

Report on Patient Privacy Volume 19, Number 4. April 10, 2019 Risk Assessment Should Be Continual To Meet OCR Standards, Avoid Penalties

By Jane Anderson

HIPAA risk assessment isn't a once-a-year procedure that produces a checklist. Instead, to satisfy the HHS Office for Civil Rights (OCR), risk assessment should be a continual activity that identifies and documents a health care organization's threats and vulnerabilities and prioritizes remediation, security experts say.

"Risk analysis is an ongoing process. It's not a destination; it is a journey," Steve Cagle, CEO, Clearwater Compliance, told attendees at the HIPAA Summit in Washington, D.C., in March. "The security rule does not specify how often you need to do risk analysis, so you really need to determine how often you need to do this. A lot of health care organizations struggle with this."

It's critical to get this right, Cagle said, because a total of 89% of electronic protected health information (ePHI) OCR enforcement actions cited risk analysis failure. These failures ranged from submission of the wrong report to not having a detailed enough report or not enough documentation, he said.

Cagle said that OCR guidance has outlined nine key elements for HIPAA risk analysis:

1. Scope of the analysis
2. Data collection
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Finalize documentation
9. Periodic review and updates to the risk assessment

Cagle said that Clearwater Compliance would add a tenth key element: Meeting the emerging OCR standard of care.

Matthew Farry, senior security specialist at GreyCastle Security LLC in Troy, New York, told conference attendees that risk management should focus on confidentiality, integrity and availability of information assets.

This document is only available to subscribers. Please [log in](#) or [purchase access](#).

[Purchase Login](#)
