STRATEGIC MANAGEMENT SERVICES

Meeting HIPAA Mandates and Standards in 2024

Richard P. Kusserow | January 2024

Key Points:

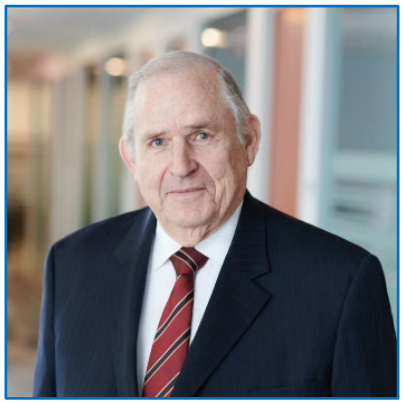
- **Organizations are mandated to have a Privacy Officer**
- **Four out of five organizations have HIPAA Privacy under the Compliance Office**
- **Encounter with OCR is seven times more likely than with the OIG, DOJ, or MFCU**
- **Meeting HIPAA Privacy requirements is a significant challenge for smaller organizations**
- **Proper use of outside experts might be a cost-efficient means to meet obligations**

HIPAA compliance is required for all covered entities and is vital to maintaining a healthcare organization or business and ensuring patient privacy and patient data. The 2023 Compliance Benchmark Survey results show that over three out of four healthcare organizations have responsibility for HIPAA Privacy under the Compliance Office. Also, results indicated that organizations were seven times more likely to encounter the DHHS OCR than the OIG, DOJ, or Medicaid Fraud Control Unit. Failure to comply can result in severe penalties. The complexity of compliance is significant due to the range of meeting requirements to comply with federal and related state laws. For many organizations, HIPAA compliance is more taxing than corporate compliance for (a) conducting HIPAA compliance assessments, (b) keeping policies/procedures up to date with federal and state-related rules, (c) developing and delivering comprehensive employee training programs, and (d) incident management where there are data breaches in Protected Health Information (PHI). All this makes efficient management of the program challenging with Compliance Offices, especially those with limited staff. All this has resulted in a mounting trend to look outside the organization for solutions. Many smaller organizations simply outsource HIPAA Privacy Officer functions part-time to consultants specializing in meeting the requirements of the laws. Other organizations have an on-call arrangement with qualified consultants to be available, as needed, to address all the required actions. These steps have the advantage of having experts who deeply understand what is required and needed. This can translate to better compliance with the many requirements at a lower cost. Engaging consultants

to assume the responsibility for being the HIPAA Privacy Officer or as supplemental support for the program means the organization has someone who can:

1. Develop a year-round compliance plan based on industry standards
2. Conduct risk analyses and assessments
3. Develop and deliver effective HIPAA Privacy training
4. Guide management on protecting PHI
5. Develop and keep up-to-date HIPAA policies, procedures, and internal controls
6. Develop best practices for ongoing compliance and remediation activities
7. Prepare for and plan actions to respond to data breaches
8. Address breaches in data if they occur
9. Assist in incident response and reporting

For more details on alternative approaches to meeting HIPAA-mandated standards, contact rkusserow@strategicm.com.



About the Author

Richard P. Kusserow established Strategic Management Services, LLC, after retiring from being the DHHS Inspector General, and has assisted over 2,000 health care organizations and entities in developing, implementing and assessing compliance programs.