Keeping Member Data Secure

Ensuring Trust and Security to Protect Data for Health Plans and Their Members

Data security is crucial for health plans to protect sensitive patient information and ensure compliance with regulatory requirements. Trust is essential when sharing member data with technology vendors, because health plans must rely on partners to maintain the same high standards of data protection.

The CAQH Coordination of Benefits (COB) Solution and the Member Data Portal employs stringent security protocols to safeguard sensitive data, including end-to-end encryption, multifactor authentication, and single sign-on.

A Three-pronged Approach to Protecting Data

1 Administrative Security

- **Security and Privacy Policies:** Guided by the CAQH Oversight Committee.
- **Employee Training:** Frequent mandatory data security training for all CAQH employees.
- **Third-Party Assessments:** Regular SOC2 audits and HITRUST Certification to ensure compliance.

2 Physical Security

- **Separate Environments:** Distinct production and testing environments to prevent data breaches.
- **Data Archive Process:** Data that is older than six months is removed from the production environment.
- **Role-Based Access Controls:** CAQH COB Solution and Member Data Portal access based on job roles via the principle of least-privilege.
- **Network Protection:** Comprehensive strategies to secure network and infrastructure. Secure, non-deprecated protocols and ciphers suites are only used to ensure secure connectivity.

3 Technical Security

- **SFTP and PGP Data Encryption:** Sensitive member data is encrypted at rest, in transit, and during storage.
- **Multifactor Authentication (MFA) and Single Sign-On (SSO):** Secure remote logins and streamlined end-user access to the Member Data Portal.
- **Access Control:** CAQH data access is restricted on a need-to-know basis.
- **Device Encryption:** CAQH laptops and workstations are encrypted.
- **Enterprise Protection:** CAQH antivirus, firewall, and monitoring systems safeguard devices.
- **Regular Assessments:** Frequent vulnerability scanning, and penetration testing conducted by the CAQH information security team to identify and mitigate potential threats.

Data security and cyber resiliency are critical components of the CAQH COB Solution and Member Data Portal. Policies and security measures are continually evaluated and updated to protect health plans, members, and all data partners

To learn more about how our data solutions drive better outcomes, visit **CAQH.org**.