protiviti®
Global Business Consulting

Top Compliance Priorities for U.S. Healthcare Organisations in 2025

Featuring detailed insights for provider, payer and life sciences organisations

by Leyla Erkan, Managing Director, Global Healthcare Compliance Leader

Face the Future with Confidence®

Table of contents

Introduction

With a second Trump administration, Republican control of Congress and a conservative-leaning Supreme Court, the healthcare industry will likely see both deregulation and a reduction of the powers of the various healthcare-related agencies. We anticipate significant focus by the new administration on the following areas: drug pricing, Medicare and Medicaid, price transparency, data privacy and security, artificial intelligence (AI), and telehealth. Additionally, chief compliance officers (CCOs) will face the unique challenge of trying to motivate for compliance in the face of an administration focused on deregulation and reducing the burden associated with legal and regulatory adherence.

In this dynamic environment, the CCO plays a vital role in supporting the organisation's well-being. While there are indications of less federal regulatory oversight under the Trump administration, it's crucial to consider the possibility of increased audits aimed at recouping past funds or reimbursements, as well as regulatory oversight being pushed down to state governments. This decentralisation could lead to a patchwork of state-specific regulations, such as those regarding privacy, which might vary widely in terms of enforcement, requirements and oversight. States could be given more leeway to implement their own healthcare policies, which could result in new mandates, reporting requirements and compliance measures to which healthcare organisations must adapt. For CCOs and organisations, this dual shift – focusing on recouping funds through audits and dealing with potential new state-level regulations – means there must be an even greater emphasis on maintaining robust compliance programs. This is a unique opportunity for compliance departments to not just mitigate risk and safeguard against penalties, but also act as a driving force that helps healthcare organisations stay ahead of regulatory changes, protect revenue and position themselves as strategic advisors.

The 2024 reversal by the Supreme Court of the Chevron Doctrine will likely play a significant role in shaping healthcare policy under the new administration, with President Trump seeking to maximise executive authority to reduce the scope and power of federal agencies. Deference to courts and judicial decisions will slow down administrative actions, making it more difficult for agencies to issue broad healthcare regulations, especially in areas like the Affordable Care Act (ACA). This will lead to greater uncertainty and increased litigation within the industry, while requiring CCOs to navigate a more complex legal landscape.

Healthcare organisations and CCOs also need to consider the potential ramifications of tariffs imposed by the Trump administration. Tariffs could, for example, require medical devices and supplies to be procured from different nations or call for new locations to perform research, all of which could have compliance-related implications.

Further, momentum around compliance program effectiveness created by recent Department of Health & Human Services' Office of Inspector General (HHS-OIG) and Department of Justice (DOJ) guidance documents may wane. CCOs will likely need to act fast to capitalise on the leverage provided by the recent guidance publications, expediting efforts to secure their seats at the table and increase their access to organisational resources.

On a related note, in January this year, HHS published a Notice of Proposed Rulemaking (NPRM) which details significant enhancements to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Should these changes become final, they will have a considerable impact on regulated entities (we provide a rundown of this NPRM in the Appendix on page 40).

The implications of the United States withdrawing from the World Health Organisation (WHO) are yet to be seen but the impact could impair the United States' leverage and influence in shaping global health and trade policies. Implications could include increased trade barriers, regulatory divergence and conflicts with international standards. While the United States might retain the flexibility to establish its own regulations in areas such as pharmaceuticals and medical devices, it could face difficulties in accessing global markets that prioritise WHO-compliant products or standards.

Successfully navigating this sea change isn't just about understanding new regulations or changes to existing regulations; it's also about overcoming new staffing challenges within healthcare compliance departments. The industry is grappling with an aging workforce and compliance professionals are no exception. Experienced CCOs who are well-versed in regulatory requirements but less familiar with analytics and advanced technology are exiting the workforce, resulting in an unprecedented number of vacancies. In contrast, we're seeing an influx of young professionals, adept with digital tools but limited in their knowledge of complex regulations and internal politics.

In this changing landscape, CCOs and the boards and CEOs to whom they report will need to embrace change proactively to thrive in this dynamic legal and regulatory environment. The purpose of this guide is to assist U.S. industry players in identifying and addressing the most pressing compliance priorities. In this paper, we provide guidance on compliance priorities for providers, payers and life sciences organisations. Note that there are a number of compliance issues – for example, growth in emerging technologies, data security and privacy – that apply to all three types of organisations. In these cases, we have repeated them, as each priority has its own nuances pertaining to the different segments of the industry.

Protiviti
February 2025

Overview of industry compliance priorities

The provider, payer and life sciences segments each have unique compliance priorities while similarly trying to ensure, at their core, they achieve exceptional patient, consumer and member care along with high levels of satisfaction and employee retention.

Healthcare industry compliance priorities for 2025

Providers	Payers	Life Sciences
Management of emerging technologies	Medicare Advantage governance and compliance	Artificial intelligence
Privacy and data security	Risk adjustment	Privacy and data security
Quality and safety compliance	Fraud, waste and abuse	Marketing and advertising
Billing and coding compliance	Vendor and FDR management	Third-party relationships
	Privacy and data security	Anti-corruption

Please note that these priorities are not listed in order of importance.

Provider compliance priorities for 2025

Management of emerging technologies

Highlights

- **Promise of emerging technologies:** New technologies like AI, PowerApps and RPA offer significant improvements in patient care and operational efficiency.
- **Compliance risks and challenges:** These technologies also introduce complex regulatory challenges requiring attention to compliance and ethical standards. Compliance professionals need to broaden their knowledge bases to grasp fully the risks associated with emerging technologies.
- **AI's role in data management:** While AI has the potential to enhance preventive care strategies and streamline data collection, it also creates substantial risks in the areas of data privacy, security and patient consent.
- **Strategies for effective compliance:** Comprehensive risk assessments, policy development and cross-functional collaboration are among the keys to managing these technologies.

As the healthcare industry continues to evolve and integrate new technologies, providers face a multitude of new compliance risks. Emerging technologies – such as AI, telehealth platforms and wearable health devices – hold great promise for improving patient care, reducing costs and enhancing operational efficiency. However, they also introduce complex regulatory challenges that healthcare organisations must address to align with existing and developing regulations and ethical standards.

Compliance professionals need to broaden their knowledge bases to grasp fully the risks associated with emerging technologies. These technologies have the capability to revolutionise electronic medical record (EMR) systems and medical coding through various enhancements but will have compliance impacts:

- **Automated data entry:** AI algorithms can streamline the data input process by extracting relevant information from unstructured sources, such as physician notes and imaging reports. However, ensuring the accuracy and integrity of data as it is transferred from unstructured formats into structured databases is critical, as errors in data extraction can lead to misdiagnoses and incorrect patient records, affecting care and compliance. Data privacy (especially when utilising third-party AI systems) should be considered throughout the development lifecycle to verify compliance with data governance requirements.
- **Enhanced data analytics:** Tools such as PowerApps can leverage machine learning models and analyse extensive EMR datasets to uncover trends and patterns that may not otherwise be readily observable, facilitating more personalised patient care and proactive health management strategies. Compliance must be mindful of bias in AI models that can develop based on the data on which they are trained, leading to skewed outcomes that could impact patient care and violate non-discrimination laws. Outcomes from these systems need to be reviewed for trustworthiness and explainability to confirm organisational awareness and acceptance of key factors influencing the automated decision-making process.
- **Predictive analytics:** By analysing historical health data stored in EMRs, AI can predict patient risks and enhance team communication and coordination for efficient patient care, enabling clinicians to intervene earlier in disease progression. If patient data is being used for predictive analytics, proper notice should be provided to the patients about how their data may be used and, in some cases, authorisation or consent may be required if those activities do not fit squarely within healthcare operations as defined by HIPAA. Additionally, overreliance on AI predictions without adequate human oversight can lead to errors in clinical decision-making, raising quality and safety concerns.
- **Automated coding:** Utilising robotic process automation (RPA) or natural language processing (NLP), AI can automatically assign codes to patient encounters based on documentation, reducing human error and increasing coding speed. However, erroneous outputs can lead to noncompliance with billing, coding and reimbursement regulations.

- **Fraud detection:** Machine learning algorithms can identify anomalies in coding practices, potentially signalling fraud or abuse, thereby supporting compliance with regulations such as the False Claims Act (FCA). However, those organisations using data for fraud risk management must take steps to facilitate compliance with legal restrictions on data usage, ensuring that methods and practices adhere to regulatory guidelines.
- **Revenue cycle management optimisation:** AI-driven tools enhance the entire revenue cycle by facilitating accurate coding, which leads to appropriate reimbursement while minimising denials resulting from coding errors. However, integrating AI tools with existing financial systems must be performed in a manner that maintains data security and system integrity to avoid breaches and data loss.

Overall, while AI has the potential to enhance preventive care strategies and streamline data collection for health management, it also raises substantial concerns regarding data privacy, security and patient consent given the sensitive nature of health information. The stakeholders of AI and other emerging technologies should take these risks into account within the context of organisational goals and regulatory requirements to develop appropriate mitigating strategies.

