COSMOS
Navigate the Compliance Universe

Compliance Today - May 2024

Melissa Andrews (melissa.andrews@clearwatersecurity.com, linkedin.com/in/melissa-andrews-086229103/) is a Principle Consultant, Privacy and Compliance at Clearwater Security in Whitehouse, TX.

The compliance officer’s challenge: Riding the technological wave in healthcare

by Melissa Andrews

I was cleaning out my research collection a couple months ago. One that caught my eye was an article about telehealth. This article was published in 2018, and the author’s perspective made me laugh. In the piece, the author discussed telehealth and how they did not believe it would ever catch on. They reasoned that it was not real healthcare, insurance would never pay for it, and patients would not want to talk to their providers over the phone because they wanted to see them face to face. Oh, how times have changed!

Telehealth and remote patient monitoring

Not only do some patients prefer telehealth visits to in-person visits, but telehealth has also given patients in rural areas access to medical care they previously did not have. Insurance companies have joined the bandwagon by taking advantage of the cheaper reimbursement rates and pushing telehealth use for better care coordination. While the COVID-19 pandemic was a big driver behind this push, I believe society’s increasing acceptance of technology-aided care should get most of the credit. As a compliance officer, I see technology changing healthcare right before my eyes, and I cannot be the only one having difficulty keeping up.

Regulators are also struggling to keep up with this rapid pace. Several guidance materials about the appropriate use of technology—specifically in healthcare—are being released from different government agencies. For example, members of the House of Representatives are asking the Centers for Medicare & Medicaid Services (CMS) to investigate the use of artificial intelligence (AI) in reducing claim denial rates.[1] This is a great idea, and the benefits are undeniable. However, a previous payer tried using AI in claims processing with a different result. UnitedHealth Group (UHG) is currently being sued by members stating that UHG used AI to make life-altering decisions about patient care. The lawsuit says that the algorithm used to determine eligibility had parameters that were too rigid and unrealistic causing many individuals to receive denial of care. According to court documents, 90% of these denials were overturned through appeals.

Technology is also being used in treating patients. While some merely use AI as a resource, others use AI to complete documentation and assist in making diagnoses. Wellness apps, heart monitors, and other devices are used by providers in real-time to make treatment decisions. This has proven to be lifesaving and cost-effective for patients; however, there are also many concerns, such as protecting patient’s data, securing devices against cyberattacks, documenting data from device applications in the patient’s medical record, and determining whether the use of the data from devices meets payer requirements for reimbursement.

CMS is trying to keep up with the technology used to replace in-person monitoring but can still fall short. If a specific evaluation and management or cardiac event detection monitoring code requires a hospital inpatient visit, then the provider cannot use data gathered—be it outpatient or telehealth—from an electronic device or AI without risking reimbursement at best and a fine at worst.[2] As previously mentioned, telehealth has become an excellent way for patients to receive cost-effective care if your facility can meet all the requirements. This includes meeting security and privacy requirements and all regulatory telehealth requirements, including prescribing practices for each visit.

Technology and electronic medical records

Another concept of technology we may have no control over is the electronic health record (EHR). We are dependent on our vendors to ensure they can deliver on the promises they have made. For example, in 2017, eClinicalWorks (ECW) settled False Claims Act allegations for $155 million and entered a corporate integrity agreement (CIA) when they allegedly misrepresented the capabilities of its software.[3] Specifically, ECW misrepresented its ability to accurately record user actions in an audit log, record diagnostic imaging, perform drug interaction checks, and retrieve appropriate drug codes. Although the enforcement action is seven years old, the impact is long-lasting and far-reaching. This incident is often referenced at conferences by compliance officers and staff. As a compliance officer, the EHR is a significant risk area, and as it involves more AI, it should be consistently monitored and audited by the compliance department. Because fraud, waste, and abuse are usually the number one risk in compliance, monitoring and auditing the EHR makes sense and ideally reduces the risk to your organization. It would be almost impossible for a compliance officer to review every patient's medical record to determine the impact this had on their health system.

Messaging applications technology is becoming the norm not only for quick communications but also for making business decisions. The U.S. Department of Justice released an updated *Evaluation of Corporate Compliance Programs* in March 2023 stating that "prosecutors should consider a corporation's policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications . . . and ensure that business-related electronic data and communications are accessible and amenable to preservation by the company."[4] Many organizations use applications like texting, GroupMe, Slack, and Teams Messenger for all types of business discussions. Compliance officers should evaluate whether conversations on these applications have been included in data retention policies and documented in the medical record.

