SAI360
RISK FROM EVERY ANGLE

Healthcare Compliance in Changing Regulatory Landscape

Introduction

Before the onset of the coronavirus pandemic, forces at the federal level were in motion to transform the healthcare industry from a closed to a more open system. A nationwide public health emergency simply served as a catalyst driving digital transformation at a rapid clip. As evidenced by the quick shift to virtual care, the healthcare industry is more than capable of moving quickly when all forces are aligned in the same direction.

But rapid change also introduces the potential for risk. Virtual care allows patients new ways to access care. Still, it also opens the door for new forms of fraud, waste, and abuse, which federal authorities have shown a penchant for monitoring closely and prosecuting aggressively. While healthcare organizations have turned to third parties through outsourcing to service their patients and members, they must remain compliant with operating rules with costly consequences for non-compliance. And with federal officials pushing increased access and exchange of health data, covered entities and their business associates must ensure that their operations do not run afoul of HIPAA and health data security and privacy rules.

For healthcare organizations to avoid financial penalties, they require new resources to manage internal and external risks. Providers and payers must go above and beyond in terms of monitoring the work of their business partners to root out fraudulency and the downstream financial implications for their organizations. Doing so will allow these healthcare organizations to meet the requirements of federal rules and regulations while meeting the evolving expectations of consumers.

Understanding the Fraud Risks of Expanded Telehealth Use

While telehealth enabled the healthcare industry to remain open and accessible to patients during the pandemic, its widespread use, coupled with the relaxation of many restrictions, has made the modality ripe for abuse. Based on the federal government's history of aggressively investigating medical fraud and abuse, healthcare organizations that fail to remain compliant with telehealth regulation run the risk of exposing their practices to costly litigation and fines.

The utility of telehealth predates the public health emergency, but the latter spurred unprecedented growth in provider and patient adoption of the technology. During the first half of 2020, nearly one-third of all visits for commercially insured and Medicare Advantage enrollees occurred using telehealth — a 23-fold increase of the same period the prior year. What's more, the availability of telehealth services has resonated with consumers, with health plans reporting double-digit gains in overall member satisfaction as a result.

In other words, telehealth has become a staple of care delivery. However, the ubiquity of telehealth has also drawn the attention of bad actors and growing interest from federal agencies in the potential for telehealth fraud and abuse.

Last fall, the Department of Justice (DoJ) announced the largest healthcare fraud takedown in the agency's history: $6 billion in alleged fraud losses, $4.5 billion tied to telehealth. Government officials documented instances of telemedicine executives providing kickbacks to providers for unnecessary orders of durable medical equipment (DME), genetic and diagnostic testing, and pain medications. In Operation Rubber Stamp, DoJ alleged that one telehealth scheme alone had bilked Medicare for $1.5 billion in durable medical equipment. As a result, more than 250 providers saw their ability to bill Medicare revoked.

While telehealth is a recent phenomenon for many users, its association with healthcare fraud and abuse predates the pandemic. In August 2020, the owner of a Florida telemedicine company was charged with healthcare fraud, illegal kickbacks, and tax evasion stemming from allegedly fraudulent orders to durable medical suppliers that led to $784 million in Medicare claims. One year earlier, DoJ charged 35 healthcare professionals from telehealth and cancer genetic testing laboratories with healthcare fraud tied to $2.1 billion in Medicare claims between 2017 and 2019.

Given telehealth's growth over the past two years, federal investigators are likely to take action against bad actors.

"It is important that new policies and technologies with potential to improve care and enhance convenience achieve these goals and are not compromised by fraud, abuse, or misuse. OIG is conducting significant oversight work assessing telehealth services during the public health emergency," the acting head of the Officer of Inspector General Christi A. Grimm noted earlier this year.

With increased federal and state oversight an inevitability, healthcare organizations must educate their staff about the potential for telehealth fraud and abuse and put in place systems to prevent instances of noncompliance.

Legal experts from Troutman Pepper have identified four potential telehealth fraud schemes most likely to draw scrutiny from government officials.

Upcoding time and complexity

The Centers for Medicare & Medicaid Services will look closely at the amount of time providers claim to have spent delivering telehealth services to patients.

Misrepresentation of provided services

The number of virtual services now available to patients requires that providers fully understand the activities that qualify and the necessary procedures for coding and billing.

Services not rendered

The law firm warns that submitting claims for services providers have not rendered at all or effectively represents a "significant enforcement risk." Ineffective telehealth services could result from technical difficulties or obstacles in the way of a patient being able to benefit fully from their virtual visit.

Kickbacks

Federal authorities have made clear their interest in rooting out schemes wherein providers receive payments for orders of unnecessary durable medical equipment, diagnostic testing, or medications.