To manage these risks effectively, compliance departments should:

- Conduct comprehensive risk assessments to identify potential compliance issues stemming from the adoption of emerging technologies.
- Engage in continuous policy development and revision, considering technological advancements and their implications for patient confidentiality and data integrity.
- Develop an understanding of existing and proposed regulatory requirements (e.g., European Union (EU) AI Act) and frameworks (e.g., National Institute of Standards and Technology (NIST) AI Risk Management Framework) to identify and assess gaps in organisational risk mitigation (e.g., U.S. DOJ Criminal Division Evaluation of Corporate Compliance Program Guidance).
- Implement robust cybersecurity measures tailored to protect against vulnerabilities introduced by new technological solutions.
- Develop transparency standards to help ensure algorithms used in AI-based decision support systems avoid biases that could impact patient outcomes.
- Foster cross-functional collaboration among IT professionals, legal experts, clinical staff and compliance personnel to facilitate comprehensive management of technological integration.
- Develop protocols for handling disputes or grievances related to AI decisions.
- Monitor and audit emerging technologies and processes continuously, including data handling practices, vendor compliance and performance of algorithms.

Privacy and data security

Highlights

- **Data protection priorities:** As data transforms patient care, its protection becomes increasingly vital.
- **Shifts in regulatory landscape:** The uncertain future of proposed HIPAA rules, the direction of regulatory enforcement and evolving state laws require attention from compliance officers.
- **Technological integration and compliance:** Navigating risks associated with AI and automation in healthcare requires comprehensive operational planning.
- **Privacy and security strategies:** Compliance should partner with key privacy and security personnel to help ensure periodic privacy and security program assessments are being conducted across all applicable assets and environments.

As data and advanced analytics become more integral to enhancing patient outcomes, the protection of that data remains paramount. With the growing adoption of more advanced tools and technologies (e.g., AI, automation, data analytics), it's crucial for CCOs and privacy officers to manage associated risks effectively, promoting and facilitating regulatory compliance and data protection.

The future of HIPAA regulations and enforcement in President Trump's second term remains uncertain. With new appointments for HHS secretary and the Office for Civil Rights (OCR) director, the trajectory for healthcare policies and HIPAA rules updates may change. However, because privacy regulations are not exclusive to the federal government, many states will continue to enact and maintain their own laws related to healthcare privacy, some of which are already more stringent than those at the federal level.

Among other developments that should be monitored:

- The recently finalised 42 CFR Part 2 Rules for Substance Use Disorder (SUD) records will require providers to make policy, procedure and process updates.
- President Trump's inclination toward deregulation may impact pending HIPAA Privacy Rule updates, particularly provisions aimed at strengthening reproductive healthcare privacy, which are currently being contested by the Texas attorney general. However, given the OCR's focus on cybersecurity initiatives during President Trump's first term, it's expected there will be continued efforts to enhance cybersecurity measures across healthcare.

- The findings in an audit report[1] released in November 2024 by HHS-OIG may result in heightened HIPAA enforcement by the OCR in 2025. The auditors found weaknesses within the OCR's audit procedures and emphasised the need for effective HIPAA enforcement in the face of increasing data breaches. The audit revealed that OCR's program supervision did not effectively enhance cybersecurity protection due to a limited assessment of security criteria and a lack of covered entity implementation of data safeguards like encryption, access controls and ransomware protection. HHS-OIG suggested that OCR should broaden its HIPAA audit scope and provide guidance on addressing compliance shortcomings of auditees.
- The HIPAA Security Rule NPRM was officially released on January 6, 2025, with a comment period open until March 7, 2025, and a proposed 180-day compliance timeline (see Appendix). The proposed updates significantly raise the bar for mandatory data security measures, with requirements like multi-factor authentication, network segmentation, and much more robust expectations around assessing the environment's controls on a specified annual or semi-annual basis, including penetration testing, vulnerability management, user access reviews, testing of backups and recovery capabilities, and more. What remains to be seen is whether these regulatory updates will stick and whether the timeline for compliance will also be enforced by the new HHS leadership.

As providers embrace cutting-edge technologies, it's imperative for compliance departments to initiate measures that manage the associated risks. But first, they must understand the implications of these technologies on data privacy and security, regulatory compliance and operational processes.

Providers are evolving their strategies to use data more effectively for patient care, engagement and health management. As these strategies are employed, providers must implement measures for ensuring data integrity and establish clear usage guidelines. The emergence of data commercialisation, continued focus on interoperability and technology advancements make these measures all the more vital.

As providers embrace cutting-edge technologies, it's imperative for compliance departments to initiate measures that manage the associated risks. But first, they must understand the implications of these technologies on data privacy and security, regulatory compliance, and operational processes. Compliance and privacy departments need to work closely with

[1] "The Office for Civil Rights Should Enhance Its HIPAA Audit Program to Enforce HIPAA Requirements and Improve the Protection of Electronic Protected Health Information," Department of Health and Human Services, Office of Inspector General, Office of Audit Services, Nov. 2024: https://oig.hhs.gov/documents/audit/10065/A-18-21-08014.pdf.

information technology, information security and operational teams to help ensure new technologies are implemented in a manner that adheres to regulatory standards, protects patient information and maintains the integrity of healthcare services. By taking such proactive steps, healthcare providers can leverage the benefits of new technologies while protecting the security and privacy of their patients' information.

Providers often struggle with effective data management and governance, leading to fragmented aggregation, maintenance and utilisation of data. Therefore, maintaining data integrity and usage guidelines is critical as providers deploy strategies to enhance patient care and engagement as well as to promote informed decision-making through better data use. Further, as organisations seek revenue from data commercialisation through partnerships, new privacy and security risks arise that must be managed accordingly. Providers should take a programmatic approach to data governance that includes aligning data strategies with organisational goals. This includes ensuring the quality control and secure management of data; facilitating policy compliance regarding data use, access and authorisation/consent; and deploying data analytics for continuous monitoring and targeted audit activities.

As mergers and acquisitions are expected to continue throughout the industry, it is important to realise the impacts on privacy compliance. Mergers and acquisitions often involve the consolidation of large volumes of sensitive patient data from multiple entities, which requires organisations to harmonise their privacy and security practices as well as their IT systems to address vulnerabilities and mitigate risk.

Large troves of healthcare data, whether they reside with the provider or their vendors, continue to be top targets for cyber and ransomware attacks, as evidenced by several massive, high-profile breaches in 2024. Attackers are taking advantage of healthcare providers' typically complex organisational structures and outdated technologies. These attacks carry significant consequences for provider organisations, including disruption of essential systems, revenue loss, regulatory scrutiny, reputational harm and compromised patient care.

Additionally, provider organisations frequently partner with third parties to outsource services, increase efficiency, control costs and provide other competitive advantages. However, with this comes the need to take measures to ensure third-party vendors maintain compliance not only with internal policies but also with the ever-evolving requirements of data privacy and security laws and regulations. For example, the proposed HIPAA Security Rule currently includes more rigorous requirements to which business associates must adhere, such as reporting to the covered entity the activation of its contingency plan within 48 hours, notification of any terminated individual whose access needs to be removed within 24 hours, and an annual reporting through a written certification that the organisation has deployed technical safeguards in line with the Security Rule. Furthermore, given the increased trend of offshoring certain operations, such as coding and/or information security, CCOs will need to be diligent in helping to ensure these partners are aware of and adhering to the new requirements.

Compliance officers should be partnering with key privacy and security personnel to ensure periodic privacy and security program assessments are being conducted across all applicable assets and environments, using established frameworks.

While third-party access to data is top of mind for many providers, it is equally important to manage access to data within the confines of the organisation. Managing user access effectively in complex healthcare settings is challenging, especially with diverse workforce roles across disparate systems and geographic locations. Handling access for non-employees adds complexity. It is crucial to assess the sufficiency of user-access management procedures, including the effectiveness of automated systems. Continuous monitoring is essential to maintain minimum necessary access for each role and user.

Compliance officers should be partnering with key privacy and security personnel to ensure periodic privacy and security program assessments are being conducted across all applicable assets and environments, using established frameworks – for example, from NIST, Center for Internet Security (CIS), Payment Card Industry (PCI), International Organisation for Standardisation (ISO), and OCR HIPAA Audit Program Protocols – while also understanding the associated risk management strategies for known risks.

Specific privacy and security program considerations that should be top of mind for all compliance and privacy officers include, but are not limited to:

- **Data governance:** Provider organisations should implement robust data classification and mapping processes to gain a comprehensive understanding of how data is used and disclosed throughout the organisation. This involves identifying different types of data, determining their relevance and sensitivity, and tracking their flow across various departments and functions. Providers should also establish effective identity and user access management controls. Additionally, compliance departments should develop and implement robust processes to monitor, track and communicate regulatory changes in order to facilitate compliance and minimise disruption to operations.
- **Third-party risk management:** Providers must implement risk mitigation strategies to help ensure that vendors, especially business associates with which the organisation

shares protected health information (PHI) and personally identifiable information (PII), do not compromise the organisation's compliance, privacy and security standards, or its operational integrity. This can be achieved through implementing a multidisciplinary third-party risk management governance structure that incorporates key stakeholders (e.g., Compliance/Privacy, Information Security, Legal, Risk, Procurement, Finance, etc.) from across the organisation. These risk mitigation processes should include regularly assessing and monitoring third-party relationships and related contracts to understand and address the changes in the organisation's risk landscape that come with the outsourcing of certain functions.

