STRATEGIC MANAGEMENT SERVICES

Meeting HIPAA Privacy Challenges In 2023

Richard P. Kusserow | March 2023

Key Points:

- **HIPAA violations are the most common cause of enforcement encounters**
- **Many Compliance Officers have HIPAA Privacy responsibility**
- **Strain on available resources has been aggravated by the Pandemic**
- **Great fluctuation in staffing complicates managing HIPAA Privacy**
- **For smaller organizations, outsourcing may be the right option**

For the last several years, the national Compliance Benchmark Survey by SAI360 and Strategic Management Services found that by far, healthcare organizations encounter Office for Civil Rights (OCR) HIPAA enforcement encounters involving breaches of Protected Health Information (PHI) more often than other enforcement agencies, including DOJ, OIG, and MFCUs. With most Compliance Offices having responsibility for HIPAA Privacy, there has been added workload that often rivals that of compliance in terms of expertise, time and effort. The strain of additional responsibilities has been exacerbated by the COVID-19 pandemic that caused widespread staffing shortages. Another factor is the great fluctuation of routine privacy duties with spikes in work for annual assessments, training, and addressing breaches. To meet the challenges of HIPAA privacy requires finding people with wide knowledge, expertise, and experience often difficult to engage. Relying on an existing staff member without HIPAA experience as a secondary duty may not work because of needed expertise and experience in addressing the complexities of the laws and regulations. However, hiring someone exclusively devoted to this area may be difficult and costly. As a result, many organizations find outsourcing the privacy function to experts to develop implement and maintain key documents in accordance with applicable federal and state laws to be the right solution for them. This is most often found with organizations lacking resources to support a full time Privacy Officer. An outsourced expert can address assessing the program; confidentiality, consent and authorization forms; information notices and other materials describing policies and requirements; ensuring employee awareness and responsibilities through education and training programs; overseeing the monitoring of data access; performing annual

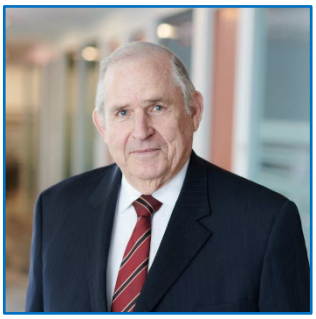
mandated risk assessments, and conducting investigations and remediation of data breaches and complaints. When outsourcing, it is critical to engage a party properly qualified that has multi-million-dollar liability insurance coverage. Outsourcing advantages include:

- Less costly and avoids loaded cost of a W-2 employee (FICA, leave, and other benefits)
- Lower fixed costs and reduced staff workload
- Able to manage fluctuation in workload
- Paying only for hours worked
- Already knowledgeable of privacy state/federal laws, requirements and standards
- Availability and experience in conducting mandated annual HIPAA risk assessment
- Able to update annual HIPAA Privacy training and education programs
- Experience in dealing with data breaches and other privacy issues
- Provide better risk protection
- Expertise in HIPAA/HITECH privacy and security compliance

For more information on this topic, contact Lisa Shuman (lshuman@strategicm.com)

For answers to compliance FAQs, see https://www.compliance.com/faqs/

Keep up-to-date with Strategic Management Services by following us on LinkedIn.



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.