To avoid telehealth fraud and abuse, healthcare organizations must work with their staff and business partners to ensure compliance with federal and state law. Activities should include a number of essential activities:

- Policy management to respond to changing regulation and remediate gaps
- Third-party/vendor risk management to identify potential risks and manage contracts
- Incident management to improve incident reporting and investigation
- Revenue risk integrity to monitor claims and denials for financial exposure and trends

Telehealth is not going, nor is the interest of federal and state agencies into activities constitution healthcare fraud and abuse.

How Health Plans Must Prepare for Vendor Risk, Noncompliance

Managed care organizations, ranging from Medicare Advantage plans to accountable care organizations, must be prepared to comply with federal regulatory compliance that now extends to a growing body of business associates and other third-party organizations.

Beginning in October 2021, covered entities, which include qualified health plans as defined by the Department of Health & Human Services, must ensure that their business associates comply with new requirements of the HIPAA Privacy Rule as well as ongoing regulation pertaining to the coronavirus pandemic, namely continued telehealth enforcement discretion.

Compliance with these regulations is critical given the growing reliance of health plans on outsourcing. Market projections anticipate that business process outsourcing is set for dramatic growth over the next five years, rising globally from $264.4 billion in 2021 to $468.5 billion in 2026 across providers, payers, and the life sciences. More than 40 percent of that outsourcing spend — north of $155 billion — will be made by healthcare organizations in the United States. Almost $20 billion in 2026 will be earmarked by payers for claims management alone. As a result of COVID-19, the healthcare industry, including health plans, has encountered staffing shortages necessitating the increased use of outsourcing.

In light of this outsourcing, health plans contracted with the Centers for Medicare & Medicaid Services through the QHP program must comply with a provision to maintain compliance oversight of business associates, known in the Medicare Advantage space as first-tier, downstream, and related entities (FDRs) or on the Federally Facilitated Marketplace as delegated and downstream entities (DDEs).

Understanding the terms

To ensure compliance, it is essential for health plans to understand their responsibilities relatives to their business partners that provide a host of administrative functions (e.g., care management, claims processing, healthcare services, patient management, credentialing).

First tier entities are organizations that enter into a written agreement with Medicare Advantage Organizations (MAOs) or Part D plans to provide administrative or healthcare services to Medicare beneficiaries. One step down is the downstream entity, which enters into written agreements with either the MAO/Part D plan or first tier entities. Lastly, related entities through common ownership of control of the MAO or Part D plan are organizations that perform under contract or delegation management functions, furnish services to Medicare beneficiaries under verbal or written agreements, or "leases real property or sells materials to the MAO or Part D plan sponsor at a cost of more than $2,500 during a contract period."

The Federally Facilitated Marketplace has more simplified definitions relative to delegated and downstream entities. UPMC Health Plan provides a succinct explanation:

- **Delegated entity:** Any party, including an agent or broker, that enters into an agreement with a QHP issuer to provide administrative services or health care services to qualified individuals, qualified employers, or qualified employees and their dependents (45 CFR § 156.20).
- **Downstream entity:** Any party, including an agent or broker, that enters into an agreement with a delegated entity or with another downstream entity for purposes of providing administrative or health care services related to the agreement between the delegated entity and the QHP issuer. The term "downstream entity" is intended to reach the entity that directly provides administrative services or health care services to qualified individuals, qualified employers, or qualified employees and their dependents (45 CFR § 156.20).
- **Examples of functions performed by DDEs include (but are not limited to):** plan design, marketing, enrollment, customer service, claims administration, network development, benefit management, quality improvement.

Why it all matters

Simply put, FDRs and DDEs must comply with program requirements set by CMS through annual attestation.

Under the CMS Compliance Program, business associates must demonstrate adherence to the code of conduct within 90 days of hire or contracting. The program stipulates expectations for all employees to act ethically, appropriate mechanisms for reporting issues of noncompliance and potential fraud, waste, and abuse (FWA), and remedies for addressing and correcting these issues. As noted in the modifications to the HIPAA Privacy Rule, "all affected covered entities would need to adopt or change some policies and procedures and re-train some employees."

Federal officials have emphasized FWA over the past few years with major investigations and severe financial penalties, signaling the importance of this issue to health plans and business associates.

While CMS has provided FWA guidance to reduce the potential burden on FDRs and DDEs, health plans must do their due diligence to ensure that their business partners comply with relevant laws and regulations and maintain appropriate policies and procedures. Doing so requires that health plans manage third-party risk as a top priority.

Fortunately, health plans can leverage strategic partnerships with technology providers that specifically address vendor risk management. A comprehensive solution should be able to identify risks associated with specific vendors, track vendor progress in completing self-assessments, report a summary of known issues, viewing vendor responses to assessments, and review contract status, among others.

While federal officials have relaxed enforcement of HIPAA-related activities to ensure that the healthcare industry can address the coronavirus pandemic, they are more than willing to aggressively investigate bad actors looking to exploit federal programs and consumers. As a result, health plans must go above and beyond in terms of monitoring the work of their business partners to root out fraudulency and the downstream financial implications for their organizations.