- **Data protection and incident response:** Implementing robust cloud security measures and conducting vulnerability assessments and penetration tests are important components for determining security weaknesses, but they represent only one aspect of comprehensive protection of PHI and sensitive data. Incident response readiness is another. Compliance and privacy officers should be prepared to respond quickly to potential threats that may compromise the privacy and security of PHI and other sensitive data maintained by the organisation.
- **Training and awareness:** Implementing comprehensive workforce education programs that raise awareness and provide role-specific training are critical to facilitating organisation wide adherence to compliance standards. This involves designing tailored educational materials that address the unique responsibilities and risks associated with different roles within the organisation. As the use of emerging technologies such as AI continues to proliferate, training programs should consider whether existing educational materials appropriately inform personnel about the unique risks presented by these systems.
- **Audit and monitoring:** Provider organisations should adhere to robust auditing and monitoring processes to validate ongoing compliance with data privacy and security standards. This includes conducting regular internal audits to review and assess adherence to policies and procedures and identifying any deficiencies or gaps in compliance. Also, organisations should implement continuous monitoring systems to track compliance activities in real-time, enabling prompt detection and response to potential issues. Regular reviews and adjustments are essential to adapt effectively to the dynamic regulatory and technological environment.

Quality and safety compliance

Highlights

- **Compliance risks and value-based outcomes:** Quality and patient safety are growing compliance risks for healthcare organisations, which often struggle with resource management, data management and practice standardisation.
- **Collaboration for better outcomes:** Compliance and quality programs must work together to improve care.
- **Data utilisation for safety:** Transforming data into actionable insights is a key to enhancing patient safety.
- **Health equity and SDoH:** Compliance should evaluate how effectively SDoH data is collected and used.

Quality and patient safety are increasingly viewed as compliance risks for healthcare provider organisations. Despite the many advances in technology and innovation in the delivery of services, the challenges associated with managing healthcare resources, data management and standardisation of practice continue to impact patient outcomes.

The HHS-OIG's latest guidance[2] recommends that entities better integrate oversight for quality control and patient safety into their compliance programs. That includes regular compliance reporting on quality controls and patient safety to the board. To facilitate Compliance's coverage of quality and patient safety risks, the OIG has issued a number of reports, toolkits and board guidance on quality of care. Adherence to clinical guidelines and quality standards is essential to providing safe and effective patient care while avoiding legal liability.

Further emphasising Compliance's role with quality and patient safety, the HHS-OIG's "Nursing Facility: Industry Segment-Specific Compliance Program Guidance"[3] focuses on the importance of improving the quality of care and safety of residents within nursing facilities. The OIG suggests there should be a collaboration of efforts between compliance and quality programs to monitor nursing facilities' compliance with laws and regulations that govern health and safety standards, resident care, and quality of life. These areas may extend beyond traditional compliance program oversight and require clinical or other specialised expertise and assessment.

[2] "General Compliance Program Guidance," U.S. Department of Health and Human Services, Office of Inspector General, Nov. 2023: https://oig.hhs.gov/documents/compliance-guidance/1135/HHS-OIG-GCPG-2023.pdf.

[3] "Nursing Facility: Industry Segment-Specific Compliance Program Guidance," U.S. Department of Health and Human Services, Office of Inspector General, Nov. 2024: https://oig.hhs.gov/documents/compliance/10038/nursing-facility-icpg.pdf. https://oig.hhs.gov/documents/compliance/10038/nursing-facility-icpg.pdf.

Although most healthcare organisations have access to a plethora of data, they are often described as data rich and information poor. Providers should focus on converting this data into information that can be used to improve access to services and the achievement of best practices. Underutilisation of data can hinder efforts to improve patient safety and reduce adverse patient outcomes.

Further, given guidance from the OIG suggesting that Compliance play a role in supporting quality and patient safety efforts, Compliance should integrate quality and patient safety considerations into their workplans. Just a few examples include:

- Patient safety monitoring
- Event reporting tracking and trending
- Quality improvement management
- Patient satisfaction
- Accreditation readiness
- Quality outcomes reporting

CMS's focus on health equity has emphasised that provider organisations need to document, code, collect and analyse Z codes associated with social determinants of health (SDoH).[4] These Z codes represent nonmedical conditions which impact a patient's ability to manage their health and any medical conditions. Compliance should play a role in evaluating the effectiveness of the organisation's efforts to collect and use SDoH data. However, if Trump's first term is to be any indication, SDoH may not be a priority for his second term.

Finally, collaboration between compliance and quality and patient safety team members is paramount to fostering a healthcare environment that prioritises patient well-being and adheres to regulatory standards. This partnership helps ensure that clinical guidelines are meticulously followed, adverse events are promptly addressed, and continuous improvements are made based on data-driven insights.

[4] "Comprehensive Error Rate Testing (CERT)," Centers for Medicare & Medicaid Services: www.cms.gov/data-research/monitoring-programs/improper-payment-measurement-programs/comprehensive-error-rate-testing-cert.

Billing and coding compliance

Highlights

- **Provider documentation practices:** Cloning documentation continues to be a significant source of compliance risk and can result in poor patient outcomes and billing noncompliance.
- **Substantiation of diagnoses:** Ensuring diagnoses are supported thoroughly in medical records helps prevent overpayments and compliance risks.
- **Documentation of medical necessity:** Thorough documentation is required to justify services billed, preventing billing errors and audits.
- **Preventing upcoding:** Comprehensive training and advanced technology can help mitigate the risks associated with upcoding and noncompliance.

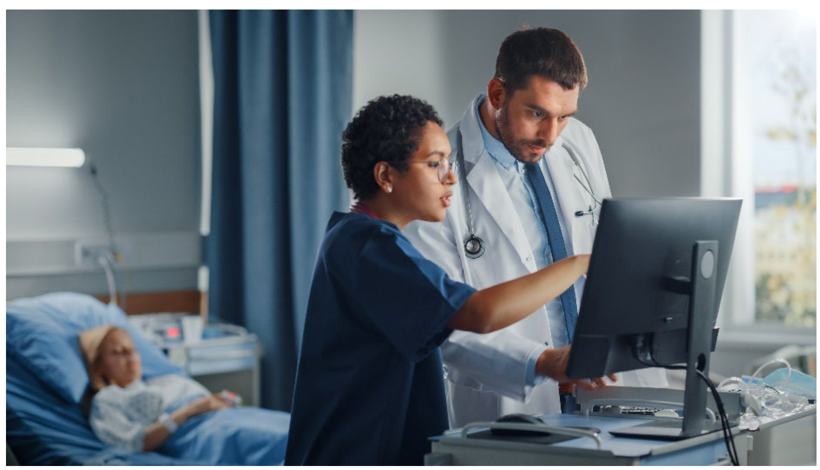
The importance of compliant clinical documentation and coding cannot be overstated due to the continued pressure on margins and the increasing sophistication of enforcement agency auditing capabilities. A few specific risks of which compliance personnel should be aware include:

- **Poor provider documentation practices:** If providers are not documenting accurately and in a timely manner, the organisation and its patients face a host of serious implications, including negative impacts to patient care, missed revenue and risk of noncompliance. One example of noncompliant provider documentation practices is cloning of the medical record. CMS defines cloned documentation as "multiple entries in a patient's health record that are exactly alike or similar to other entries in the same patient's health record or another patient's health record."[5] Inappropriate use of cloned documentation damages the integrity of the record of patient care. There are also reimbursement and legal implications.
- **Coding for diagnoses not sufficiently substantiated:** Coding of diagnoses that are not sufficiently supported in the medical record can result in significant overpayments by inflating the acuity of the patient, which can result in an incorrect diagnostic-related group (DRG) or inflating a patient's risk adjustment factor (RAF). The OIG and other enforcement entities frequently audit for specific diagnoses which may impact reimbursement in an inpatient setting. For example, coding for diagnoses like sepsis, respiratory failure or renal failure can result in a capture of a Major Complication Comorbidity (MCC), which can change the MS-DRG and may result in significantly more

[5] "Electronic Health Records Provider," Centers for Medicare & Medicaid Services: www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Downloads/docmatters-ehr-providerfactsheet.pdf.

reimbursement. During audits, government agencies will assess whether documentation supports the captured diagnosis code and, if not, could extrapolate error rates, resulting in multimillion-dollar recoupments. Compliance departments should determine whether these diagnoses are coded only when provider documentation and official guidelines for coding and reporting (OGCR) support capturing the condition. Note that governmental enforcement entities deploy sophisticated data analytics to target specific ICD-10 CM codes associated with frequently upcoded diagnoses.

- **Billing for services with insufficient documentation of medical necessity:** CMS maintains a lengthy list of medical necessity criteria – national coverage determinations (NCDs) and Medicare Administrative Contractor (MAC)-specific local coverage determinations (LCDs) – that need to be met and documented in order for services to be billed. The following are examples in which services are often billed without adequate evidence to support their medical necessity:
  - Imaging services without indicative symptoms
  - Unwarranted procedures
  - Physical therapy beyond normal recovery periods
  - Durable medical equipment

  Providers must maintain thorough records demonstrating why each service is medically necessary, based on clinical guidelines and individual patient assessment findings. Adequate documentation should include clear indications, relevant history, examination findings, test results if applicable, treatment plans outlining the rationale behind decision-making processes, informed consents where needed, and progress notes reflecting any changes in conditions substantiating continued intervention at specific levels of care.

