Risky Business? OIG Finds Room for Improvement in NIH's Data Sharing

Earlier this month, the National Institutes of Health (NIH) received the results of an audit by the Department of Health and Human Services' Office of the Inspector General (OIG). The agency's findings included concern over risks in NIH data sharing processes, despite the fact that NIH itself disputed some of those OIG conclusions.

The audit specifically sought to assess whether the NIH was sufficiently protecting sensitive data when it was shared. The OIG's assessment lens was established Federal guidance, and the agency also interviewed NIH employees to reach its determination.

NIH is urged to bring in outside experts

Ultimately, the OIG concluded that NIH's controls regarding data access permissions and monitoring are not fully adequate for those critical tasks. The OIG furnished NIH with specific suggestions for strengthening those data access controls, and also urged the agency to seek help from a firm outside the government that has experience with ameliorating the misuse of scientific data.

"NIH could strengthen its controls by developing a security framework, conducting a risk assessment, and implementing additional appropriate security controls designed to safeguard sensitive data," the OIG's report stated.

Although the OIG did not share the specific data control risks it found with the public, the statement went on to say, "We also recommend that NIH develop and implement mechanisms to ensure data security policies keep current with emerging threats. . . [W]e recommend that NIH make security awareness training and security plans a requirement."

NIH rejects some of the audit's conclusions

However emphatic the tone of the OIG's findings, NIH officials did not accept them all as fact, according to the OIG. Specifically, the NIH pushed back when it came to the OIG suggesting the implementation of new data controls, the carrying out of a risk assessment, the creation of a security framework, and new controls to guarantee training and security plan mandates.

Where the two agencies saw eye to eye was in the matter of the need for NIH's policies to change according to changes in the types of threats to sensitive data. Further, NIH officials reported the development of a group tasked with decreasing security risks to intellectual property as well as the protection of the fruits of peer review processes.

Acknowledging NIH's refutation of parts of the OIG's findings, the latter doubled down on its conclusions (calling them "valid") and urged the biomedical research agency to remain open to ways of evaluating and addressing issues highlighted in the report.

"We recognize that NIH reported that it is already taking certain actions, such as the working group that was recently established, that may address our recommendations," OIG officials said. "If NIH determines that it does not need to strengthen its controls, it should document that determination consistent with applicable Federal regulations and guidance."

According to the OIG, "NIH is the largest public funder of biomedical research agency in the world, investing more

than $30 billion in taxpayer dollars to achieve its mission. NIH's mission is to seek fundamental knowledge about the nature and behavior of living systems and the application of that knowledge to enhance health, lengthen life, and reduce illness and disability."

This article is provided for educational purposes only and is not offered as, and should not be relied on as, legal advice. Any individual or entity reading this information should consult an attorney for their particular situation. For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.