Change Healthcare Data Breach HIPAA Considerations

Issued date: 07/24/24

Earlier this year, Change Healthcare, a large health payment processing company, announced a massive data breach which compromised personal information, including health information. Many large health insurance carriers and third-party administrators ("TPAs") utilize Change Healthcare for claims processing and payment. Recently, Change Healthcare announced it is in the late stages of its data review and has identified certain customers whose members' or patients' data was impacted. This includes protected health information ("PHI") of millions of health plan beneficiaries, possibly in the range of one-third of all Americans. The Department of Health and Human Services ("HHS") has initiated an investigation. In addition, dozens of lawsuits have been filed.

Multiple insurance carriers and TPAs of employer-sponsored group health plans, including UnitedHealthcare, some Blues plans, Cigna, and Aetna, have now begun informing plan sponsors that their data may have been disclosed as a result of the data breach. It is expected that more service providers will be notifying impacted plans in the future. The mailing process to affected individuals is expected to begin in late July. Change Healthcare has published a Payer list that reflects the parties that utilize Change Healthcare's services and could be impacted by the breach.

This data breach has far-ranging implications, from concerns around benefit plan claims payments to the unauthorized release of PHI. It is important that plan sponsors of impacted health plans understand the requirements and obligations that the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") places on "covered entities" in the event of a PHI breach. Covered entities are health plans, health care clearinghouses, and health care providers.

Background

HIPAA's privacy, security, and breach rules apply directly to "covered entities" and have strict requirements around the safeguarding of PHI. PHI is any personally identifiable health information that is created, received, maintained, or transmitted by a covered entity or its business associates. A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity.

Among the many requirements imposed by HIPAA, and of particular relevance here, are the obligations for a covered entity to:

- Maintain breach notification procedures;

- Obtain a signed business associate agreement with any business associate who may create, transmit, retain, or use the covered entity's PHI; and

- In the event of a PHI breach, provide certain notifications to impacted individuals, HHS, and in certain cases, the media.

In the event of a breach of PHI, covered entities must notify impacted individuals of the breach "without unreasonable delay" and, in any case, no later than 60 days after the breach is discovered. Where the breach occurred at a business associate, the business associate must also notify the covered entity without unreasonable delay and no later than 60 days after the breach is discovered.

In addition, the Office of Civil Rights ("OCR") must be notified by the covered entity of any PHI breach. If less than 500 individuals are impacted by the breach, OCR must be notified within 60 days following the end of the calendar year in which the breach occurred. If more than 500 individuals are affected, the covered entity must notify OCR at the same time that they notify impacted individuals. In addition, "prominent media outlets" in the state or region must be notified if more than 500 individuals are impacted in a single state.

HHS Guidance

HHS published guidance specifically addressing the Change Healthcare breach and the requirements under HIPAA applicable to covered entities.

The guidance confirmed that covered entities are permitted to delegate HIPAA's notification obligations to a third party (in this case, to Change Healthcare). Importantly, however, HHS emphasized that the responsibility to comply with these requirements ultimately remains with the covered entity. If a covered entity delegates these requirements to such a third party and the third party fails to comply with these requirements, the covered entity would ultimately be held responsible for the noncompliance.

The guidance also contained relief for covered entities related to the timing of notifications. HHS noted that as of the time of their most recent update (May 31, 2024), neither Change Healthcare nor UnitedHealth Group ("UHG") (who owns Change Healthcare) had filed a breach report with HHS or notified impacted individuals. HHS stated that the 60-day notification deadline does not begin to toll until affected entities are provided with necessary information by either Change Healthcare or UHG.

Employer Action

PHI breaches should always be taken seriously, especially where a breach has received as much attention and scrutiny as the Change Healthcare breach.

Fully insured plans: the covered entity with the reporting obligation is the carrier and should therefore be responsible for handling all notifications. Likewise, a provider is the covered entity with the reporting obligation. Employers may want to consider communicating to plan participants that they should expect a notice from the carrier.

Self-funded plans: the TPA is the business associate and the covered entity with the reporting obligation is the plan. Self-funded plans should consider the following:

- Await notification. TPAs are required to notify the covered entity if it was impacted by the Change Healthcare data breach. Many affected TPAs have begun the notification process (or will do so in the near future).

- Coordinate with Change Healthcare or their TPA as to which party will provide notice to impacted individuals, OCR, and media (where necessary).
  - While Change Healthcare has indicated it is willing to provide the necessary notifications, covered entities will need to determine whether they are comfortable relying on another entity since ultimate responsibility to comply rests with the covered entity.
  - Change Healthcare has set up a website that provides information about its anticipated notification procedures. Impacted plans should review this information when making the determination as to whether to delegate their notification responsibilities.
  - Plans should document whether they chose to delegate their notification requirements or not and their rationale.
  - If Change Healthcare is handling the notifications, employers should consider informing their plan participants that they should expect a notification in the future.