- **Upcoding of services not furnished:** Upcoding distorts the true nature of the patient encounter, painting a picture of care more extensive and costly than what was delivered. Upcoding often occurs when the physician is responsible for most of the coding, such as in clinics, as physicians may not fully understand or focus on the coding guidelines governing Current Procedural Terminology (CPT) and/or Healthcare

Common Procedure Coding System (HCPCS) code assignment. This can be of particular concern for organisations implementing new technologies like automated coding. If the technology or underlying logic incorrectly captures a higher dollar CPT code (for example a higher-level Emergency Department Evaluation and Management (E/M) code), an organisation can go for long periods of time without realising a trend of upcoding, potentially resulting in a significant overpayment. CCOs should ensure that compliance workplans include auditing and monitoring for emerging technologies.

Noncompliant coding and billing practices not only trigger audits from insurance companies and government agencies but can also lead to hefty fines under the FCA, even if the provider did not intentionally misrepresent the level of service. Enforcement agencies like the OIG maintain a list of active audit topics that they investigate and utilise analytics to identify potential noncompliance. Examples of high-risk audit topics include mechanical ventilation more than 96 hours, rehabilitation services, telehealth, sepsis, trauma activation, level 4 and 5 hospital outpatient evaluation and management services, and skilled nursing facility therapy services. Severe cases can even result in criminal charges or exclusion from federal health programs. Beyond these direct consequences, such actions damage trust between healthcare providers and patients, insurers and regulatory bodies.

Through comprehensive training programs on proper documentation and coding procedures along with regular internal audits for quality assurance, providers can help prevent upcoding and its associated risks. Investing in advanced health information technology can also aid in reducing errors by providing decision-support tools that guide accurate coding, flag potential discrepancies for review and facilitate thorough electronic documentation. Finally, fostering a culture of compliance is crucial.

Payer compliance priorities for 2025

Medicare Advantage governance and compliance

Highlights

- **Regulatory changes under Trump administration:** Potential deregulation and expansion of MA benefits require new compliance oversight strategies.
- **Scaling compliance departments:** The need for effective compliance oversight grows as MA enrollment rises and regulatory requirements evolve.
- **CMS Interoperability Rule risks:** New requirements may be challenging for MA plans to implement due to system limitations.
- **PBM disclosure mandates:** Compliance with new prescription drug pricing transparency regulations is imperative.

Compliance officers should be on the lookout for regulatory shifts and policy changes that could present risk to Medicare Advantage (MA) organisations. The Trump administration's expected focus on deregulation could lead to modifications in the regulatory framework governing MA plans. The administration may continue to promote the expansion of MA benefits as seen in Trump's previous term and welcome innovative product offerings, which may require implementation of new oversight strategies. MA plans are already facing a broad spectrum of risks stemming from increased regulatory scrutiny, the myriad program requirements applicable to operational processes and the frequent release of new regulatory guidelines. Compliance officers should focus on the impact of the Trump administration on these areas.

Moreover, although over 50% of Medicare-eligible individuals[6] are now enrolled in MA plans, the scaling of compliance departments and roles dedicated to compliance oversight is not occurring at a commensurate rate, leading to greater compliance risk associated with lack of oversight. In addition, operational departments are frequently tasked with conducting many of their own regulatory monitoring activities. However, these departments often lack the necessary expertise to conduct effective compliance monitoring, which not only increases the risk of noncompliance but also places additional pressure on existing compliance personnel to bridge these gaps.

Although over 50% of Medicare-eligible individuals are now enrolled in MA plans, the scaling of compliance departments and roles dedicated to compliance oversight is not occurring at a commensurate rate, leading to greater compliance risk associated with lack of oversight.

Administering MA plan-directed care is complex and frequently results in inaccurate cost-sharing for members who have been referred to out-of-network providers by their primary care physicians or other in-network providers. As many MA plans increasingly rely on delegates for numerous services, there is an increased need for rigorous oversight of the delegated functions. Ensuring compliance with regulatory requirements and managing third-party risks effectively are paramount.

The CMS Interoperability and Prior Authorisation Final Rule was created to require the electronic exchange of healthcare data, streamline prior authorisation processes through application programming interfaces (APIs) and facilitate process improvements. The requirements of this rule will be phased in from January 1, 2026, to January 1, 2027. However, they pose substantial risks to payers as they necessitate advanced system and reporting capabilities that may not currently exist within many MA plans. In addition to this, the 2024 and 2025 Final Rules[7,8] limit the use of internal utilisation management (UM) coverage criteria and require public posting of those criteria as well as mandate creation of a UM committee

[6] Meredith Freed, Jeannie Fuglesten Biniek, Anthony Damico and Tricia Neuman, "Medicare Advantage in 2024: Enrollment Update and Key Trends," KFF, Aug. 8, 2024: www.kff.org/medicare/issue-brief/medicare-advantage-in-2024-enrollment-update-and-key-trends/.

[7] "2024 Medicare Advantage and Part D Final Rule (CMS-4201-F)," Centers for Medicare & Medicaid Services, Apr. 5, 2023: www.cms.gov/newsroom/fact-sheets/2024-medicare-advantage-and-part-d-final-rule-cms-4201-f.

[8] "Contract Year 2025 Medicare Advantage and Part D Final Rule (CMS-4205-F)," Centers for Medicare & Medicaid Services, Apr. 4, 2024: www.cms.gov/newsroom/fact-sheets/contract-year-2025-medicare-advantage-and-part-d-final-rule-cms-4205-f.

including health equity expertise, limit coordinated care plan prior authorisation use and ban prior authorisation requirements during the 90-day transition period when a member receiving active treatment changes MA plans. Many health plans are uncertain about how CMS will evaluate their UM procedures under these new requirements – particularly during a UM-focused audit or CMS program audit, given the limited data on the criteria used to perform these UM audits. Additionally, compliance departments often lack sufficient staffing or clinical resources to perform highly specialised UM auditing and monitoring effectively.

The Inflation Reduction Act introduced the Medicare Prescription Payment Plan (M3P). This innovative measure allows eligible members to make instalment payments for prescription drugs, rather than a single upfront copayment. While this policy change aims to ease financial burdens for members, it introduces substantial and multifaceted risks for MA plans as they adapt their operations to comply with these new regulations and facilitate member adherence to these payment schedules. New auditing and monitoring strategies must be developed to help ensure consistent compliance.

MA plans should ensure they are receiving comprehensive information regarding prescription drug costs and pricing that pharmacy benefit managers (PBMs) are now mandated to disclose. That information is ultimately shared with members to allow for informed decision-making regarding their prescription drug costs. Noncompliance with these disclosure requirements, as stipulated by the Consolidated Appropriations Act (CAA), poses significant risks for PBMs, especially as HHS conducts monitoring efforts to promote compliance. PBMs failing to adhere to these mandates, including meeting fiduciary obligations to act in the best interest of participants and beneficiaries of group health plans, may face regulatory actions including fines and other penalties.

Finally, HHS-OIG has reported that it will release new compliance program guidance tailored specifically to MA plans. The forthcoming guidance could influence changes to the current compliance program frameworks outlined in CMS's *Medicare Managed Care Manual* and *Prescription Drug Benefit Manual*, Chapters 12 and 9, respectively. Substantial revisions to existing compliance program guidance would likely significantly alter the landscape of compliance practices across the MA industry.

Risk adjustment

Highlights

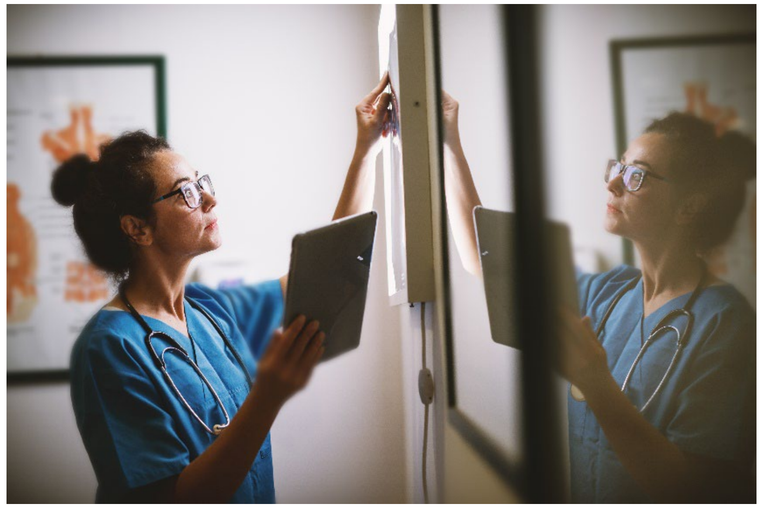
- **Importance of HCC capture:** Accurate HCC capture facilitates fair compensation and resource allocation for MA plans.
- **Recent settlements highlight compliance risks:** Multiple $150 million-plus settlements underscore the need for rigorous coding practices.
- **OIG's data analytics initiative:** Leveraging analytics tools to identify inappropriate HCC capture is crucial for compliance.
- **Comprehensive risk adjustment strategy:** Routine audits and oversight are essential to maintain compliance and avoid financial penalties.

Compliant risk adjustment processes and hierarchical condition category (HCC) capture are crucial for facilitating accurate and fair compensation in healthcare, particularly within MA plans. CMS utilises HCCs to adjust payments to MA plans based on members' health statuses, aiming to allocate resources appropriately for those with complex medical needs. However, submission of unsupported HCCs can lead to significant financial repercussions and legal and regulatory actions.

Recent cases underscore the importance of compliance, with several large healthcare systems each paying settlements of well over $150 million for violations under the FCA. These examples highlight the heightened scrutiny by the OIG and DOJ and emphasise the need for rigorous adherence to accurate coding practices in risk adjustment processes.

