reduce care interruptions and keep patients safe from transmission of the coronavirus. However, signs indicate telehealth services will continue as a practical and even preferred form of care delivery beyond the duration of the pandemic. One survey found 76% of patients are interested in using telehealth services in the future.[3]

At the start of the COVID-19 pandemic, many healthcare organizations rushed to implement or significantly scale their telehealth programs to minimize care disruptions for their patients. With the pressure to quickly scale telehealth programs, organizations may have overlooked associated risks. As the demand for telehealth services increases, now is the time for healthcare provider organizations to ensure their telehealth programs, revenue cycle processes, and supporting technology are in place and compliant with applicable laws and regulations. Healthcare internal auditors play a vital role in this process, helping to protect the organization from lost revenue, exposure of patient information, and threats to the organization's assets, among other risks.

This white paper outlines some of the main risk areas associated with telehealth expansion in healthcare provider organizations and offers risk prevention strategies,

particularly in the areas of cybersecurity, coding and clinical documentation, billing, and denials.

Cybersecurity risks: Caution in an already threatening environment

The threat of cybersecurity attacks within the healthcare industry has risen steadily over the past few years. The Department of Health and Human Services (HHS) reported that an increase in cybersecurity breaches at healthcare provider organizations from February to May 2020 might have been due to the COVID-19 pandemic.[4] News reports of cyberattacks on healthcare facilities are stark reminders of this ever-present threat. For example, the September 2020 debilitating attack on one of the largest hospital chains in the U.S. compromised computer and phone systems at hundreds of its hospitals.[5]

Increased use of telehealth invites additional risk within telehealth platforms and their supporting technical infrastructures. In the rush to quickly implement or scale up their telehealth programs, organizations might have overlooked cybersecurity concerns. Organizations must ensure telehealth programs and supporting technology adhere to the *Health Insurance Portability and Accountability Act* (HIPAA) and are designed to protect patient information and the organization's assets.

Auditors should consider telehealth cybersecurity risks in three key areas: governance, application security (security of the telehealth platform), and infrastructure security.

Governance. A strong telehealth governance program is an essential asset to managing cybersecurity risk. To help mitigate risks, organizations should verify that proper oversight of telehealth programs is in place, including implementation and monitoring of related policies, procedures, and standards. In addition, organizations should integrate their telehealth governance programs with existing cybersecurity programs. Telehealth technologies will continue to evolve, but a strong governance program should address the ever-changing threat landscape surrounding telehealth security.

A strong telehealth governance program should include implementing:

- **Appropriate technology standards.** Questions auditors should ask:
    - Does the organization have adequately documented policies and procedures addressing technology standards of the telehealth platform?
    - Are controls in place to effectively monitor these standards for compliance and update the standards when necessary?
- **Security and privacy standards.** Questions auditors should ask:
    - Does the organization have documented telehealth security and privacy standards?
    - Has appropriate documentation been provided to clinicians and patients (for example, a telehealth acceptable use policy and privacy updates)?
- **An effective training program.** Questions auditors should ask:
    - Are effective educational programs in place to inform and support providers and other staff and improve their ability to use telehealth platforms?
    - Have staff been adequately trained to help patients with telehealth platforms and technology?

Application security (the telehealth platform). Misconfigurations of the telehealth platform and use of unapproved technologies are two of the greatest risks to telehealth security.

To minimize security risks, organizations should:

- **Assess the organization's documented telehealth program** to understand approved technologies and practices.
- **Interview telehealth program participants,** including providers, to identify processes followed and potential use of unapproved technologies or practices.
- **Identify key areas of improvement** that could benefit from additional training of staff.

- **Review application security controls**, verifying proper encryption, backup and retention, and user-access protocols.

Infrastructure security. Auditors should be aware of risks to the technological infrastructure supporting the telehealth platform. Internet-facing devices and devices internally connected to an organization's network (including computers and mobile devices such as tablets and smartphones), create vast and multipronged risk exposures.

Because telehealth platforms are supported by all the other technologies in place within an organization, inappropriate configurations could expose the organization to multiple points of entry, leading to security breaches.

To minimize risks related to infrastructure security, organizations should:

- **Analyze configuration settings** of telehealth technology platforms to assess potential security gaps, including how exposed the application is to the internet.
- **Assess supporting infrastructure,** including networking controls, email security, backup and retention controls, and endpoint security.
- **Verify technology implementation** has no vulnerabilities or misconfigurations.

Clinical documentation risks: Monitoring compliance

Internal auditors must assess whether healthcare organizations have the correct systems and processes in place to deliver telehealth services and accurately document, code, and bill for these services. In addition, processes must be in place to monitor updates related to telehealth service coding to ensure the organization remains in compliance with regulations.

