CalOptima Health

Cybersecurity Update

Finance and Audit Committee Meeting
November 19, 2026

James Steele
Senior Director, Information Security

Our Mission

To serve member health with excellence and dignity, respecting the value and needs of each person.

Our Vision

Provide all members with access to care and supports to achieve optimal health and well-being through an equitable and high-quality health care system.

Agenda

- CalOptima Health has experienced 0 major* cybersecurity incidents
- CalOptima Health experienced 0 notable non-reportable cybersecurity incident
- CalOptima Health received 3 notable Third-party cybersecurity incidents
  - Astrana Health CYQ3
  - Papa CYQ4
  - Quest Diagnostics CYQ4

*A major cybersecurity incident is one that would require a regulatory disclosure or interrupts business operations.

Agenda

- Relevant Cybersecurity News
- Cybersecurity Metrics
- First 24-hours of an attack

CalOptima Health

Relevant Cybersecurity News

Quest Diagnostics Reports Cyberattack Affecting Laboratory Patient Records

Quest Diagnostics disclosed **unauthorized access to its Quanum Lab Services Manager platform, which healthcare organizations use to order laboratory tests and retrieve results**. Quest reported that certain patient records may have been accessed and engaged cybersecurity specialists to investigate. The scope of the exposure was still undetermined at the time of disclosure. Associated Press

Health Plan Vendor Exposes Information of More Than 238,000 Members

Denver Health Medical Plan disclosed a security incident involving **238,083 current and former members after an AI analytics vendor inadvertently exposed a database access key on a public website**. The key remained publicly accessible for more than a year and could have provided read-only access to sensitive member information, including eligibility records and health data. The health plan reported no evidence of misuse. HIPAA Journal

HHS Continues Ransomware Enforcement Against Healthcare Organizations

HHS OCR announced an **$800,000 settlement with Lehigh Valley Health Network following a ransomware attack that exposed protected health information belonging to 248,359 individuals**. The investigation identified potential failures involving HIPAA risk analysis, regular review of system activity, and breach notification requirements. The organization also agreed to a three-year corrective action plan. HHS

CalOptima Health

Cybersecurity Metrics for CY26 Q3

Reportable Major Cybersecurity Incidents	Cybersecurity Incidents	CY26 Q3	Last 12M
0	Third party cybersecurity notifications	6	42
	Non-reportable cybersecurity incidents	0	1
	Data loss prevention escalations	3	19
	Cybersecurity Tools	**CY26 Q3**	**Last 12M**
	Total Email Received	1.77 M	24.06 M
	% of total emails blocked due to malicious content	66%	68%
	Phishing websites blocked	40	497
	Malicious applications blocked	354	4,465

Asset Type	Total
Workstations	2,146
Servers	539
Other systems	3,185
Network Device	154

Risk Register	Open*
Critical Findings	0
High Findings	2
Med Findings	1
Low Findings	5

Patching Management	Goal	Jul-26	Aug-26	Sep-26
Servers - Patching	>95%	99%	99%	98%
Workstations - Patching	>95%	97%	95%	97%

Security Awareness	Goal	Jul-26	Aug-26	Sep-26
Monthly Security Awareness Training	85%	98%	98%	97%

* Workstreams in process for open items

CalOptima Health

First 24-hours of an attack

7:30 AM: A cyberattack is discovered

The response team detects suspicious activity involving member-facing and internal systems.

WHAT WE KNOW

- **Possible ransomware activity**
  Multiple systems show indicators of compromise.
- **Potential exposure of member information**
  The scope is unknown and requires investigation.

THE IMMEDIATE DILEMMA

Contain the attack

while preserving critical member and provider services.

Early decisions must balance cybersecurity containment with continuity of care.

CalOptima Health

Contain. Coordinate. Stabilize.

Illustrative phases, not fixed deadlines. Workstreams often run in parallel.

0–4 HOURS

Investigate & contain

- Confirm suspicious activity
- Isolate affected systems
- Activate incident command
- Assess critical service impacts

4–12 HOURS

Coordinate & sustain

- Determine scope and dependencies
- Activate business continuity plans
- Engage Legal, Privacy and partners
- Coordinate executive updates

12–24 HOURS

Plan safe recovery

- Prioritize critical service restoration
- Assess possible data exposure
- Evaluate notification obligations
- Report validated status and risks

24 hours is a decision window, not a guarantee of full recovery.

CalOptima Health

What should the Board do in a crisis?

Management directs the incident response. The Board provides oversight and accountability.

MANAGEMENT LEADS

- Containment and investigation
- Continuity of member and provider services
- Recovery and external coordination
- Regulatory and stakeholder communications

BOARD OVERSIGHT

- Adequacy of resources and preparedness
- Receive updates when material thresholds are met
- Evaluate preparedness through routine oversight
- Review significant lessons and improvements afterward

How would we know that the organization is prepared before an attack?

CalOptima Health

CalOptima Health

Stay Connected With Us

www.caloptima.org