As of December 15, 2025

General FAQs:

Allegiance – HCI cyber event

---

1. What happened?
Allegiance's vendor, HCIactive (HCI) discovered unauthorized parties accessed and/or acquired files containing information pertaining to Allegiance members. The incident occurred between approximately July 8, 2025, and July 12, 2025. Upon learning of this, HCI took containment action by taking all systems offline and hired a third-party forensics firm to perform an investigation. This incident occurred on HCI's systems and did not impact or threaten any Allegiance systems.

2. Has the issue been resolved?
Yes. On August 5, 2025, an independent forensic firm confirmed HCI's environment was secure. Allegiance resumed data feeds the same day.

3. Was any data compromised?
HCI has confirmed the threat actors were able to exfiltrate some client data.

4. What information was potentially disclosed?
HCI confirmed information impacted varies by individual but may include names, contact information, dates of birth, claim information and Social Security Numbers (SSN).

5. Will Credit monitoring be provided to impacted individuals?
HCI will be offering credit monitoring to impacted customers. The standard duration of credit monitoring is 12 months. Where required by law (CA, CT, DE, MA and PA) residents will receive 24 months of credit monitoring.

6. How will customers be notified if their data was impacted?
HCI is prepared to issue notifications and offer credit monitoring services directly to affected individuals, in accordance with applicable state and federal laws. Allegiance notes that clients generally prefer to have the vendor send notifications on their behalf.

7. Did HCI notify the FBI?
The Federal Bureau of Investigation was notified of the incident, and Allegiance is cooperating with its investigation into this incident. Local Howard County Police were also notified of the incident.

8. Have you identified the threat actor?
The threat actor group claiming responsibility is Pure Extortion Ransomware Team, which according to law enforcement and the third-party cybersecurity consultants, appears to be a new ransomware group.

9. Was a third party engaged for forensics? If yes, which one?
Yes, HCI's external counsel engaged At-Bay Security to perform an investigation into this matter.

10. What are some of the steps taken by HCI to remediate and prevent future security incidents?

HCI moved quickly to secure their systems and reduce further risk by taking the following steps:

- Rebuilt affected systems
- Strengthened security settings
- Restricted access to sensitive systems and enforced secure sign-ins
- Deployed advanced monitoring tools to detect and stop threats

11. What was the high-level incident timeline?

Allegiance was informed on August 1, 2025, by HCI of an incident involving unauthorized access to its systems; however, the impact was unknown at that time. On the same day, Allegiance temporarily disconnected from vendor HCI due to unusual activity affecting HCI's network security. While the AskAllegiance portal remained accessible, data was not refreshed during this time.