A telehealth program should include:

- Establishing education programs and training nurses and physicians on documentation requirements for telehealth services
- Establishing ongoing monitoring processes to validate the effectiveness of the education provided

- Validating the central billing office is aware of payer-specific guidelines and is monitoring telehealth services to track and trend root cause analysis of denials
- Validating electronic medical record systems and billing forms have been updated with the new telehealth current procedural terminology (CPT) codes, place and service, and modifiers
- Evaluating state laws and licensing by capturing the location of the provider of services (at the time the services were rendered) and the location of the patient (for example, whether the patient or provider was out of the country or their state at the time of the service)
- Validating that documentation supports the services rendered for accurate adjudication of claims

Key risk areas related to clinical documentation include documentation gaps and incorrect CPT coding:

Clinical documentation gaps. Knowledge gaps might exist if providers and staff have not been trained properly on the documentation requirements for telehealth services. Documentation for telehealth services rendered might not clearly support the medical necessity of the services billed, resulting in missed reimbursement or overpayment.

To minimize risks related to telehealth clinical documentation, organizations should:

- **Provide staff training** on the importance of documentation that supports the most accurate clinical picture and the codes assigned for each telehealth visit. Documentation should include:
    - Verbal consent for the visit
    - Whether video or audio was used for the visit
    - Start and stop time, or total length of call
    - Why telehealth services were used
    - Which telehealth technology platform was used
    - Where both the provider and patient were located during the service

- **Monitor all quality assurance processes** to ensure they are working as intended.

- **Retain evidence of the time of service to meet the time-based provision** by documenting either the start and end time or total duration of the telehealth visit.
- **Perform clinical documentation improvement audits** to determine whether documentation supports correct coding.

Providers using incorrect CPT modifier and diagnosis codes for telehealth services.[6] Insurers vary in how they expect telehealth services to be coded and billed. Coding staff and providers may be unaware of the varying requirements, which might result in incorrect billing and claims denials.

To minimize risks related to incorrect CPT codes and modifiers, organizations should:

- **Provide continuing training for staff** in the areas of regulatory guidance, payer requirements, and proper coding of telehealth services.[7]
- **Educate staff and providers on COVID-19-related coding guidelines,** including specificity and proper sequencing of diagnoses. Provide continuing education on any changing guidelines and requirements as the pandemic unfolds.
- **Perform coding audits for COVID-19 and other patients** to validate correct coding as expected by payers.

Billing risks: Understanding diverse payer requirements

Throughout the pandemic, telehealth guidelines for each payer have been changing – often rapidly – making it difficult for providers to understand how each payer should be billed for telehealth services. Determining whether coinsurance or deductibles have been waived for patients using telehealth services might be particularly confusing. Organizations must understand payer guidelines and have clear, organized telehealth services billing plans to properly bill for services rendered.

To minimize risks related to telehealth billing, organizations should:

- **Create a matrix** that includes each insurer and outlines:
    - If telehealth services, e-visits, video, or telephone visits are accepted

    - Telehealth requirements for CPT codes, modifiers, and place of service along with effective dates
    - Important notes about coverage, including a list of plans for which telehealth policies apply
    - Whether cost sharing or coinsurance is waived
    - Requirements of how to capture telehealth services, including CPT codes, modifiers, and place of service as well as effective dates or changes to the guidance
- **Validate whether patients should receive bills** for coinsurance or cost sharing if these have not been waived by the patient's insurance company.
- **Validate reimbursement** to make sure the organization is getting paid as outlined for telehealth services.

Denials risks: Data analytics – a vital ally

With insurers continually changing or updating their policies for covering telehealth services, organizations should have controls in place to keep up with the changes. Problems can be exacerbated in organizations with limited staff due to COVID-19 related absences or staff members being temporarily assigned to work in other departments.

These challenges can result in claims denials, an unwelcome outcome in already financially challenging circumstances. Swiftly addressing causes of telehealth denials results in compliant billing and increased reimbursement. Data analytics can be an effective tool to reduce telehealth services claims denials.

To minimize risk of denials in telehealth billing, organizations should:

- **Use data analytics to confirm data integrity** and accurate mapping as well as to help the organization understand electronic medical record and third-party administrator configurations.
- **Analyze claims data** compared to the payer-specific matrix created by the billing team. Results of this analysis might indicate claims that need to be corrected and refiled as well as claims missing some of the telehealth

requirements. Performing this analysis on a periodic basis can assist with timely corrections and pinpoint needed process changes or additional oversight controls.

