Top Seven Regulatory and Enforcement Themes in Health Care for 2024

2024 is shaping up to be a very active year for regulatory and enforcement developments in the healthcare industry – developments that concern not just hospitals and nursing facilities, but many non-healthcare companies as well, including technology companies, that engage in business practices that directly create compliance risk for the industry.

Among the top new regulatory and enforcement initiatives that either have already entered force or will be forthcoming in 2024 include:

- New healthcare-specific cybersecurity requirements
- Higher penalties for violations of the Health Insurance Portability and Accountability Act (HIPAA)
- New policy initiatives to scrutinize healthcare-related anticompetitive practices
- Enhanced oversight of private equity (PE) firms' ownership structures
- New regulations addressing the use of artificial intelligence in health care

In short, 2024 promises to be an especially busy year for chief compliance officers, chief risk officers, and their counsel across many sectors and subsectors of the healthcare industry.

With these regulatory and enforcement developments, the U.S. Department of Health and Human Services (HHS) will not be the only agency enhancing its oversight over HIPAA violations and non-compliant patient health and safety practices, generally. Other federal agencies focusing on the healthcare industry will be the Antitrust Division of the U.S. Department of Justice (DOJ), the U.S. Federal Trade Commission (FTC), and the Cybersecurity and Infrastructure Security Agency (CISA) as it relates to cybersecurity practices in health care.

Alongside this current wave of regulatory and enforcement initiatives come several new compliance guidance documents as well. Risk and compliance professionals in the healthcare industry will want to use these guidance documents to their benefit to benchmark their compliance programs and stay on the right side of the many regulatory enforcement bodies that will be bringing down the hammer on healthcare-related violations in 2024.

New voluntary healthcare-specific cybersecurity performance goals

On January 25, 2024, HHS published its widely anticipated voluntary healthcare-specific Cybersecurity Performance Goals (CPGs) intended to help healthcare organizations "strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety," according to HHS.

The CPGs outline ten "essential" and "enhanced" cybersecurity goals for healthcare organizations to adopt. The essential goals address common vulnerabilities and establish safeguards to better protect against cyber-attacks, improve responses when events occur, and minimize residual risk, HHS said. Such goals include mitigating known vulnerabilities; deploying email security and encryption; implementing multi-factor authentication; handling credentials; cybersecurity training; incident response; and more.

The enhanced cybersecurity goals are designed to encourage healthcare organizations to adopt advanced cybersecurity practices. Such goals include, for example, identifying a healthcare organization's asset inventory; responding to third-party threats and vulnerabilities; engaging in penetration testing; specific technical protocols for detecting and responding to cyber threats; and structuring cybersecurity incident response plans for relevant threat scenarios.

Risk and compliance professionals in the healthcare industry seeking additional guidance should review the healthcare-specific CPGs in combination with the cybersecurity toolkit released by the HHS and CISA in October 2023. The toolkit consolidates several additional resources, including CISA's Cyber Hygiene Services, HHS's Health Industry Cybersecurity Practices, and the Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide.

New cybersecurity requirements and higher penalties

Publication of the healthcare-specific CPGs followed a concept paper that HHS released in December 2023, in which it highlighted a forward-looking strategy for tackling cyber risks in the healthcare industry. In its concept paper, HHS announced its intent to not only create an incentives program to encourage hospitals "to invest in advanced cybersecurity practices," but also to "enforce new cybersecurity requirements through the imposition of financial consequences for hospitals."

As explained by HHS, "Voluntary goals alone will not drive the cyber-related behavioral change needed across the healthcare sector." HHS said it further aspires to incorporate the CPGs into existing regulations and programs to "inform the creation of new enforceable cybersecurity standards."

As part of the U.S. government's broader effort to enhance cybersecurity practices in the healthcare industry, the Centers for Medicare and Medicaid Services (CMS) is considering proposed new cybersecurity requirements for hospitals through Medicare and Medicaid. Additionally, the Office for Civil Rights (OCR) has indicated its intent to revise the HIPAA Security Rule in the Spring of 2024 to include new cybersecurity requirements as well.

HHS further warned the industry in its concept paper that it will work with Congress to "increase civil monetary penalties for HIPAA violations and increase resources for HHS to investigate potential HIPAA violations, conduct proactive audits, and scale outreach and technical assistance for low-resourced organizations to improve HIPAA compliance."

OCR and FTC enforcement of online tracking technologies

Another area of HIPAA non-compliance federal agencies will be paying continued attention to is the use of online tracking technologies by hospitals and telehealth providers, particularly.

