HEALTHSURE
prevent.protect.prosper

## OCR Quick-response Checklist

Has your entity just experienced a ransomware attack or other cyber-related security incident, and you are wondering what to do now? The guide issued by OCR explains, in brief, the steps for a HIPAA covered entity or its business associate (the entity) to take in response to a cyber-related security incident.

In the event of a cyber attack or similar emergency, a covered entity:

- ☐ **Must execute its response and mitigation procedures and contingency plans**.
  For example, the entity should immediately fix any technical or other problems to stop the incident. The entity should also take steps to mitigate any impermissible PHI disclosure. These steps may be performed by the entity's own information technology staff, or by an outside entity brought in to help (which would be a business associate, if it has access to PHI for that purpose).

- ☐ **Should report the crime to appropriate law enforcement agencies**.
  These agencies may include state or local law enforcement, the FBI or the Secret Service. Reports to these agencies should not include PHI unless otherwise permitted under HIPAA. If a law enforcement official tells the entity that any potential breach report would impede a criminal investigation or harm national security, the entity must delay reporting a breach for the time the law enforcement official requests in writing or for 30 days if the request is made orally.

- ☐ **Should report all cyber threat indicators to federal and information-sharing and analysis organizations (ISAOs).**
  These organizations may include the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs. Reports to these organizations should not include PHI. The OCR does not receive these reports from its federal or HHS partners.

- ☐ **Must report the breach to affected individuals and to the OCR as soon as possible**.
  - If a breach affects 500 or more individuals, the covered entity must notify the affected individuals, the OCR and the media **no later than 60 days** after discovering the breach, unless a law enforcement official has requested a delay in the reporting.
  - If a breach affects fewer than 500 individuals, the entity must notify the affected individuals without unreasonable delay, but **no later than 60 days** after discovery of the breach, and notify the OCR within **60 days after the end of the calendar year** in which the breach was discovered.