Compliance and cyberattacks

While cyberattacks are, first and foremost, a security concern, they impact compliance. A ransomware attack does not mean you no longer have to follow required regulations. For example, the affected hospitals in the recent Ardent Health cyberattack had to divert emergency room patients, and the compliance officer considered whether there was compliance with the Emergency Medical Treatment & Labor Act was impacted. Additionally, in some cyberattacks, workforce members can no longer access the EHR system, which means they cannot document or pull medical history in the EHR. Compliance officers should evaluate how medical necessity determinations and other CMS requirements are met based on the patient's history in a paperless world and how compliance with other healthcare regulations, such as HIPAA and the information blocking rule (21st Century Cures Act), will be accomplished during this time. Compliance officers should engage clinicians and others within the organization to develop "downtime" procedures and provide training and education as appropriate.

Healthcare is becoming more dependent on technology. We use technology to determine how inpatients get their food, communicate with patients, for documentation in the medical record, make treatment decisions about patients, and for billing purposes. So, when I think about developing an effective compliance program for 2024, I know I will have to stay on top of technology and the ever-changing regulations that apply.

Conclusion

As a compliance officer, it is hard to determine where to start. The new U.S. Department of Health and Human Services Office of Inspector General's General (OIG) *Compliance Program Guidance* mentions technology several times.[5] In following this guidance, compliance officers should perform compliance risk assessments and review your organization's security risk assessment.

Here are some other recommendations for ensuring you don't get swept away in the wave of new healthcare technology:

1. Talk to your chief information officer and chief information security officer and become their best friends. Most technology that comes into your organization should go through them.
2. Consider data mapping and inventory to identify hardware, software, and applications used by your organization, how data flows throughout these systems, and categorize the types of data on these systems.
3. Meet with your chief medical officer, chief nursing officer, and other department leaders. With their help, review and update policies to address AI, ChaptGPT, digital health apps, and other technology.
4. Identify high-risk areas like billing and coding, medical decision making, documentation, prescribing practices, telehealth visits, digital health devices, and automatic data retention/destruction.
5. Remember to authenticate data by regularly auditing and monitoring. OIG has consistently enforced this compliance program element in CIAs.
6. Finally, know your resources, and don't be afraid to ask for help from an expert. Using an outside resource with fresh eyes can help identify areas of risk and help you prioritize those risks based on best practices and industry standards.

Takeaways

- Regulators and healthcare providers are struggling to keep up with the pace of innovation and demand for tech-enabled care delivery. As artificial intelligence (AI) takes center stage in the proliferation of new tools —from telehealth to charting and documentation to diagnosis and treatment plans—the use cases and the regulatory landscape around it grow more complicated.
- Security and privacy requirements are critical components of the regulatory requirements that accompany any technology adoption.
- The electronic medical record represents one of a covered entity's greatest risk areas, partly because it depends upon the honesty and transparency of the electronic health record (EHR) vendor and because the technology within the EHR continues to be involved at an increasing pace.
- Cyberattacks have compliance implications in addition to being a significant security concern. The downstream impact of a ransomware attack, for example, the diversion of patients from the emergency room, can put an organization at odds with regulations like the Emergency Medical Treatment & Labor Act.
- In today's age of interoperability and tech-dependent healthcare delivery, effective compliance programs depend on an organization's ability to stay on top of the changing technology trends and the changing regulations that result.

[1] American Hospital Association, "House letter on AI use in Medicare Advantage denials," November 6, 2023, https://www.aha.org/news/headline/2023-11-06-house-letter-ai-use-medicare-advantage-denials.
[2] Centers for Medicare & Medicare Services, "Chapter 3 – Verifying Potential Errors and Taking Corrective Actions," *Medicare Program Integrity Manual*, Pub. 100-08, Rev. 12056, May 25, 2023, https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/pim83c03.pdf.
[3] U.S. Department of Justice, Office of Public Affairs, "Electronic Health Records Vendor to Pay $155 Million to Settle False Claims Act Allegations," news release, May 31, 2017, https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations.
[4] U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, updated March 2023, https://www.justice.gov/criminal-fraud/page/file/937501/download.
[5] U.S. Department of Health and Human Services, Office of Inspector General, "Compliance Guidance," accessed February 26, 2024, https://oig.hhs.gov/compliance/compliance-guidance/.

This publication is only available to members. To view all documents, please log in or become a member.

Become a Member Login