

## **OCR Returning to Stricter Enforcement with End of the Public Health Emergency**

**Richard P. Kusserow | June 2023**

### **Key Points:**

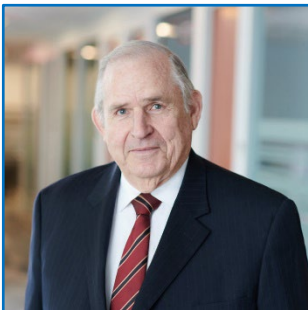
- **Flexibility and tolerance extended during the emergency are coming to an end**
- **With the end of the PHE, HIPAA-covered entities must quickly come into compliance**
- **Tips for Compliance Officers**

The Office for Civil Rights (OCR) **announced** with the end of the COVID-19 Public Health Emergency (PHE), that they would exercise stepped-up enforcement of Covered Entities' compliance with HIPAA Privacy and Security requirements. They intend to focus on communications technologies that fail to comply with HIPAA, such as flexibilities that allow technology providers access to protected health information (PHI) without a HIPAA Business Associate Agreement (BAA). OCR permitted flexibility during the PHE for Business Associates to share COVID-19 data with government agencies without specific authority under BAAs. However, now that the PHE has ended, Covered Entities and their service providers who qualify as business associates under HIPAA (Business Associates) must bring any ongoing services into compliance. This includes bringing Risk Assessments up to date. OCR noted that many BAAs may not have signed during the PHE because they were not required at the time by OCR. BAA compliance is more than a written agreement, and Covered Entities must do their usual diligence to ensure that vendors have the compliance infrastructure necessary to protect PHI in accordance with HIPAA requirements. Noteworthy is that the period of enforcement discretion ends August 9, 2023, for telehealth and ended May 11, 2023, for all other OCR notices of enforcement discretion. With the end of PHE, all HIPAA-regulated entities need to quickly come into compliance and should:

1. Identify BAA needs and take steps to ensure compliance.
2. Perform due diligence on all subcontractors with respect to privacy and security practices.

3. Conduct due diligence regarding HIPAA compliance.
4. Conduct due diligence on vendors relating to privacy and security requirements.
5. Conduct security risk assessments.
6. Update risk management plans and security policies and procedures.
7. Train employees on what the end of the PHE means from a HIPAA compliance perspective.
8. Identify all subcontractors that will need BAAs.
9. Vendors should also ensure they have BAAs with their subcontractors with access to PHI.
10. Business Associates should provide training to employees regarding HIPAA compliance.

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.