Compliance Program Updates in Response to DOJ's Updated Compliance Program Guidance

In September 2024, the U.S. Department of Justice ("DOJ") updated its corporate compliance program guidance which DOJ officials use to evaluate the effectiveness of an organization's compliance program guidance for purposes of making decisions on who to prosecute, what charges to bring, and settlement agreements and plea deals. In response, healthcare providers should review and update their compliance programs to address the DOJ updates including:

- Conduct a periodic risk assessment which includes identifying and managing internal and external risks that could impact your organization's compliance with the law, including how emerging and new technologies may impact your ability to comply with the law.
- Incorporate and consider new and emerging technologies, including artificial intelligence ("AI"), into your organization's compliance risk assessment.
- Identify and implement measures to mitigate the risk posed by your organization's use of new and emerging technologies, including AI.
- Adopt an organizational policy on the use of AI, including how the organization is attempting to curb any potential negative impact or unintended consequences as a result of using AI as well as any misuse of technology by the organization or its officers and employees.
- Implement controls to monitor and ensure the trustworthiness, reliability, and use of AI in compliance with applicable law and the organization's policies, including ensuring AI technology is only used for its intended purpose and is functioning as intended.
- Train employees on AI technologies and your organization's policies relating to AI technologies.
- Periodically monitor the use of AI and enforce policies relating to AI.
- Identify data and leverage data analytics tools to promote compliance, including creating efficiencies in compliance operations and gaining insight into the effectiveness of your compliance program.
- Implement mechanisms to ensure the quality and accuracy of the data used by the organization.
- Implement processes to identify misconduct at the earliest stage possible, such as periodic proactive audits.
- Periodically measure the success and effectiveness of your compliance program.
- Ensure your compliance personnel have knowledge of and access to relevant data sources in a reasonably timely manner.
- Compare the assets, resources, and technology your compliance and risk management departments have compared to other departments within the organization to determine whether they are commensurate and if not, whether

there is an opportunity to improve assets, resources, and technology to the compliance and risk management functions.

- ☐ Implement a process to update policies and procedures to reflect lessons learned from your organization's compliance issues or reported non-compliance of other similar providers or organizations in the same geographic area.
- ☐ Update policies to address new and emerging risks, including new technologies.
- ☐ Ensure compliance-related trainings are tailored to your organization and personalized to your employees so that they are highly relevant to them and are more likely to be effective.
- ☐ Include in your compliance training information on how to report compliance concerns and lessons learned from prior non-compliance incidents in your organization and other similar organizations.
- ☐ Evaluate the effectiveness of your compliance training, including whether the employees learned the subject matter.
- ☐ Encourage reporting by employees and others of compliance concerns, including publicizing how compliance concerns should be reported internally as well as your anonymous reporting policy.
- ☐ Assess employee knowledge and comfortability reporting compliance issues, such as through an anonymous employee survey.
- ☐ Adopt an anti-retaliation policy if you do not already have one.
- ☐ Include in your discipline policies consideration of whether the employee reported the misconduct.
- ☐ Ensure you have a process to review and evaluate vendors promptly and consider how you can leverage available data to evaluate the risks posed by the vendor.

In any merger or acquisition, the DOJ also will be evaluating how you're integrating the new business into your compliance program, including:

- ☐ How is the organization including compliance and risk management into the integration strategy?
- ☐ What is the organization's process to implement and integrate a compliance program post-transaction?
- ☐ Does the organization have a process in place to ensure appropriate compliance oversight of the new business?
- ☐ How is the new business incorporated into the organization's risk assessment activities?
- ☐ How are compliance policies and procedures organized?
- ☐ Are post-transaction audits conducted at the newly acquired entity?