MA plans are plagued with risk adjustment issues, including lack of knowledge of risk adjustment regulatory requirements, the absence of a risk adjustment strategy at the organisation level, lack of personnel experienced in HCC coding and failure to identify HCC-related overpayments. Compliance plays a pivotal role in risk adjustment processes, helping to ensure that health plans accurately capture and report members' health statuses to secure appropriate reimbursement. Robust risk adjustment compliance strategies also enable organisations to identify and mitigate potential risks proactively, reducing the likelihood of costly penalties, legal actions and regulatory enforcement activities such as Corporate Integrity Agreements.

The OIG is making significant strides toward leveraging data analytics to identify instances of inappropriate HCC capture utilising a variety of sophisticated tools, such as predictive and geospatial analytics alongside AI technologies. Plans that fail to maintain compliant risk adjustment practices, including "looking both ways" in their coding reviews, are particularly at risk. The concept of looking both ways, or submitting additional HCCs that may not have been captured while deleting HCCs that are not supported within the provider's clinical documentation, is a key tactic for plans to help ensure compliant coding.



A comprehensive risk adjustment oversight strategy is essential for MA plans to maintain compliance and avoid significant financial penalties. A robust strategy should include routine internal audits utilising the comprehensive toolkit released by the OIG in December 2023 to review the appropriateness of diagnosis codes and the clinical support of those codes to identify and correct coding errors proactively, before they trigger regulatory investigations. Even smaller MA plans and other programs that leverage risk-adjustment processes, such as the Program for All-Inclusive Care for the Elderly (PACE), should prioritise effective risk adjustment oversight given the fact that OIG scrutiny is going beyond just the large insurers.

Fraud, waste and abuse

Highlights

- **Impact of FWA in healthcare:** FWA results in billions lost annually, increasing costs and premiums for payers and members.
- **Role of investigators:** SIUs lead FWA detection but face challenges due to a shortage of qualified professionals.
- **New opportunities for fraudsters:** Telehealth and other legislative changes present new risks that payers must address.
- **Strategies for fraud prevention:** Effective use of data analytics and metrics enhances oversight and distinguishes genuine FWA from errors.

Healthcare fraud, waste and abuse (FWA) results in billions of dollars lost annually, affecting members, providers, payers and the government. FWA creates unique problems for payers by generating unnecessary costs that can hinder the provision of adequate care and coverage and lead to higher-than-anticipated medical expenses and increased premiums. Various regulatory agencies, including the OIG, DOJ and Drug Enforcement Administration (DEA), play pivotal roles in combating healthcare fraud.

Special investigation units (SIUs) typically lead the FWA prevention and detection charge for payers but should collaborate closely with stakeholders such as provider relations, claims, payment integrity and legal teams. SIUs depend on seasoned investigators to detect and halt FWA activities. However, many are experiencing a shortage of certified professionals, such as Certified Fraud Examiners and Accredited Health Care Fraud Investigators. As a result, many payers are utilising inexperienced investigators, increasing the risk of fraudulent activities going undetected.

Telehealth expanded significantly during COVID-19 and presents significant FWA risk, particularly for audio-only consultations which are ripe for misrepresentation by members or providers and billing for services not rendered.

Fraudsters continually seek new opportunities to exploit, especially with the advent of new regulations. Telehealth expanded significantly during COVID-19 and presents significant FWA risk, particularly for audio-only consultations which are ripe for misrepresentation by members or providers and billing for services not rendered.

Legislation such as the M3P and the Cap Insulin Prices Act have the potential to foster black markets for drug diversion outside the United States or escalate identity theft to procure drugs. Insulin may become a particularly attractive target for bad actors due to the capped pricing, perceived high quality and consistent availability of U.S. insulin, coupled with the limited worldwide supply. Payers should ensure their PBMs and SIUs have a thorough understanding of regulations, both current and those that may be issued by the new administration, so that they can detect and mitigate associated FWA risks.

Payers need to ensure strategies are implemented aimed at identifying and preventing fraud both internally and at the delegate level, including timely monitoring of FWA risks and investigating reports of potential FWA. Compliance officers should enhance oversight by utilising key metrics and regularly reviewing these metrics for anomalies. Leveraging interactive dashboards and data analytics will aid in distinguishing between genuine FWA and erroneous data.

Vendor and FDR management

Highlights

- **Risks of vendor delegation:** Delegating responsibilities to vendors introduces privacy, security and compliance risks.
- **Complexity in oversight strategies:** Designing efficient delegation oversight is challenging due to diverse risk spectrums, including privacy, finance, operational and compliance.
- **Importance of pre-delegation review:** Involving Compliance in pre-delegation reviews ensures operational and regulatory readiness.
- **Adapting to regulatory changes:** Payers must ensure delegates understand and implement new regulations effectively.

Delegation of responsibilities to vendors and related entities, including First Tier, Downstream and Related Entities (FDRs), introduces a multitude of risks. These organisations undertake various aspects of a payer's operations, from member-centric activities such as claims handling, utilisation management and credentialing to administrative tasks such as data storage and distribution of correspondence. Despite the inherent risks, delegation continues to be a prevalent strategy for achieving operational efficiency and cost reduction, particularly in times of economic volatility. These risks are underscored by recent data breach incidents at third parties that resulted in significant reputational damage, exposure of sensitive medical information, and the inability to process claims or payments.

The risk spectrum associated with delegated operations encompasses privacy, security, IT, finance, operational and compliance risks. This diversity adds layers of complexity to the design and implementation of an efficient delegate oversight strategy. The challenge is further compounded by limited compliance resources for conducting delegate-specific sample reviews or delegation oversight teams that lack expertise in the operational areas they are tasked to oversee. Additionally, payer-delegate contracts often fail to include sufficient audit rights, or there may be a lack of internal coordination to facilitate effective auditing within the contractual parameters.

Additional risk arises when healthcare plans, seeking to distribute risk through value-based arrangements and other operational delegations, engage with inexperienced vendors. Delegating responsibilities to vendors lacking the requisite knowledge, operational processes or technology can result in substantial member impact, reputational risk, and legal/regulatory compliance risk. Compliance officers need to ensure they are consulted during the pre-delegation review and contracting processes, thereby facilitating an opportunity to exercise appropriate oversight when entering into a delegation arrangement. Implementing a thorough pre-delegation review involving subject-matter experts across all impacted areas is a critical step. It should be complemented by an audit strategy, initiated immediately upon delegate go-live, to assess compliance with contract terms and regulatory requirements, as well as operational capabilities.

Regulatory changes pose specific risks for healthcare payers using delegates, as these entities might lack the infrastructure or knowledge to comply properly with applicable regulations. They may also lack robust compliance testing. Thus, payers should develop a strategy to communicate their interpretations of new regulations and how they apply to their delegates. It's equally important to perform oversight and auditing to confirm that the regulations are being implemented correctly.

Privacy and data security

Highlights

- **Embracing advanced technologies:** The rapid pace of technological change requires taking proactive steps to stay updated on emerging trends and associated risks in order to leverage the benefits of new technologies while ensuring privacy and care quality.
- **Data governance challenges:** Organisations continue to grapple with effective data management and governance, with an increasing focus on data commercialisation and interoperability.
- **Continuous improvement in data privacy and security:** Regular risk assessments and updated policies protect member information.
- **Proactive management of cyber threats:** Collaboration among compliance, IT and security teams is essential for managing data privacy and security amid regulatory changes.

The volume and complexity of data leveraged by healthcare organisations continue to grow exponentially to drive better health outcomes for members. As big data drives more innovation, its protection continues to be paramount. Embracing advanced technologies like generative AI, the "Internet of Things," robotic process automation and machine learning that leverage big data is crucial for maintaining privacy standards and enhancing care quality.

Organisations continue to grapple with effective data management and governance, with an increasing focus on data commercialisation and interoperability. As a result, payers need to take proactive measures to maximise the advantages of new technologies while ensuring the security and privacy of member data. Effective data governance and robust risk management practices are essential to maintain compliance and protect sensitive patient and member information.

Payers can protect members' PHI and PII by implementing a multifaceted, continuous improvement approach to data privacy and security. This includes conducting regular risk assessments to identify potential vulnerabilities and implementing strong access controls to ensure that only authorised personnel can access sensitive data. Compliance, security and privacy officers should regularly review and update policies and procedures based on the latest regulations, industry best practices, and findings from internal audits and assessments. Regular training sessions for workforce members and delegates on data privacy and security policies and the handling of PHI and PII securely can significantly reduce the risk of incidents and breaches caused by human error. Additionally, payers should have a clear and tested incident response plan to address any data breaches or security incidents quickly. It's also essential to monitor third-party vendors that have access to PHI and PII to help ensure they comply with applicable regulations such as HIPAA and state privacy and confidentiality laws, while having adequate security measures in place. The proposed HIPAA Security Rule would require all regulated entities to notify other regulated entities within 24 hours of any individual whose authorisation to access ePHI or relevant systems is changed or terminated. The proposed rule also requires business associates to verify at least once every 12 months through a written certification that they have deployed technical safeguards required by the Security Rule (see Appendix for further details).

Effective data governance and robust risk management practices are critical to maintain compliance and protect sensitive member information. The rapid pace of technological change necessitates continuous updates to data strategies and close collaboration among compliance, IT and security teams. Additionally, as the industry faces ongoing regulatory and legislative changes, organisations must stay proactive in managing data privacy and security, especially with increasing threats from cyberattacks and the complexities of third-party relationships.