In a joint letter sent in July 2023 to approximately 130 healthcare organizations, the OCR and the FTC cautioned hospitals and telehealth providers about "privacy and security risks related to the use of online tracking technologies" that may be present on their websites or mobile applications and that impermissibly could be disclosing consumers' sensitive personal health information (PHI) to third parties.

While OCR administers and enforces compliance with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), which set minimum privacy and security standards for PHI, the FTC enforces deceptive or unfair business practices, including the misuse and exploitation of PHI.

Because tracking technologies are used to collect and analyze information on users' interactions with websites or mobile apps, the HHS and FTC in their joint letter remind healthcare organizations of their compliance obligations under the HIPAA Rules when using tracking technologies related to PHI. As OCR Director Melanie Fontes Rainer warned, "OCR continues to be concerned about impermissible disclosures of health information to third parties and will use all of its resources to address this issue."

Samuel Levine, director of the FTC's Bureau of Consumer Protection, similarly warned, "The FTC is, again, serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."

The OCR and FTC further stressed that companies not covered by HIPAA – such as digital healthcare platforms – also have a responsibility to prevent unauthorized disclosure of PHI. Through a series of recent enforcement actions, the FTC forewarned companies to monitor the flow of PHI to third parties that use tracking technologies, because unauthorized disclosure could

constitute a violation of the FTC Act and a security breach under the FTC's Health Breach Notification Rule.

Risk and compliance professionals of HIPAA-covered entities and business associates seeking further guidance should refer to the OCR's December 2022 bulletin, which provides further clarity on not just what tracking technologies are, but how the HIPAA Rules apply. They should also familiarize themselves with the requirements under the FTC's Health Breach Notification Rule.

Enhanced scrutiny over anticompetitive practices in health care

On Dec. 7, 2023, the White House issued a fact sheet announcing new initiatives to enhance scrutiny over anticompetitive practices in health care. As part of this collective effort, the DOJ, FTC, and the HHS through a joint Request for Information will examine how anticompetitive power and control in health care adversely impacts patient health and safety. This information gained will be used to identify future regulatory and enforcement priorities, according to the fact sheet.

One top priority for the FTC, DOJ, and HHS will be greater scrutiny over "roll-up" deals, whereby PE firms, health insurers, or healthcare providers can gain monopolistic power in the healthcare industry by making a series of small-scale acquisitions. While some illegal roll-up deals might have escaped antitrust scrutiny in the past, that's likely to change under the 2024 antitrust enforcement regime.

The FTC, DOJ, and HHS have indicated they intend not only to assert a greater oversight role but also engage in more data-sharing. Leading these efforts will be a newly appointed chief competition officer at HHS and newly appointed counsels of health care at the FTC and the DOJ's Antitrust Division, according to the White House fact sheet.

As Jonathan Kanter, assistant attorney general for the DOJ's Antitrust Division, warned, "Protecting and promoting competition in health care markets is among the Division's top priorities." Risk and compliance professionals of PE firms, health insurers, and healthcare providers – particularly those that have engaged in recent roll-up deals – should take heed, as 2024 portends to be a busy year for new antitrust investigations and enforcement activity.

Enhanced scrutiny over private ownership in health care

Private investors in health care, especially PE firms, could face the most scrutiny in 2024 as it regards anticompetitive practices. Transparency measures over ownership structures will be a key area of focus. For example, a final rule published by CMS that took effect on Jan. 16, 2024, requires Medicare- and Medicaid-participating nursing homes to disclose "certain ownership, managerial, and other information."

The information required to be disclosed includes:

- Each member of the facility's governing body, including their name, title, and period of service;
- Each person or entity who is an officer, director, member, partner, trustee, or managing employee of the facility, including their name, title, and period of service;
- Each person or entity who is an additional "disclosable party" of the facility; and
- The organizational structure of each additional disclosable party of the facility and a description of the relationship of each such additional disclosable party to the facility and to one another.

CMS indicated that it issued the final rule after receiving information that certain categories of nursing facility owners, including PE firms and real estate investment trusts, "generated concerns about the quality of care that nursing facility residents receive." According to CMS, "having sufficient data on these owners could help CMS better monitor and hold accountable their nursing facilities," and that these new data collection requirements will assist in achieving that goal.

New policies addressing the use of artificial intelligence in health care

On Oct. 30, 2023, the Biden Administration issued an executive order highlighting the U.S. government's plan for addressing the use of artificial intelligence (AI) across numerous industries, including health care.

As part of that broader initiative, the executive order called on HHS to establish an AI Task Force to "develop a strategic plan that includes policies and frameworks – possibly including regulatory action, as appropriate – on responsible deployment and use of AI

and AI-enabled technologies in the health and human services sector."

