

Express Scripts Security Fact Sheet

For protection of sensitive information, including personal health information and personally identifiable information of members, Express Scripts utilizes multiple safeguards.

Express Scripts Tightly Controls Access Points to Our Network

- Express Scripts utilizes commercial firewalls and router Access Control Lists at all public network access points to appropriately restrict network traffic.
- Express Scripts' internal network address space is not advertised to the Internet and all outside requests for information are blocked.
- Commercial Network Intrusion Detection Systems are in place to monitor inbound/outbound traffic for attack patterns and to alert security personnel when appropriate.
- Express Scripts conducts regular vulnerability scans against its Internet points of presence to ensure no vulnerabilities exist.
- Vulnerability scans are also conducted monthly by ESI's Payment Card Industry auditor. ESI is also audited annually by the U.S. Department of Defense against the DoD Information Assurance Certification and Accreditation Process (DIACAP) to ensure that we conform to their security requirements for the protection of member information.

Internet Accessible Systems are Isolated

- ESI's Internet-accessible systems have hardened operating systems and are located in a firewall protected DMZ, which means it is isolated from both the Internet and Express Scripts' internal network.
- In addition, commercial Host Intrusion Detection Software has been deployed on the DMZ systems as an additional measure.
- An additional layer of commercial firewalls separates Express Scripts' Web Portal DMZ from the internal network.

Express Scripts Utilizes Strong Encryption

- Express Scripts utilizes SSL 128-bit encryption for Web session security.
- For all portals, data access is authenticated and authorized.
- Express Scripts also utilizes digital certificates for client-side authentication and authorization to perform business and other transactions with our systems via the Internet

Other Tools We Use

- Inside its internal network, Express Scripts utilizes a variety of tools and methods for additional protection.
- Internal systems are regularly scanned utilizing commercial tools to identify potential security vulnerabilities, which are then addressed.
- Security software patches are applied on a regular basis to all platforms after evaluation and testing.
- Authentication and authorization controls are in place at the platform and application to limit data access to authorized users.
- All ESI workstations have current antivirus protection and are kept up-to-date with security patches.
- All ESI laptop computers have encrypted hard drives.

Data Center Maintains Rigorous Security

- Electronic Data Systems (EDS) is responsible for Express Scripts' data center operations and has established rigorous procedures to safeguard the security of the computer equipment and operating environment.
- The operations center is located on a physically secure, controlled-access campus and is equipped with proximity detector systems, key locks, and video cameras at all building entrances and exits.
- Strict identification and access protocols are in place for employees and visitors, and the facilities are monitored 24 hours a day.

We Also Maintain Strict Physical Security Procedures

- Express Scripts' facilities have strict identification and access protocols for employees and visitors.
- Facilities are monitored 24 hours a day and employees are required to visibly display their access badge.
- In addition to the technical controls, Express Scripts maintains a comprehensive set of corporate security policies which guide its security efforts and which are communicated to the Express Scripts user community.
- The Express Scripts user community is required to sign an acknowledgment of their security responsibilities on an annual basis. They have also passed background checks as a condition of employment.

We Take Our Security Responsibilities Seriously

- At Express Scripts, we take the security of our client and member data very seriously.
- We are actively participating in the development of an industry standard security framework for the protection of sensitive healthcare information through the HITRUST Alliance (<http://www.hitrustalliance.org>) to assist us in the protection of our members' information.