HHS Updates Change Healthcare Cybersecurity Incident FAQs

EBIA Weekly (June 6, 2024)

Change Healthcare Cybersecurity Incident Frequently Asked Questions (updated May 31, 2024)

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

HHS's Office for Civil Rights (OCR) has updated its FAQs addressing the investigation of Change Healthcare (a unit of United Healthcare Group (UHG) that serves as a HIPAA business associate for health plans and providers nationwide). As background, in March 2024, OCR announced in a letter that it had initiated an investigation into the Change Healthcare cyberattack to determine if a breach of protected health information (PHI) occurred. Initial FAQs elaborated on why OCR opened the investigation and reiterated that covered entities and business associates are obligated under HIPAA to have business associate agreements in place. The FAQs also highlighted that if a covered entity is aware of a potential business associate breach, it must proactively investigate whether a breach has occurred and timely report the breach as outlined in the HITECH Act and the HIPAA breach notification rule.

The updated FAQs address inquiries OCR has received regarding who is responsible for providing breach notifications of a business associate breach, and when the notifications must be provided. The FAQs clarify that—

- covered entities affected by a breach may delegate to the business associate (in this instance, Change Healthcare or UHG) the task of providing the required HIPAA breach notifications on their behalf;
- only one entity (either the covered entity or the business associate) needs to complete breach notifications to affected individuals, HHS, and the media; and
- if covered entities work with a business associate to perform the required breach notifications consistent with the HITECH Act and the HIPAA breach notification rule, there are no further notice obligations.

The FAQs confirm that while a covered entity may delegate the responsibility of providing breach notices to the business associate, it is responsible for ensuring individuals are notified of a breach without unreasonable delay, and in no case later than 60 calendar days from the discovery of the breach. (In this case, because UHG has offered to provide notifications on behalf of covered entities, the 60-calendar day period will not start until covered entities have received a breach report from Change Healthcare or UHG.) Covered entities are obligated to assure that notices issued by the business associate comply with the breach notification rule's requirements regarding timing, content, and form.

EBIA Comment: In response to the initial FAQs, covered entities associated with the Change Healthcare incident had requested clarification regarding whether they were obligated to provide breach notifications before receiving confirmation from Change Healthcare or UHG that a breach had occurred. The FAQs clarify that covered entities do not have to provide HIPAA breach notifications before a business

associate breach has been reported. Once the business associate provides necessary information to the covered entity that a breach has occurred, covered entities have 60 calendar days to ensure that breach notifications are provided to impacted individuals. Covered entities can delegate HIPAA notice obligations to business associates but must ensure that notices comply with the breach notification rule. 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.