UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, DC 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): **September 22, 2026**

ASTRANA HEALTH, INC.

(Exact Name of Registrant as Specified in Charter)

Delaware	**001-37392**	**95-4472349**
(State or Other Jurisdiction of Incorporation)	(Commission File Number)	(I.R.S. Employer Identification No.)

1668 S. Garfield Avenue, 2nd Floor, Alhambra, California 91801
(Address of Principal Executive Offices) (Zip Code)

(626) 282-0288
Registrant's Telephone Number, Including Area Code

(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, $0.001 par value per share	ASTH	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 Incident.

Astrana Health, Inc. (the "Company") recently became aware that its subsidiary Astrana Health Management, Inc. detected unusual activity within its environment.

The incident involved a series of social engineering attempts in which threat actors, impersonating Company personnel and spoofing the Company's main corporate telephone number, contacted certain employees in an effort to obtain unauthorized access to Company systems. The Company's cybersecurity team detected and responded to the unauthorized activity, launched an investigation, engaged a leading third-party cybersecurity and digital forensics firm, notified law enforcement, and is notifying state and federal regulators, and payer partners. The Company has also taken remedial measures, including resetting affected credentials, restricting remote access tools, restoring certain systems from clean backups, and enhancing monitoring, logging, and detection capabilities across its environment. The Company's investigation into the nature and scope of the incident, including the matters described above, remains ongoing.

Based on the current status of the Company's ongoing investigation, the Company believes that certain private and/or confidential information maintained on the Company's servers has been accessed and/or acquired without authorization.

The Company continues to assess whether, and to what extent, patient, employee, credentialed provider, confidential business and financial information, intellectual property, or other information may have been accessed, acquired, or exfiltrated and continues to evaluate the potential impact of the unauthorized activity. The Company continues to evaluate applicable regulatory and legal notification requirements, and the Company intends to make all required notifications based on its findings, including to impacted patients.

While the investigation is ongoing, the Company has determined that the incident is material as ofSeptember 22, 2026, due to the potential confidential and sensitive nature of the data that is involved.

However, the Company is, at this time, unable to estimate the full potential impact of the incident on the Company's business strategy, operations, financial condition, or results of operations, including remediation and response costs, legal, regulatory and notification-related matters, and possible effects on providers, patients, counterparties and the Company's reputation, or the impact on the trading price of the Company's common stock. The Company maintains cybersecurity insurance that may cover certain losses associated with the incident, although there can be no assurance that such coverage will be sufficient to cover all losses the Company may incur. Although the Company is unable to predict the full impact of this incident, the Company currently does not expect that it will have a material effect on the Company's financial condition and results of operations.

The trust of our valued providers, patients, and payer partners is deeply important to us, and we regret any concern or inconvenience this may cause.

To the extent any information required by Item 1.05(a) 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 forward-looking statements within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended. These statements include words such as "forecast," "guidance," "projects," "estimates," "anticipates," "believes," "expects," "intends," "may," "plans," "seeks," "should," or "will," or the negative of these words or similar words. Forward-looking statements involve certain risks and uncertainties, and actual results may differ materially from those discussed in each such statement. These forward-looking statements reflect current beliefs, understanding, and expectations regarding the incident, its impact on the Company, and its remediation and investigation. A number of important factors could cause actual results to differ materially from those included within or contemplated by the forward-looking statements, including, but not limited to, the ongoing assessment of the cybersecurity incident and analysis of the scope and details of the incident and the potential discovery of new and additional information related thereto; the Company's expectations regarding its ability to contain and remediate the cybersecurity incident, including the success of containment and remediation activities to date; any unauthorized release of the Company's data, including third-party data held by the Company, or the use of any such data for fraudulent purposes; potential loss or destruction of Company data or adverse impacts to the Company's operations; the impact of the cybersecurity incident on the Company's relationships with customers, employees, governmental regulators, and other stakeholders; diversion of management's attention from the Company's operations to address the cybersecurity incident; legal, regulatory, reputational, and financial risks resulting from the incident or any additional cybersecurity incidents, including those that may arise from any potential regulatory inquiries and/or litigation to which the Company may become subject in connection with the incident; other reputational risk related to the cybersecurity incident; regulatory scrutiny of the cybersecurity incident; risks related to the availability and adequacy of the Company's insurance coverage for losses and costs associated with the cybersecurity incident; remediation and other additional costs that may be incurred by the Company in connection with the investigation and remediation of the cybersecurity incident; and the factors described in the Company's filings with the Securities and Exchange Commission, including the Company's last Annual Report on Form 10-K and subsequent quarterly reports on Form 10-Q. The Company does not undertake any responsibility to update any of these factors or to announce publicly any revisions to any of the forward-looking statements contained in this or any other document, whether as a result of new information, future events, or otherwise, except as may be required by any applicable securities laws.

SIGNATURES

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

ASTRANA HEALTH, INC.

Date: September 23, 2026

By: /s/ Brandon K. Sim
Name: Brandon K. Sim
Title: Chief Executive Officer and President