April 16, 2024

The Robinson+Cole Health Law Group is committed to examining and reporting on issues important to the health care and life sciences industries. For more updates on news and developments for the health care and life sciences industries, we invite you to subscribe to our Health Law Diagnosis blog.

Additional States Implement Notice Requirements for Healthcare Transactions

Authored by Leslie J. Levinson, Danielle J. Tangorre, and Erin C. Turkis

In a prior blog post, we noted the trend of states enacting legislation implementing reporting requirements for certain healthcare transactions. On March 13, 2024, Indiana joined this trend as Indiana Governor Eric Holcomb enacted Senate Enrolled Act No. 9 (the Act). The Act mandates that, effective July 1, 2024, Indiana health care entities involved in a merger or acquisition with another health care entity with total assets of at least ten million dollars ($10,000,000) must notify the Office of the Indiana Attorney General of the transaction at least ninety (90) days prior to closing. Indiana joins several other states with previously passed notice laws, including California, Colorado, Connecticut, Hawaii, Illinois, Massachusetts, Minnesota, Nevada, New York, Oregon, Rhode Island, and Washington.

However, the Act's scope is broader than similar legislation recently enacted in other states. For example, the ten-million-dollar ($10,000,000) threshold is lower than the threshold included in legislation from other states, and the definition of "health care entity" applies to a wide array of entities. The definition of "health care entity" within the Act includes "any organization or business that provides diagnostic, medical, surgical, dental treatment, or rehabilitative care" and also includes various types of insurers. The term "health care entity" additionally encompasses private equity partnerships seeking to enter into a merger or acquisition with an Indiana health care entity regardless of where the private equity partnership is located. *Read more*

Forecasting the Integration of AI into Health Care Compliance Programs

Authored by Kathleen G. Healy and Josh Yoo*

Health care entities maintain compliance programs in order to comply with the myriad changing laws and regulations that apply to the health care industry. Although laws and regulations specific to the use of artificial intelligence (AI) are limited at this time and in the early stages of development, current law and pending legislation offer a forecast of standards that may become applicable to AI. Health care entities may want to begin to monitor the evolving guidance applicable to AI and start to integrate AI standards into their compliance programs in order to manage and minimize this emerging area of legal risk.

Executive Branch: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

Following Executive Order 13960 and the Blueprint for an AI Bill of Rights, Executive Order No. 14110 (EO) amplifies the current key principles and directives that will guide federal agency oversight of AI. While still largely aspirational, these principles have already begun to reshape regulatory obligations for health care entities. For

example, the Department of Health and Human Services (HHS) has established an AI Task Force to regulate AI in accordance with the EO's principles by 2025. Health care entities would be well-served to monitor federal priorities and begin to formally integrate AI standards into their corporate compliance plans.

- Confidentiality and Security: Federal scrutiny of the privacy and security of entrusted information extends to AI's interactions with data as a core obligation. This general principle also manifests in more specific directives throughout the EO. The EO also orders the HHS AI Task Force to incorporate "measures to address AI-enhanced cybersecurity threats in the health and human services sector."
- Transparency: The principle of transparency refers to an AI user's ability to understand the technology's uses, processes, and risks. Health care entities will likely be expected to understand how their AI tools collect, process, and predict data. The EO envisions labelling requirements that will flag AI-generated content for consumers as well.
- Governance: Governance applies to an organization's control over deployed AI tools. Internal mechanical controls, such as evaluations, policies, and institutions, may ensure continuous control throughout the AI's life cycle. The EO also emphasizes the importance of human oversight. Responsibility for AI implementation, review, and maintenance can be clearly identified and assigned to appropriate employees and specialists.
- Non-Discrimination: AI must also abide by standards that protect against unlawful discrimination. For example, the HHS AI Task force will be responsible for ensuring that health care entities continuously monitor and mitigate algorithmic processes that could contribute to discriminatory outcomes. It will be important to permit internal and external stakeholders to have access to equitable participation in the development and use of AI.

National Institute of Standards and Technology: Risk Management Framework

The National Institute of Standards and Technology (NIST) published aRisk Management Framework for AI (RMF) in 2023. Similar to the EO, the RMF outlines broad goals (i.e., Govern, Map, Measure, and Manage) to help organizations address and manage the risks of AI tools and systems. A supplementary NIST "Playbook" provides actionable recommendations that implement EO principles to assist organizations to proactively mitigate legal risk under future laws and regulations. For example, a health care organization may uphold AI governance and non-discrimination by deploying a diverse, AI-trained compliance team. *Read more*

**This post was co-authored by Josh Yoo, legal intern at Robinson+Cole. Josh is not admitted to practice law.*

HC3 Warns Health Sector About Social Engineering Attacks Against IT Help Desks

Authored by Linn F. Freedman

The Health Sector Cybersecurity Coordination Center (HC3) recently issued an Alert warning that "threat actors employing advanced social engineering tactics to target IT help desks in the health sector and gain initial access to target organizations" have been on the rise.

The social engineering scheme starts with a telephone call to the IT help desk from "an area code local to the target organization, claiming to be an employee in a financial role (specifically in revenue cycle or administrator roles). The threat actor is able to provide the required sensitive information for identity verification, including the last four digits of the target employee's social security number (SSN) and corporate ID number, along with other demographic details. These details were likely obtained from professional networking sites and other publicly available information sources, such as previous data breaches. The threat actor claimed that their phone was broken and, therefore, could not log in or receive MFA tokens. The threat actor then successfully convinced the IT help desk to enroll a new device in multi-factor authentication (MFA) to gain access to corporate resources."

After the threat actor gains access, login information related to payer websites is targeted, and they submit a form to make ACH changes for payer accounts. "Once access has been gained to employee email accounts, they sent instructions to payment processors to divert legitimate payments to attacker-controlled U.S. bank accounts. The funds were then transferred to overseas accounts. During the malicious campaign, the threat actor also registered a domain with a single letter variation of the target organization and created an account impersonating the target organization's Chief Financial Officer (CFO)."

The threat actors are leveraging spearphishing voice techniques and impersonating employees, also known as "vishing." IC3 noted that "threat actors may also attempt to leverage AI voice impersonation techniques to social engineer targets, making remote identity verification increasingly difficult with these technological advancements. A recent global study found that out of 7,000 people surveyed, one in four said that they had experienced an AI voice cloning scam or knew someone who had."

IC3 provides numerous mitigations to assist with the prevention of these vishing schemes, which are outlined in the Alert.

If you have any questions, please contact any member of Robinson+Cole's Health Law Group.

Lisa M. Boyle **(Chair)** | Nathaniel T. Arden | Conor O. Duffy | Kathleen G. Healy | Leslie J. Levinson

Danielle H. Tangorre | Melissa (Lisa) Thompson | Theodore J. Tucci | Peter H. Struzzi

Patricia D. Weitzman | Yelena Greenberg | Michael G. Lisitano | Erin C. Turkis

Above is the latest from our *Health Law Diagnosis* blog, where we post on fraud and abuse, government enforcement, Medicare and Medicaid, reimbursement, hospitals and health systems, pharmaceuticals, medical devices, and other areas of interest.

For more updates on news and developments for the health care and life sciences industries, we invite you to subscribe.

Boston | Hartford | New York | Washington, DC | Providence | Miami
Stamford | Wilmington | Philadelphia | Los Angeles | Albany | **rc.com**