Life sciences compliance priorities for 2025

Artificial intelligence

Highlights

- **AI opportunities in life sciences:** AI accelerates innovation and can improve patient care quality but introduces new risks.
- **Addressing bias and fairness:** Using diverse datasets and unbiased AI models is necessary to prevent skewed outcomes.
- **Transparency and explainability in AI:** Interpretable models and detailed documentation are vital for regulatory compliance.
- **Cybersecurity and privacy concerns:** Robust frameworks are essential to protect sensitive data processed by AI models.

AI presents tremendous opportunities for the life sciences segment – accelerating innovation, enhancing efficiencies and improving the quality of patient care. However, it also introduces significant risks that exacerbate the need for regulatory alignment, the preservation of operational and data integrity, and patient safety assurance efforts. Compliance functions must identify, manage and mitigate emerging risks throughout the AI lifecycle as these technologies become more prevalent within organisations' operations. Beyond the deployment process, individual applications of AI technology should also be subject to risk assessment and the identification of mitigation strategies in alignment with the determined risk level. Existing and proposed regulatory requirements such as the EU AI Act and risk management frameworks such NIST's for AI should be considered during the development of organisational AI risk management frameworks to support appropriate risk coverage.

The use of AI in operational processes introduces risks associated with bias and fairness. AI models are only as good as the data on which they are trained. Data sets containing historical inequities or unrepresentative samples may create new or perpetuate existing biases. Any compromise in data accuracy, consistency and reliability can lead to flawed research outcomes, regulatory scrutiny and patient harm. For instance, algorithms used in clinical trials that favour specific demographic groups may yield skewed results when applied to broader populations.

Regulatory bodies will continue to scrutinise AI models to verify that AI-driven decisions do not discriminate against any group based on race, gender, age or other characteristics. Compliance functions must help ensure that mitigation strategies for bias and fairness-related risks are deployed by management. This may include regular auditing to verify the use of diverse datasets that represent all relevant demographics. Similarly, the results of any automated decision-making models need to be audited to probe for biased outcomes. Further, be mindful of any potential push for selective reporting or bias in the interpretation of data, which would undermine the integrity of the research and potentially put patient safety at risk.

Regulatory bodies will continue to scrutinise AI models to verify that AI-driven decisions do not discriminate against any group based on race, gender, age or other characteristics. Compliance functions must help ensure that mitigation strategies for bias and fairness-related risks are deployed by management.

Other risks to monitor include the transparency and explainability of AI models. Regulators expect organisations to be able to explain and validate the decision-making logic embedded in AI models. Researchers need to understand the factors that an AI model deems significant and how it reaches its conclusions, as these AI models are used to predict the structure of drug candidates, analyse genetic information and simulate their effects. Black-box models can present challenges in drug discovery use cases. However, those challenges can be overcome by, when possible, favouring interpretable models over complex black-box algorithms, maintaining detailed documentation of model development and decision-making processes, and utilising tools designed to increase model interpretability without sacrificing performance.

Prioritising cybersecurity and privacy is essential for AI functions. AI models in healthcare often process large volumes of sensitive patient and clinical data, making them attractive targets for cyberattacks. Compliance officers must help ensure robust cybersecurity frameworks are integrated into AI deployments and that AI vendors adhere to data protection standards.

The repeal of the Biden administration's executive order on AI could result in a reduction in regulatory oversight but can also introduce additional risks. Absence of robust AI safety programs would likely increase the risks associated with using AI in clinical trials, drug formulation or patient data analysis. Compliance teams can address these challenges by taking a principles-based approach, establishing their own standards to facilitate ethical and safe AI practices, and striving for transparency and accountability to maintain public trust.

Notwithstanding the approach the Trump administration elects to take, life sciences and pharmaceutical companies will have to comply with other requirements, such as the EU AI Act, in the jurisdictions in which they operate.

Compliance officers play an important role in the AI journey by providing the necessary oversight as well as the audit and regulatory expertise required to navigate these complex landscapes successfully. Through collaboration between technical teams developing AI solutions and the compliance function's oversight, life sciences organisations can continue their innovative AI practices without compromising compliance with regulatory obligations or ethical standards.

Privacy and data security

Highlights

- **Complex privacy landscape:** Life sciences organisations must navigate varying state and international privacy laws.
- **Medical device security challenges:** Compliance with FDA cybersecurity rules is crucial for device manufacturers.
- **Data governance and risk management:** Organisations need to establish robust data governance frameworks and manage third-party risks.
- **International privacy developments:** Updates to the GDPR and EU AI Act influence global data protection strategies.

Life sciences organisations continue to grapple with a complex privacy landscape. Because some organisations do not meet the definition of a covered entity or do business with covered entities, they are not always subject to the stringent federal privacy protections that HIPAA rules mandate. This leaves life sciences companies navigating a patchwork of state and international privacy laws. While we saw enforcement by the Federal Trade Commission (FTC) ramp up during the Biden administration, what will happen during President Trump's second term remains uncertain. The trajectory for healthcare policy and enforcement within the United

States will depend on key changes made by the Trump administration, such as whether the new FTC director will continue to pursue actions against healthcare organisations related to protecting and securing the personal and sensitive health information of consumers. Additionally, the future of the American Privacy Rights Act of 2024 (APRA) is unclear.

In the absence of a comprehensive federal privacy law, life sciences organisations must navigate an intricate web of state regulations that change frequently and vary widely. This decentralised approach creates significant compliance challenges for companies operating across multiple states. Several states, including Delaware, Iowa, New Jersey, New Hampshire and Tennessee, have enacted new privacy laws that take effect in 2025. These laws introduce stringent requirements for entities that control or process personal data, particularly focusing on enhancing consumer rights and regulating the sale of such data. Additionally, many of these new laws promote transparency by mandating that companies provide clear and concise privacy notices to consumers. These notices must detail how their data is collected, used, shared and protected, while also informing individuals of their right to access, correct and delete their personal data. As a result, companies operating in these states will need to implement robust data protection measures to comply with these new requirements.

Additionally, medical device security continues to be a concern due to the increased connectivity of these devices and their integral role in patient care. Food and Drug Administration (FDA) rules (e.g., Section 524B of the FD&C Act) around medical device security pose specific challenges for companies manufacturing Level III medical devices. As of October 1, 2023, device manufacturers are required to include detailed cybersecurity information that addresses cybersecurity requirements – such as identifying and protecting against threats, detecting cybersecurity events, responding to incidents, and recovering from breaches – in their premarket submissions. The FDA has the authority to refuse to accept any submissions that fail to contain proper cybersecurity controls and has exercised this new authority over the past year.

While it's essential to have robust security measures in place, they should not hinder the operational efficiency of devices. The goal is to ensure the devices are secure and, at the same time, easy to use for healthcare providers.

While these rules aim to facilitate robust cybersecurity throughout the device's lifecycle, they pose significant challenges for manufacturers due to the critical nature of these devices, which have higher-risk profiles and are often life-sustaining or supporting. Balancing security with operational efficiency continues to be a challenge. While it's essential to have robust security measures in place, they should not hinder the operational efficiency of devices. The goal is to ensure the devices are secure and, at the same time, easy to use for healthcare providers. Therefore, it is crucial for manufacturers to have a comprehensive understanding of where their devices are, how they are being used and how they are connected to other systems. Compliance can assist front-line stakeholders navigate the complexities of FDA regulations by working with regulatory affairs and legal departments to provide interpretations of the new FDA rules, helping organisations understand the specific cybersecurity requirements for their medical devices, and conducting thorough risk assessments to identify and mitigate potential cybersecurity vulnerabilities throughout the device's lifecycle. Further, Compliance can aid in preparing comprehensive premarket submissions to the FDA that include all required cybersecurity information.

To strengthen national security, the DOJ issued a comprehensive final rule on December 27, 2024,[9] implementing President Biden's executive order[10] aimed at preventing foreign access to sensitive data. The rule establishes a new program to prevent access to Americans' sensitive personal data by adversarial nations such as Russia, Iran and China. As a result, the final rule prohibits the sale of six categories of sensitive personal data relating to U.S. persons to covered entities or persons with ties to six countries of concern. The DOJ seeks to strike a balance between inhibiting necessary research and promoting national security by considering some exemptions for healthcare entities; however, some data restrictions will continue to impact life sciences organisations.

The DOJ seeks to strike a balance between inhibiting necessary research and promoting national security by considering some exemptions for healthcare entities; however, some data restrictions will continue to impact life sciences organisations.

Life sciences organisations often work globally, sharing data across borders for research and development purposes. This final rule could limit the ability to share large volumes of sensitive personal data with entities in the countries of concern. Additionally, the final rule could affect partnerships and collaborations with entities in the countries of concern. While the final rule does not prohibit U.S. entities from conducting medical, scientific or other research in these countries, or from partnering or collaborating to share data for research purposes, it does stipulate that these activities cannot involve the exchange of payment or other considerations as part of a covered data transaction. Therefore, this measure would require life sciences organisations engaged in genetic research or managing substantial patient data volumes to revise their international data exchange and research collaboration protocols. This move by the DOJ underscores the importance of data privacy and national security concerns, highlighting the need for robust data protection measures that extend beyond traditional privacy

[9] "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons," A Rule by the Justice Department, Federal Register, Jan. 8, 2025: www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern.