In an update to that initiative, a White House fact sheet released on Jan. 29, 2024 announced that HHS completed the establishment of the AI Task Force. Next steps will be to develop a strategic plan in the following areas:

- Development, maintenance, and use of predictive and generative AI-enabled technologies in healthcare delivery and financing, including human oversight;
- Long-term safety and real-world performance monitoring of AI-enabled technologies;
- Incorporation of equity principles in AI-enabled technologies and helping to identify and mitigate discrimination and bias in current systems;
- Incorporation of safety, privacy, and security standards into the software development lifecycle to protect personally identifiable information;
- Development, maintenance, and availability of documentation to help users determine appropriate and safe uses of AI in local settings;
- Collaboration with state, local, Tribal, and territorial health and human services agencies to advance positive use cases and best practices for use of AI in local settings; and
- Identification of AI uses to promote workplace efficiency, including reducing administrative burdens.

The executive order further directs HHS to establish an AI Safety Program that "establishes a common framework for approaches to identifying and capturing clinical errors resulting from AI deployed in healthcare settings." A central tracking repository also will be created to track "incidents that cause harm, including through bias or discrimination, to patients, caregivers, or other parties."

Tying it all together: HHS Compliance Program Guidance

On Nov. 6, 2023, the HHS Office of the Inspector General (OIG) issued its long-awaited General Compliance Program Guidance (GCPG), a one-stop-shop reference guide for the healthcare compliance community.

From a resource standpoint, the GCPG provides an extensive overview of certain federal healthcare laws – including the Anti-Kickback Statute, Stark Law, False Claims Act, and HIPAA – and related enforcement actions. The GCPG further provides a long list of OIG processes and resources, including Advisory Opinions, Special Fraud Alerts, Corporate Integrity Agreements, and more.

The most significant portion of the GCPG discusses each of the "seven elements" of a robust compliance program:

- Written policies and procedures
- Compliance leadership and oversight
- Training and education
- Effective lines of communication with the compliance officer
- Enforcing standards: Consequences and Incentives
- Risk assessments, auditing, and monitoring
- Responding to offenses and developing corrective action initiatives

The GCPG further devotes an entire section on how small entities can meet the above seven elements, even with limited resources. Some recommended measures include, for example, designating an individual as the compliance contact with responsibility for ensuring the completion of compliance activities; having in place policies, procedures, and training; fostering a culture that facilitate communications about compliance concerns; and more.

Conclusion

Many of the top regulatory and enforcement themes for the healthcare industry in 2024 are mentioned in the GCPG. For example, the guidance stresses that compliance with the HIPAA Rules "should be a top compliance priority and included in all risk assessments."

The GCPG also directly addresses new entrants in the healthcare industry, including technology companies. Specifically, the OIG noted in the guidance that many business practices that are common in other sectors create compliance risk in health care, including potential criminal, civil, and administrative liability.

Practically speaking, the compliance message for new entrants, according to OIG, is to "take steps to ensure that they and any business partners possess a solid understanding of the federal fraud and abuse laws, in addition to other applicable laws, and that they possess an understanding of the critical role an effective compliance program plays in preventing, detecting, and addressing potential violations." OIG added that new entrants should use the GCPG as a practical tool to assist them in "establishing and operating effective compliance programs for healthcare lines of business."

The GCPG also flags – albeit, briefly – concerns about the growing prominence of private investors in health care, particularly its impact on "ownership incentives (e.g., return on investment) on the delivery of high quality, efficient health care." The GCPG advises healthcare entities, including their investors and governing bodies, to "carefully scrutinize their operations and incentive structures to ensure compliance with Federal fraud and abuse laws and that they are delivering high-quality, safe care for patients."

In addition to the GCPG, the OIG will soon also be releasing industry-specific CPGs (ICPGs) for a variety of healthcare industry subsectors that will replace several existing compliance guidance documents issued over the last three decades. According to OIG, the ICPGs "will be tailored to fraud and abuse risk areas for each industry subsector and will address compliance measures that the industry subsector participants can take to reduce these risks."

The first two ICPGs to be issued will address managed care plans and nursing facilities and are expected at some point in 2024. Both the GCPG and ICPGs will be updated periodically to address newly identified risk areas, compliance measures and regulatory updates.

Although these guidelines are voluntary, risk and compliance professionals in the healthcare industry should use the GCPG, in combination with the relevant ICPG and the healthcare-specific cybersecurity CPG, to benchmark their current compliance program, including cybersecurity practices, to evaluate whether enhancements need to be made in alignment with the best-practice recommendations in these guidance documents.