COSMOS
Navigate the Compliance Universe

Compliance Today - September 2023

Amy M. Joseph (ajoseph@hooperlundy.com, linkedin.com/in/amyjoseph1/) is a Partner at Hooper, Lundy & Bookman P.C., Boston, MA.

Jeremy D. Sherer (jsherer@hooperlundy.com, linkedin.com/in/jeremy-sherer-b8481630/) is a Partner at Hooper, Lundy & Bookman P.C., Boston, MA.

Artificial intelligence: Compliance considerations for provider organizations

by Amy M. Joseph, Esq. and Jeremy D. Sherer, Esq.

Artificial intelligence (AI) is nothing new to the healthcare industry, as many organizations and clinicians have utilized such tools in some capacity for many years. Imaging-related AI to support radiologists is not uncommon, to use one example. However, more recently, there has been a marked increase in interest in the use of such tools in healthcare (and across all industry sectors), including generative AI—i.e., where the technology creates a new output based on existing data—and the range of uses of such tools continues to expand. AI can create potential efficiencies in care delivery as well as in administrative activities and create new touchpoints for patient engagement. For instance, in addition to the development of AI as a clinical decision support tool for practitioners, AI tools can serve as virtual assistants for practice management and provide interactive symptom checkers for use by consumers. AI tools also have the potential to significantly improve healthcare outcomes, such as providing means for earlier detection of a disease or condition. More generally, it is likely that at least some individuals in every organization's workforce have at least tried ChatGPT since its launch in late 2022 for purposes of research or drafting content as part of their responsibilities. All the innovation occurring makes for an exciting time in healthcare, but the opportunities presented by such innovation must be balanced with efforts to mitigate risks.

Key healthcare regulatory risk areas

In addition to the key risks lawmakers and media tend to emphasize—including risk of bias, general data privacy protection laws, and lack of transparency concerning the algorithms used—existing healthcare laws and regulations applicable in other contexts also apply to AI. A summary of some key risk are as follows:

- **Patient privacy laws:** Developing an AI solution requires significant amounts of data. Before using or disclosing any patient information for this purpose, a provider organization should identify applicable laws in place that protect the information and confirm that their intended use or disclosure is permitted. Potentially applicable laws and regulations include, without limitation, HIPAA, 42 C.F.R. Part 2, and state patient privacy laws.
- **Unlicensed practice of medicine:** Any AI solution utilized to inform clinical care must maintain the practitioner's role as the ultimate decision-maker concerning diagnosis and treatment. Technological solutions can be tremendously useful aids to the practice of medicine by quickly analyzing data, identifying patterns, and providing potential recommendations. However, it is critical that practitioners using such solutions limit their application of the tools to *support*, not *supplant*, their independent clinical judgment.

- **Medical malpractice and related risk:** Relatedly, medical malpractice and other tort claims are also a risk where a patient experiences an adverse outcome, and the practitioner utilizes AI as part of their decision-making process. Allegations could arise that practitioners deviated from the standard of care by relying on the AI tool. Of note, such allegations could also extend to the provider organization (e.g., a claim that an employer is vicariously liable or otherwise engaged in negligent or tortious conduct in deploying the tool for the use of its workforce).

- **Billing compliance:** Governmental and private payers each have established requirements that must be met for a particular service to be reimbursable. Though practitioners may determine it is possible for different categories of individuals to provide the service and/or that a lower level of physician supervision is required when utilization of an AI tool is incorporated into the process, if the current payer requirements impose more stringent standards, those requirements should be followed.

- **Anti-kickback laws:** The Office of the National Coordinator of Health Information Technology (ONC) recently raised the concern that remuneration to a developer of AI could implicate the federal Anti-Kickback Statute.[1] An example would be a pharmaceutical manufacturer that provides remuneration to a developer to build the AI in a manner that recommends the order of a particular drug as part of a treatment care plan. The U.S. Department of Health and Human Services (HHS) Office of Inspector General has previously flagged the potential for similar risk with respect to electronic health record vendors, which could equally apply in the context of AI.[2]

- **Addressing bias and unlawful discrimination:** Various government agencies are particularly concerned about AI-producing outcomes that result in unlawful discrimination under existing laws, as reflected in a Joint Statement issued in April affirming a commitment to enforce existing laws to promote "responsible innovation."[3] HHS, in notice-and-comment rulemaking in 2022 to amend regulations implementing Section 1557 of the Affordable Care Act, proposed a new regulatory provision that would prohibit a covered entity from discriminating against an individual "on the basis of race, color, national origin, sex, age, or disability through the use of clinical algorithms in its decision-making."[4] Echoing themes addressed elsewhere in this article regarding the use of independent clinical judgment, HHS emphasized that under the proposed rule, a covered entity could be held liable for decisions made in reliance on the clinical algorithm—even if the covered entity did not itself develop the algorithm.[5]