[10] "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," Executive Order 14117, Federal Register, Feb. 28, 2024: www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

considerations. Compliance and privacy officers should familiarise themselves with the nuances of the final rule and understand potential operational impacts.

Notable international privacy developments in 2024 included updates to the General Data Protection Regulation (GDPR). The GDPR changes underscore the EU's dedication to advancing data protection and privacy standards by ensuring that they remain robust and adaptive in an evolving digital landscape. Among the updates, the reforms introduce stricter penalties for noncompliance and expand the scope of regulatory enforcement. Also, new guidelines were established for AI systems to facilitate compliance with GDPR principles.

In addition, the European Data Protection Board (EDPB) adopted a new work program to address emerging data protection challenges. The update provides clearer guidelines for businesses and enhances the efficiency of cross-border cooperation between EU member states' data protection authorities. This is particularly important for multinational companies that process data across multiple EU countries and need to navigate the complex regulatory environment.

Most organisations will need to update their compliance practices to align with these new requirements. Compliance and privacy officers must prioritise several core considerations to address and mitigate the risks associated with storing and using the sensitive health information of patients and consumers. Additionally, they should work with key business stakeholders to adopt data privacy and security strategies to promote compliance with myriad applicable laws and regulations. Some considerations should include:

- **Effective data governance:** Companies must establish strong data governance frameworks, appoint data protection officers, and conduct regular data protection impact assessments and other proactive auditing and monitoring activities while maintaining accurate and complete records of data processing activities. This involves collaborating with stakeholders to create a framework that fosters data accuracy, privacy and security throughout the data's lifecycle. This can be achieved through implementation of data management policies and procedures, adherence to contractual and regulatory obligations, and the use of technology for safeguarding sensitive information. Additionally, effective data governance necessitates defining clear roles and responsibilities for data stewardship, maintaining data quality, and facilitating reliable data analytics for research and development initiatives.

- **Third-party risk management:** Third-party risk management is critical due to the frequent outsourcing of research, clinical trials, medical devices data analysis, etc. Regular assessments and mitigation strategies are essential to help ensure these external services do not jeopardise compliance with regulatory standards, contractual requirements, and the security and integrity of sensitive data.

- **Data protection and incident response:** To protect sensitive health and research data, organisations must have robust security measures in place. This includes secure cloud storage solutions enhanced with strong encryption protocols for both data at rest and in transit, as well as sophisticated identity and access management systems to restrict data access to authorised personnel only. Compliance should ensure vulnerability assessments, penetration tests and security audits are performed regularly to safeguard against emerging threats. Comprehensive cloud security and compliance with industry-specific regulations must be maintained. Additionally, organisations should have a clearly defined incident response plan to handle data breaches or security incidents quickly and effectively. Finally, emphasising data minimisation practices by collecting only the data necessary for specific purposes and limiting its usage and retention helps maintain data privacy and reduce risk exposure.

Marketing and advertising

Highlights

- **FDA's new draft guidance:** New FDA guidance provides direction on how companies can voluntarily and compliantly address third-party misinformation.
- **DOJ's continued enforcement:** The FCA remains a key tool in the fight against misleading advertising practices.
- **Changes in pharma advertising rules:** New FDA regulations for television and radio ads emphasise clear communication of drug risks.
- **Potential ban on television ads:** The Trump administration's consideration of banning pharma television ads could significantly impact the industry.

The U.S. federal government has strict rules governing marketing and advertising for prescription drugs and medical devices in the interest of public safety and health. In July 2024, the FDA released new draft guidance, "Addressing Misinformation About Medical Devices and Prescription Drugs: Questions and Answers."[11] The guidance provides direction on how companies can voluntarily and compliantly address third-party misinformation on the internet about their products. Any advertising should be approved by the compliance, legal, medical and regulatory departments (including the promotional review committee, where applicable) to help ensure it meets advertising rules, which may vary by country.

[11] "Addressing Misinformation About Medical Devices and Prescription Drugs: Questions and Answers," U.S. Food and Drug Administration, July 2024: www.fda.gov/regulatory-information/search-fda-guidance-documents/addressing-misinformation-about-medical-devices-and-prescription-drugs-questions-and-answers.

The DOJ has not abandoned its tried-and-true enforcement tactics and continues to use the FCA as its primary tool for fighting false and misleading advertising by life sciences companies that result in payments by government programs. The DOJ initiated a staggering 500 new FCA cases in 2023, the highest number of cases brought since the FCA was strengthened through multiple amendments in 1987. For example, in 2022, a multinational life sciences organisation and its related entities agreed to pay $40 million to resolve alleged violations of the FCA reported by a whistleblower in connection with off-label marketing, downplaying safety risks and making comparisons of efficacy without head-to-head data.

The FDA has made significant changes to how pharma ads are handled on television and radio. These changes became effective in May 2024.[12] Every prescription drug ad must clearly show and explain the drug's risks, such as potential side effects.[13] This information can no longer be rushed through or quickly flashed on the screen at the end of the ad. The goal is to help ensure that people watching the ad understand the drug's risks. The new rules require that the "major statement," which outlines the key risks of a drug, be presented simultaneously in audio and text. The FDA requires that the risk information be presented in language that ordinary consumers can easily understand. The volume, clarity and pacing of the audio that presents the risks must also be on par with the rest of the advertisement. On-screen text "must be formatted such that the information can be read easily,"[14] with clear contrast between the text and background. The text must also remain on screen long enough for people to read and process it. Finally, music or visuals cannot overshadow the importance of the conveyed risk information.

Finally, the Trump administration may go a step further. Robert F. Kennedy Jr., named by President Trump as his appointee to lead the Department of Health and Human Services, has advocated for banning pharmaceutical advertising on television. Currently, only the United States and New Zealand allow direct-to-consumer prescription drug advertising. The results of a 2022 survey published by Statista[15] revealed that pharma advertising spending in the United States amounted to an average of $1 billion monthly.

[12] Matthew S. Borman, "Direct-to-Consumer Prescription Drug Advertisements: Presentation of the Major Statement in a Clear, Conspicuous, and Neutral Manner in Advertisements in Television and Radio Format," page 80959, Federal Register, Food and Drug Administration, Department of Health and Human Services, Nov. 21, 2023: www.govinfo.gov/content/pkg/FR-2023-11-21/pdf/2023-25428.pdf.

[13] Ibid.

[14] Ibid.

[15] Julia Faria, "Pharma and healthcare industry advertising in the U.S. - statistics & facts," Statista, Dec. 18, 2023: www.statista.com/topics/8415/pharma-and-healthcare-industry-advertising-in-the-us/#topicOverview.

Third-party relationships

Highlights

- **Importance of third-party management:** Effective management of third-party relationships is critical for mitigating risks and safeguarding trust.
- **Navigating anti-kickback laws:** Understanding AKS requirements is essential to avoid legal penalties and maintain compliance.
- **Notable settlements in 2024:** Recent AKS and FCA settlements highlight the importance of robust compliance policies.
- **Building a culture of compliance:** Encouraging ethical behavior and reporting of violations helps prevent conflicts of interest.

Life sciences company relationships with third parties continue to be a focus of government scrutiny. As noted by the HHS-OIG in its "General Compliance Program Guidance" and "Compliance Program Guidance for Pharmaceutical Manufacturers," effective management of third-party relationships is essential for mitigating legal and reputational risks, safeguarding patient trust, and upholding organisational integrity.[16,17]

Navigating third-party relationships necessitates a nuanced understanding of regulatory requirements, particularly the Anti-Kickback Statute (AKS). The AKS prohibits transactions intended to induce or reward referrals for services or products paid by federal healthcare programs. Inducements create conflicts of interest, which can compromise decision-making. The relationships between healthcare professionals and life sciences organisations are critical for the advancement of medicine; however, compliance officers must help ensure that all provider arrangements, particularly those involving relationships with physicians, fall into AKS "safe harbours" and possess adequate safeguards. Failure to do so can lead to criminal charges, large civil fines and exclusion from federal programs.[18]

There were several notable AKS and FCA settlements in 2024, including a medical device manufacturer that agreed to pay close to $13 million to resolve allegations of violating the FCA by paying kickbacks. There was also enforcement against a pharmaceutical company that agreed to pay close to $50 million to resolve allegations that it offered kickbacks to induce prescriptions for one of its drugs.

[16] "OIG Compliance Program Guidance for Pharmaceutical Manufacturers," U.S. Department of Health & Human Services, May 5, 2023: www.hhs.gov/guidance/document/oig-compliance-program-guidance-pharmaceutical-manufacturers.

[17] "General Compliance Program Guidance," U.S. Department of Health and Human Services.

[18] John D. W. Partridge, Jonathan M. Phillips, Katlin McKelvie and James L. Zelenay Jr., "False Claims Act Enforcement in the Life Sciences & Health Care Sectors," Gibson Dunn, Nov. 7, 2024: www.gibsondunn.com/wp-content/uploads/2024/11/WebcastSlides-False-Claims-Act-Enforcement-in-the-Life-Sciences-and-Health-Care-Sectors-7-NOV-2024.pdf.

To mitigate FCA and AKS compliance risks, HHS-OIG advises that compliance officers implement robust policies mandating disclosure of potential conflicts, supplemented by regular employee training on conflict identification and management.[19,20] Life sciences companies must establish clear guidelines for permissible interactions with healthcare providers, including limits on gifts and entertainment and provisions directing that any compensation provided be for legitimate services at fair market value. Compliance officers should also implement management plans and monitoring systems to detect and manage potential conflicts, including factors or influences that could distort or bias the way care is provided, medications are prescribed or study results are interpreted. Finally, it is important that compliance programs foster a culture of compliance and ethical behaviour, which will encourage employees to report potential AKS violations without fear of retaliation.

