December 8, 2025

Paula Stannard, JD
Director
Office for Civil Rights
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Submitted electronically via OCRPresents@hhs.gov

Dear Director Stannard:

The Workgroup for Electronic Data Interchange (WEDI) is submitting recommendations for topics to address for the Office for Civil Rights' (OCR) upcoming video reviewing the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule's Risk Management implementation specification for HIPAA covered entities and business associates.

WEDI is the leading authority on the use of health information technology to improve health care information exchange to enhance the quality of care, improve efficiency, and reduce costs of our nation's health care system. WEDI was formed in 1991 by the Secretary of the Department of Health and Human Services (HHS) and was designated in HIPAA as an advisor to HHS. WEDI's diverse membership includes health plans, providers, standards development organizations, vendors, federal and state government agencies, and patient advocacy organizations.

WEDI appreciates OCR's continuing commitment to educate the health care industry on the importance of HIPAA Security, specifically the Risk Management process. WEDI, through the expertise of our Privacy and Security Workgroup, supports furthering covered entities' and business associates' awareness of the importance of conducting a comprehensive and ongoing Risk Analysis process in support of ongoing decision making and Risk Management.

We recommend you consider addressing the following areas within the content of your video:

1. Remind viewers that effective Risk Management is only possible if the initial Risk Analysis is comprehensive. Point to the previous guidance offered about understanding the protected health information (PHI) data flow (create, receive, maintain, transmit, and store) and how this is an absolute cornerstone for effective Risk Management. If the underlying Risk Analysis is not complete and kept current, the decisions undertaken in the Risk Management process will be faulty.

2. Include the concept of Risk Management as an ongoing organizational priority and that the responsibility of the organization is to address significant changes to its environment such as legal and organizational, major operational, technical environmental, cyber events/incidents, new and renewed third-party contracts, and emerging technology usage such as artificial intelligence (AI). It will be important to emphasize that conducting a Risk Analysis prior to business decision-making is best practice. It should be stressed that all decisions that could impact PHI and data handled by the organization should be evaluated for risk.

3. Underscore that senior leaders must understand the importance of knowing where the data is, who has access (noting that the presence of third-party partners and vendors require contractual security obligations), how it is handled, and what policies and procedures and risk management processes are in place. Emphasize that that addressing potential issues is a critical step in lessening potential negative impacts of cyber incidents.

4. Highlight that a Risk Management Plan needs to be incorporated into the development of the organization's Incident Response and Business Continuity/Disaster Recovery plans. As such, we recommend the video note the value and impact of conducting a thorough Risk Analysis to support Risk Management and the entity's ongoing business operations.

5. Expand the resource listing at the end of the video, should one be included. We recommend spotlighting an updated related Merit-based Incentive Payment System (MIPS) attestation measures that modifies the security risk analysis measure with a two-part attestation to: *increase accountability among MIPS eligible clinicians who have not taken steps to reduce risks and vulnerabilities to ePHI and to provide transparency regarding the efforts of MIPS eligible clinicians that are already taking steps to manage this risk. Furthermore, the proposal is in alignment with the finalized modification to the Security Risk Analysis measure in the Medicare Promoting Interoperability Program (90 FR 37045 through 37048).* This listing would assist with visibility on the attestation measure change and support provider education and readiness. The resource list could include a link and/or brief description.

We commend the agency for developing this much needed education and appreciate the opportunity to share our content recommendations for this important educational video. We stand ready to work with OCR on this and future education on HIPAA Privacy, Security, and Cybersecurity regulations. Please contact Robert Tennant, WEDI Executive Director, at rtennant@WEDI.org with any questions on these recommendations.

Sincerely,
/s/
Merri-Lee Stine
Chair, WEDI

cc: WEDI Board of Directors