Ensuring Healthcare Industry Compliance with HIPAA in 2021

As the healthcare industry has evolved to become increasingly digital, the Department of Health & Human Services and its departments have moved to bring the Health Insurance Portability and Accountability Act (HIPAA) into the modern age to support advancements in care coordination and improve patient access to their health information.

Beginning in 2021 and moving into the next few years, covered entities (both providers and payers) and business associates must enable both secure access and disclosures (i.e., sharing) of protected health information (PHI) to avoid financial penalties for noncompliance from HHS, namely the Office for Civil Rights.

To achieve and maintain HIPAA compliance today and into the future, providers, payers, and their business partners must remain aware of all the provisions necessary for them to comply with a host of mandates. For covered entities in particular, a strategic technology partner help identify potential risks in order to protect the organization from avoidable risks and public relations fallout resulting from HIPAA noncompliance.

First and foremost, HHS is set to finalize modifications to the HIPAA Privacy Rule aimed at removing barriers to coordinate care and individual engagement.

"These modifications address standards that may impede the transition to value-based health care by limiting or discouraging care coordination and case management communications among individuals and covered entities (including hospitals, physicians, and other health care providers, payors, and insurers) or posing other unnecessary burdens," agency states in the notice of proposed rulemaking issued earlier this year.

Chief among the proposed requirements are shortening the duration to respond to individual requests for PHI (from 30 to 15 days) and making this information available electronically as ePHI. Doing so also requires reducing identity verification on individuals wishing to access their private data and enabling individuals to direct the sharing of PHI among different organizations. Considering the healthcare industry's reliance on outsourcing, these changes represent a major wakeup call to covered entities and their business associates.

Additionally, covered entities will need to act in good faith when determining whether the use or disclosure of PHI is in the individual's best interest, especially in the interest of avoiding serious harm to the safety and well-being of the individual. Requesting an individual written acknowledgment of a provider's notice of privacy practices (NPPs) is no longer required.

Lastly, the Office of Inspector General (OIG) has the authority under the 21st Century Cures Act to investigate any claim of information blocking by a health IT developer, healthcare provider, or health information exchange (HIE) or network (HIN), as noted in the HIPAA Privacy Rule NPRM.

Also specific to HIPAA in 2021 and beyond is a new law enacted to incentivize security, known as the HIPAA Safe Harbor Bill. Made into law on January 5, the bill directs HHS to take into account a covered entity's or business associate's use of industry-standard security practices within 12 months when investigating and undertaking HIPAA enforcement actions or other regulatory purposes.

HHS and its subagencies have a strong track record of enforcing HIPAA rules and issuing substantial penalties for noncompliance. In 2020, OCR issued 19 fines, one of the most significant around a business associate's failure to conduct a security risk analysis. Following a health data breach of PHI of more than 6 million individuals, Community Health Systems agreed to a $2.3-million settlement with the federal government for "longstanding, systemic noncompliance with the HIPAA Security Rule."

The HIPAA-related requirements exist against a backdrop of numerous other mandates on providers, payers, and business partners. Considering that HIPAA ensures individuals have access to their PHI, these covered entities and business associates must:

- Enable patient access to PHI using the FHIR application programming interface
- Make publicly available provider directory information via APIs
- Participate in payer-to-payer exchange of patient clinical data
- Exchange specific enrollee data for dual eligibles
- Publicly attest not to be participating in information blocking
- Publish digital contact information
- Sharing admission, discharge, and transfer event notifications

Meanwhile, the industry must still contend with the potential ending of the telemedicine enforcement discretion (which federal officials have continued to extend to support the country's response to COVID-19) and ensure that their business partners are compliant with policies around potential fraud, waste, and abuse (FWA) — as detailed in a previous post.

Altogether, HIPAA compliance in 2021 is a tall order for covered entities and business associates. The former must hold their business partners accountable and work hard to mitigate potential risks by leverage technology partners and solutions to identify potential weak points. The latter must fall in line with federal rules and regulations or else face litigation and penalties.

To ensure successful compliance, covered entities and business associates must be in alignment to enable information to move securely from point A to point B to assist patients in their healthcare journeys.

Conclusion

Healthcare organizations from providers to payers must be prepared to comply with federal regulatory compliance that now extends beyond their traditional brick-and-mortar institutions to include a growing body of business associates and other third-party organizations. New forms of care delivery, namely telehealth, are changing how care is delivered and reimbursed, but this movement has not gone unnoticed by federal and state agencies monitoring activities deemed to be forms of healthcare fraud and abuse. Lastly, forthcoming changes to HIPAA will require covered entities to hold their business partners accountable and work hard to mitigate potential risks. By leveraging technology partners and solutions to identify potential weak points, healthcare organizations can ensure operations are compliant and capable of addressing new and emerging business challenges.