Kennedy, President Trump's nominee for secretary of HHS, has expressed a strong stance against conflicts of interest. According to *AP News*, "Kennedy wants to prevent NIH from funding researchers with financial conflicts of interest, citing a 2019 ProPublica investigation that found more than 8,000 federally funded health researchers reported significant conflicts such as taking equity stakes in biotech companies or licensing patents to drugmakers."[21] Consequently, we anticipate the Trump administration will continue enforcement efforts to prevent kickbacks and conflicts of interest in life sciences research. Compliance programs should continue prioritising AKS and FCA compliance and implementing both strategic and tactical mitigation efforts to help safeguard their organisations from noncompliance.

19 "Policy Statement Regarding Gifts of Nominal Value To Medicare and Medicaid Beneficiaries," U.S. Department of Health & Human Services, Dec. 7, 2016: www.hhs.gov/guidance/document/policy-statement-regarding-gifts-nominal-value-medicare-and-medicaid-beneficiaries.

20 "General Compliance Program Guidance," U.S. Department of Health and Human Services.

21 Amanda Seitz, Matthew Perrone and Jonel Aleccia, "Here's how Robert F. Kennedy Jr. has promised to remake the nation's top health agencies," AP News, Nov. 15, 2024: https://apnews.com/article/robert-r-kennedy-rfk-vaccines-hhs-food-trump-0500f67ef53ed6862583dace587b3899.

Anti-corruption

Highlights

- **Significance of the FCPA:** The Act plays a crucial role in preventing bribery and promoting ethical practices in global markets.
- **Anticipated changes under Trump administration:** Expected shifts in FCPA enforcement may affect how companies navigate international markets.
- **Managing third-party risks:** Identifying high-risk activities related to third parties is essential for maintaining compliance.
- **Navigating new trade compliance risks:** Companies must be vigilant of emerging patterns in diversion and circumvention of regulations.

The Foreign Corrupt Practices Act (FCPA) has long been a crucial piece of legislation for global healthcare companies operating in international markets. The Act, which aims to prevent the bribery of foreign officials and promote ethical business practices, has significant implications for life sciences organisations, which often must navigate complex regulatory environments across different countries.

Under the Trump administration, the FCPA enforcement landscape may undergo changes. Historically, FCPA enforcement has varied significantly among administrations. The incoming administration's focus is expected to be on reviving economic growth and limiting the size of the federal government as well as the volume and complexity of business regulations, while at the same time pursuing aggressive trade and immigration policies. These developments will come with increased trade compliance risks. Identification of high-risk activities related to third parties is as critical as ever, since utilisation of new third parties and/or overreliance on existing ones will be inevitable for companies that wish to continue selling in existing markets. Companies may be exposed to higher third-party risks, as new patterns of diversion and circumvention of sanctions and trade regulations may emerge.

In closing

In the dynamic landscape of healthcare compliance, organisations stand at the forefront of a new era marked by innovation and regulatory transformation. It is incumbent upon compliance officers, management and staff members to navigate this complex terrain with foresight and diligence. Providers, payers and life sciences organisations must refine their strategies to align with requirements and enforcement, as well as with the advancement of emerging technologies. By fostering a culture of compliance that permeates every level of operation, healthcare organisations can help ensure the delivery of high-quality services and goods while safeguarding the trust and well-being of their patients, members, consumers and stakeholders. In this journey, proactive risk management and comprehensive education, spearheaded by Compliance, are the cornerstones that will enable healthcare organisations to not only comply with current mandates but also to adapt to future regulatory changes with resilience and the utmost integrity.

Appendix: Long-awaited HIPAA Security Rule revamp formally proposed with significant changes

Kevin Dunnahoo
Director – Security and Privacy

Kathy Murray
Associate Director – Security and Privacy

This article was originally published on Protiviti's Technology Insights blog.

The U.S. Department of Health and Human Services (HHS) published a Notice of Proposed Rulemaking (NPRM) related to the HIPAA Security Rule, which went live on January 6, 2025, followed by a 60-day open comment period. The potential changes are the most significant to the HIPAA Security Rule in over a decade. The NPRM details some significant enhancements that covered entities and business associates, collectively "regulated entities," should be aware of to begin evaluating how those enhancements may impact the organisation and how best to address them if they become final.

Some of the most significant impacts include:

- **All security specifications are required**: There will no longer be a distinction between required or addressable.
- **Definition changes:** There are 22 definition changes that cast a wider net of what regulated entities will need to consider when implementing and deploying tools and/or protocols aiming to enhance the clarity of the expectations set forth in the regulation. An example of a definition change is the term "technology assets," which will encompass all the components of electronic information systems and not focus only on certain components.
- **Formal documentation:** All Security Rule policies, procedures, plans and analyses will be expected to be formally documented, whether in paper and/or electronic form. Furthermore, it may be required that all documentation be reviewed and updated at least every 12 months.
- **Testing implemented security safeguards:** Regulated entities will be required to perform testing of some safeguards on a 12-month basis, while others may have more frequent testing. Below are examples of the frequency of testing being proposed:

- Penetration testing – at least every 12 months
- Vulnerability scanning – at least every six months
- Incident response plan testing – at least every 12 months
- Data backup and recovery testing – at least every 6 months
- Contingency plan testing – at least every 12 months
- Compliance audits – at least every 12 months

- **Technology asset inventory and network map:** Regulated entities will be required to document, review and update the inventory of all technology assets and not just those that create, receive, maintain or transmit electronic protected health information (ePHI). In addition to the inventory, data flow diagrams and network diagrams will need to be documented and reviewed at least every 12 months.
- **Elevated expectations of technical controls:** Technical controls that are considered best practice will now become requirements, which include but are not limited to the following:
    - Multi-factor authentication (MFA)
    - Encryption of ePHI in transit and at rest
    - Network segmentation
- **Expanded notification requirements:** New expectations and timelines for notifying other regulated entities of events that may impact them so they can assess and respond accordingly would include:
    - Workforce security access changes or terminations: Notifications to other regulated entities are expected to be as soon as possible but no later than 24 hours after the workforce members' authorisation of access is changed or terminated.
    - Contingency plan activation within a business associate agreement (BAA): A business associate would be required to report to a covered entity that they activated their contingency plan without unreasonable delay, but no later than 24 hours after activation.
- **More specificity to achieve compliance:** Details such as frequencies and/or expectations are provided for some specifications to assist regulated entities in meeting compliance. Examples include:
    - Data backups – Entities must ensure that copies of ePHI maintained are no more than 48 hours older than the ePHI maintained in the relevant electronic information system.

- Patch implementation – Critical patches are expected to be applied within 15 calendar days and high-risk patches are expected to be applied within 30 calendar days.
- Security awareness training – New workforce members are expected to complete security awareness training within 30 days after the first access to the entity's electronic information systems and training must be provided every 12 months thereafter.
- Information system activity review – Deploy tools that provide the regulated entity real time audit logging and monitoring of any activity that could present a risk to ePHI.
- Unique identifiers – Similar to unique identifiers for user accounts, all technology assets will be required to have a unique identifier.
- Group health plans – Plan sponsors will be required to report to group health plans if they activated their contingency plan no later than 24 hours after activation.
- Healthcare clearing houses – Entities with clearing house activities will be required to isolate such activities and establish written procedures specific to the clearing house activities.

Recommended next steps

We recommend that regulated entities, while not yet required to comply with these changes, review what elements are needed in case these changes make it to a final rule, while also considering how to address:

- **Evidence:** Ensure proper evidence is available to support the organisation's compliance with these requirements, which should include the effort to comply, along with results and how the results are being addressed.
- **Exceptions:** For specifications that are now required and have established exception protocols, regulated entities may need to consider how to align their exception process to adhere to these proposed definitions.
- **Roadmap:** Even if some of these changes and their details are not accepted within the final rule, regulated entities may fare better during an investigation if they consider leveraging the NPRM as a roadmap of HHS's expectations in achieving compliance. This will demonstrate to HHS investigators the regulated entity's culture of compliance and commitment to security best practices.

Chip Wolford, Daniel Stone and Juli Ochs also contributed to this post.

About Protiviti's Healthcare Industry Practice

At Protiviti, we know healthcare. Our global reach continues to expand at a rapid pace as we serve leading healthcare organisations amid accelerating change. We know the industry changes that are imminent and their drivers. And we know how to advise our clients to effectively address industry changes to best manage, protect and create substantial value. Our team of experienced professionals and our Healthcare Center of Excellence are your resources for understanding and managing the multitude of changes and risks affecting healthcare. Whether your organisation's chief concern is payment reform, regulatory compliance, revenue growth, cost management, cybersecurity or technology modernisation, Protiviti is here for you.

About the author

Leyla Erkan
Managing Director, Global Healthcare Compliance Leader

Leyla is Protiviti's Global Healthcare Compliance Practice Leader. She brings over 25 years of expertise in compliance and risk management, including a distinguished career as a Chief Compliance, Privacy and Research Officer. Leyla has deep expertise in regulatory compliance, clinical research, privacy, conflicts of interest, investigations and government audits, offering a comprehensive understanding of and practical approach to complex compliance challenges. She can be reached at leyla.erkan@protiviti.com.