KRIEG DEVAULT

Insights

Importance Of Having A Contingency Plan

May 23, 2018

By: Stacy Walton Long and Stephanie T. Eckerle

In March 2018, the U.S. Department of Health and Human Services Office of Civil Rights (OCR) issued a newsletter entitled, "Plan A… B… Contingency Plan!" While contingency plans are already required under the HIPAA Security Rule[1], OCR's newsletter provides guidance regarding the importance and required elements of contingency plans. "The purpose of any contingency plan is to allow an organization to return to its daily operations as quickly as possible after an unforeseen event. The contingency plan protects resources, minimizes customer inconvenience and identifies key staff, assigning specific responsibilities in the context of the recovery."[2]

Contingency plans are not only necessary to respond to natural disasters, but cyberattacks as well. "Cyberattacks using malicious software such as ransomware may render an organization's data unreadable or unusable."[3] Restoring an entity's data from backups may be the only option to recover the data and maintain normal business operations. Therefore, having a contingency plan in place is crucial for entities, especially covered entities who store protected health information.

A contingency plan sets forth step-by-step guidance on how to respond in an emergency and recover or maintain normal business operations.

The requirements for a HIPAA contingency plan are as follows:

(1) Disaster Recovery Plan that seeks to restore an organization's protected health data;
(2) Emergency Mode Operation Plan that seeks to maintain and protect critical functions that protect the security of protected health data; and
(3) Data Backup Plan that is focused on regularly copying protected health data to ensure it can be restored in the event of a loss or disruption.[4]

As part of the HIPAA contingency plan, it is crucial to identify what applications and data are critical for the contingency plan, to test the contingency plan, and revise any identified deficiencies.

When implementing a contingency plan, it is necessary to establish guidelines and procedures, such as:

(1) Maintain critical operations and minimize loss.
(2) Define time periods – What must be done during the first hour, day, or week?
(3) Establish plan activation – What events will cause the activation of the contingency plan and who has the authority to activate the contingency plan?
(4) Use plain language – The plan should be understandable to all levels of employees.[5]

When a contingency plan is created and implemented into the organization, communicate the plan with the organization and explain the responsibilities under the plan, set a test schedule for the plan to identify any issues and the effectiveness of the plan, and review the plan on a regular basis, especially when there are any organizational changes that may affect the plan.

Create a contingency plan now. Do not wait for an emergency to happen. For additional information regarding contingency plans, see:

- OCR:

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf?language=es

- National Institute of Standards and Technology (NIST):

https://csrc.nist.gov/Topics/Security-and-Privacy/security-programs-and-operations/contingency-planning

https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final (SP 800?34 rev1 and Supplemental Material)

- Assistant Secretary for Preparedness and Response:

https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/hc-coop2-recovery.pdf

If you have any questions regarding HIPAA contingency plans, please contact Stacy Walton Long at slong@kdlegal.com or Stephanie T. Eckerle at seckerle@kdlegal.com, or your regular Krieg DeVault attorney.

1 45 CFR § 164.308(a)(7).
2 https://www.hhs.gov/sites/default/files/march-2018-ocr-cyber-newsletter-contingency-planning.pdf.
3 Id.
4 https://www.hhs.gov/sites/default/files/march-2018-ocr-cyber-newsletter-contingency-planning.pdf.
5 Id.