- **Create a dedicated team** of people trained in data analytics software to assist with telehealth services.
- **Use data analytics to assist with auditing telehealth denials** to validate whether they were billed appropriately to insurance companies as outlined in their policies for proper adjudication of claims.
- **Perform due diligence** and verify patients' coverage prior to telehealth visits.
- **Confirm if a referral is needed and** obtain any necessary referrals prior to the patient's visit.

Conclusion: Staying ahead of an evolving situation

Expansion of telehealth services with 1135 waiver was underway March 6, 2020.[8] This expansion has increased who can provide telehealth services to their patients, such as doctors, nurse practitioners, clinical psychologists, and licensed clinical social workers. Additionally, the HHS Office of Inspector General has provided flexibility for healthcare providers to reduce or waive cost sharing for telehealth visits paid by federal healthcare programs. Medicare considers these visits the same as in-person visits. However, it is important for providers to be cognizant of guidelines for each payer if they plan on providing telehealth services to their patients.

In addition, during the pandemic providers must seriously explore HIPAA compliance technology as HIPAA requirements will be enforced at some point in the future.

As the healthcare industry continues to navigate the COVID-19 pandemic, the duration and overall effects of this global crisis are unknown. Healthcare organizations will need to stay informed of rapidly changing circumstances, including continued regulatory changes and evolving clinical protocols that can affect cybersecurity, clinical, and revenue areas.

Healthcare provider organizations must monitor and understand changes necessary to identify and close technology and revenue cycle-related risk gaps.

Endnotes:

[1] "Telehealth: Delivering Care Safely During COVID-19," U.S. Department of Health and Human Services, https://www.hhs.gov/coronavirus/telehealth/index.html

[2] Oleg Bestsennyy, Greg Gilbert, Alex Harris, and Jennifer Rost, "Telehealth: A Quarter-Trillion-Dollar Post-COVID-19 Reality?" McKinsey & Company, May 29, 2020, https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality

[3] Ibid.

[4] Mallory Hackett, "Number of Cybersecurity Attacks Increases During COVID-19 Crisis," Healthcare Finance, June 4, 2020, https://www.healthcarefinancenews.com/news/number-cybersecurity-attacks-increase-during-covid-19-crisis

[5] Aaron Holmes, "More Than 250 Hospitals Across the US Have Been Debilitated by a Cyberattack That Forced Staff to Cancel Surgeries and Work With Pen and Paper," Business Insider, Sept. 29, 2020, https://www.businessinsider.com/uhs-cyberattack-hack-derails-surgeries-at-hospitals-across-us-2020-9

[6] "Medicare Telemedicine Health Care Provider Fact Sheet," CMS, March 17, 2020, https://www.cms.gov/newsroom/fact-sheets/medicare-telemedicine-health-care-provider-fact-sheet

[7] "Special Coding Advice During COVID-19 Public Health Emergency," American Medical Association, May 4, 2020, https://www.ama-assn.org/system/files/2020-05/covid-19-coding-advice.pdf

[8] AMA state directives to expand telemedicine, American Medical Association, accessed Nov. 16, 2020, https://www.ama-assn.org/system/files/2020-04/telemedicine-state-orders-directives-chart.pdf

About AHIA

The Association of Healthcare Internal Auditors (AHIA) is a network of experienced healthcare internal auditing professionals who come together to share tools, knowledge, and insight on how to assess and evaluate risk within a complex and dynamic healthcare environment. AHIA is an advocate for the profession, continuing to elevate and champion the strategic importance of healthcare internal auditors with executive management and the Board. If you have a stake in healthcare governance, risk management and internal controls, AHIA is your one-stop resource. Explore our website for more information. If you are not a member, please join our network, www.ahia.org. AHIA white papers provide healthcare internal audit practitioners with non-mandatory professional guidance on important topics. By providing healthcare specific information and education, white papers can help practitioners evaluate risks, develop priorities, and design audit approaches. It is meant to help readers understand an issue, solve a problem, or make a decision. AHIA welcomes papers aimed at beginner to expert level practitioners. This includes original content clearly related to healthcare internal auditing that does not promote commercial products or services.

Interested? Contact a member of the AHIA White Paper Subcommittee.

Subcommittee

Alan Henton, White Paper Chair
alan.p.henton@vumc.org

Mark Eddy
mark.eddy@hcahealthcare.com

Linda Greer
tlbmc@cox.net

Debi Weatherford
debi.weatherford@piedmont.org

Laura L. Sak-Castellano
Laura.Sak-Castellano@advocatehealth.com

Deborah Pazourek, AHIA Board Liaison
Deborah.L.Pazourek@medstar.net