UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 OR 15(d)
of The Securities Exchange Act of 1934

Date of Report (Date of earliest event reported): June 27, 2026

AdaptHealth Corp.

(Exact name of registrant as specified in its charter)

Delaware	**001-38399**	**82-3677704**
(State or other jurisdiction of incorporation)	(Commission File Number)	(IRS Employer Identification No.)

555 East North Lane, Suite 5075 **Conshohocken, PA**	**19428**
(Address of principal executive offices)	(Zip Code)

(610) 424-4515

(Registrant's telephone number, including area code)

Not Applicable

(Former name or former address, if changed since last report.)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)
☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	**Trading Symbol(s)**	**Name of each exchange on which registered**
Common Stock, par value $0.0001 per share	**AHCO**	**The Nasdaq Stock Market LLC**

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Item 1.05 Material Cybersecurity Incidents.

AdaptHealth Corp. (the "Company") is investigating a security incident whereby a threat actor gained unauthorized access to Company systems and exfiltrated certain data therefrom. Upon learning of the incident, the Company promptly activated its incident response procedures, launched the investigation with the support of external advisors and cybersecurity experts to assess and contain the threat and notified law enforcement. While the investigation is ongoing, the Company has been able to confirm certain facts about the incident, and on June 27, 2026, the Company determined that the incident is material, due to the nature and potential volume of the data that is at risk.

Specifically, based on information obtained to date, the Company believes that a threat actor gained unauthorized access to certain of the Company's cloud-based business applications, including certain internal patient management systems and document storage platforms. On June 15, 2026, the Company received a communication from a threat actor claiming to have obtained certain data from the Company's systems. The Company has confirmed that certain data was exfiltrated from its systems including a stored password file associated with insurance billing; the Company also has confirmed that certain external electronic health record system portals were accessed by the threat actor.

The data affected includes passwords associated with insurance billing and certain personally identifiable information and protected health information of patients. **The Company does not collect Social Security numbers in the affected systems and does not store individual financial account information or payment card information in those systems.**

The incident was the result of a successful social engineering attack that compromised a user session associated with a third-party contractor. Following detection, the Company promptly implemented containment measures, including disabling the compromised user account, resetting affected credentials, and implementing additional access controls, and the incident has been contained. The Company is continuing to investigate the nature and scope of the incident with external forensics teams. The full scope of affected data sets has not yet been determined, and specific information regarding the volume of data at issue is not yet available. The Company has since taken steps intended to mitigate the risk of dissemination of the exfiltrated data.

As of the date of this Report, the incident has not had a material impact on the Company's operations and has not affected the Company's ability to service its patients. At this time, the Company is unable to determine the full financial impact of the incident, including remediation and response costs, legal, regulatory and notification-related matters, and possible effects on patients, counterparties and the Company's reputation. The Company maintains cybersecurity insurance that may cover certain losses associated with the incident.

To the extent any information required by Item 1.05 of Form 8-K was not determined or was unavailable at the time of this filing, the Company will amend this Current Report on Form 8-K as such information is determined or becomes available.

Forward-Looking Statements

This Current Report on Form 8-K contains statements that are not historical facts but are forward-looking statements for purposes of the safe harbor provisions under the United States Private Securities Litigation Reform Act of 1995. Forward-looking statements generally are accompanied by words such as "believe," "may," "will," "estimate," "continue," "anticipate," "intend," "expect," "should," "would," "plan," "predict," "potential," "seem," "seek," "future," "outlook," and similar expressions that predict or indicate future events or trends or that are not statements of historical matters. The forward-looking statements include, but are not limited to, statements regarding the Company's current beliefs, understanding, and expectations regarding the incident; statements regarding the nature and scope of the incident; the Company's ongoing assessment of the extent, categories and volume of data that was accessed or exfiltrated; the Company's ongoing efforts to assess and contain the threat, including the Company's assessment of whether there is any ongoing unauthorized access to its systems; the availability and adequacy of the Company's insurance coverage; and the potential impact of the incident on the Company's business, operations, financial condition and results of operations. These statements are based on current information, estimates and assumptions and are subject to known and unknown risks and uncertainties. Actual results may differ materially from those expressed or implied by these forward-looking statements. Factors that could cause actual results to differ from those expressed in these forward-looking statements include the ongoing assessment of the incident; the inability to determine the full scope of affected data sets and volume of data involved; the potential publication or misuse of affected data by the threat actor or other parties; legal, regulatory, reputational, and financial risks resulting from the incident or additional cybersecurity incidents; and the risks described in the Company's Annual Report on Form 10-K for the year ended December 31, 2025 and subsequent Quarterly Reports on Form 10-Q. Except as required by law, the Company undertakes no obligation to update these statements.

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, as amended, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

Dated: July 2, 2026

AdaptHealth Corp.

By: /s/ Richard Rew
Name: Richard Rew
Title: Chief Legal Officer, General Counsel and Secretary