

# Cyber-Attack Quick Response

Experienced a ransomware attack or other cyber-related security incident? This Cyber-Attack Quick Response guide will explain steps that a HIPAA covered entity or its business associate should take to respond.



RESPOND

The entity must execute response and mitigation procedures, and contingency plans.



REPORT CRIME

The entity should report the crime to criminal law enforcement agencies.



REPORT THREAT

The entity should report all cyber threat indicators to the appropriate federal agencies and ISAOs.



ASSESS BREACH

The entity must assess the incident to determine if there is a breach of protected health information.

If YES

Is there a breach?

If NO

All breaches must be reported to the affected individuals no later than 60 days from occurrence. If the breach affects 500 or more individuals, the entity must report to OCR and the media as soon as possible, but no later than 60 days from the occurrence. If the breach affects fewer than 500 individuals, the entity must report to OCR no later than 60 days after the calendar year of the breach.

The entity must document and retain all information considered during the risk assessment of the cyber-attack, including how it determined no breach occurred.