Privacy and Data Security

Our business is based on the trust of our members, states and industry health partners. They trust us to handle their most sensitive and private information in a secure and professional manner. We are committed to satisfying state and federal laws protecting the privacy and confidentiality of our members information and to continuously enhancing and strengthening our technology and security protocols.

- Molina's security and privacy policies align with best practice industry and regulatory frameworks such Health Information Portability Accountability Act (HIPAA) and National Institute Standards and Technology (NIST) 800-53 cyber security standard. Control procedures are assessed regularly to confirm their effectiveness; Ernst and Young performs an annual Service Organization Controls (SOC) II Type 2 attestation report covering the performance of safeguards deployed to protect our systems and members private data.
- Molina is conscious of the potential damage to the health industry associated with cyberattacks and we take our role seriously. Molina has implemented the following best practices outlined in President Biden's Executive Order on Improving the Nation's Cybersecurity:
  - Dedicated Chief Information Security Officer (Security Official) and Vice President, Compliance & Privacy Official
  - Modernized IT systems such as Microsoft Azure Cloud
  - Safeguards such as multi-factor authentication and encryption of sensitive data
  - Secure backups and recovery practices
  - Molina patches systems on a timely basis
  - Lateral movement controls such as network segmentation
- Molina hires experienced security professionals to conduct advanced and realistic cybersecurity attack simulations to verify our cybersecurity and privacy programs.
- Molina's Computer Incident Response Team (CIRT) monitors systems for any threats to Molina Healthcare's information systems. The team handles any security issues, ensuring the company's systems are not compromised. An Incident Response Plan is maintained and regularly tested with executive management and various departments participating to simulate their response to a cybersecurity incident.
- Employees are trained on their privacy and security policy obligations annually. Given the risks associated with email phishing attacks, employees are tested each month to identify a fake phish email to reinforce continued diligence.

MOLINA® HEALTHCARE