HHS FAQs Address Change Healthcare Cybersecurity Incident

EBIA Weekly (May 2, 2024)

Change Healthcare Cybersecurity Incident Frequently Asked Questions (Apr. 19, 2024)

Available at https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html

HHS's Office of Civil Rights (OCR) has issued FAQs related to its investigation of the recent cybersecurity incident involving Change Healthcare (which serves as a HIPAA business associate for health plans and providers nationwide). As background, in March 2024, OCR announced in a letter that they had initiated an investigation into the incident to determine whether a breach of protected health information (PHI) occurred.

Several FAQs address the letter and the investigation, explaining that while there have been no breach reports related to the cyberattack, the investigation was opened due to the threat posed to health care and billing information operations nationwide. Covered entities and business associates (collectively "regulated entities") are reminded of their obligations under HIPAA to have business associate agreements in place and to ensure that timely breach notification occurs. OCR explains that, for regulated entities affected by the cyberattacks, a breach is presumed to have occurred unless a covered entity demonstrates that there is a "low probability that the PHI has been compromised" as outlined in the breach notification rule. In the event of a breach, regulated entities have the following breach notification requirements:

- If 500 or more individuals are affected, the covered entity must provide notice to affected individuals, HHS, and the media within 60 days after the breach is discovered.
- If fewer than 500 individuals are affected, the covered entity must provide notice to the affected individuals within 60 days after discovery of the breach, and to HHS within 60 days after the end of the calendar year in which the breach is discovered.
- If the number of individuals affected by the breach is uncertain, the covered entity must provide an estimate at the time of notification, which can be updated if additional information is discovered.
- Business associates must notify covered entities following a breach without unreasonable delay, but no later than 60 calendar days from the discovery of the breach, with identification of each individual reasonably believed to be affected by the breach, and any other available information required.
- OCR verifies the accuracy of any breach report received, generally within 14 days depending on the circumstances, before posting the breach on the breach portal (if it affects 500 or more individuals). A covered entity may delegate the responsibility of providing breach notices to the business associate, but the covered entity is ultimately responsible for ensuring individuals are notified.

EBIA Comment: Regulated entities interested in avoiding the cost and inconvenience of enforcement actions should review the FAQs (which OCR says it plans to update as needed) and the provided links to resources. The FAQs specifically point to OCR's ransomware guidance, which has information on actions

© 2024 Thomson Reuters/EBIA. All rights reserved.

for regulated entities to take to determine if a ransomware incident is a breach (which is a fact-specific determination). OCR highlights that if covered entities are aware of a potential breach by a business associate, there is an obligation to proactively investigate whether a breach occurred, and report the breach to HHS, impacted individuals, and in certain cases, the media. For more information, see EBIA's HIPAA Portability, Privacy & Security manual at Sections XX ("Enforcement of Privacy, Security, and EDI Rules") and XXXII ("Electronic Transactions and Code Sets").

Contributing Editors: EBIA Staff.

© 2024 Thomson Reuters/EBIA. All rights reserved.