Firewall Requirements for PCI Compliance

Having *any* firewall is not enough to make your pharmacy PCI compliant

Achieving PCI DSS compliance requires the ***deployment of specific security technology, expert configuration, and the performance of ongoing technical tasks.***

McKesson developed the Secure Cloud Gateway (SCG) managed security option through a partnership with data security experts, ANX. PCI Compliance Assistance Services makes it easier for pharmacies to become PCI compliant if they lack the security technology, expertise, and resources to do it themselves.

Is the McKesson SCG option required to meet your PCI compliance requirements?

No. With an investment of time and technology, you can become compliant on their own. However, if you decide to handle PCI compliance yourself or partner with another vendor, be sure that you meet all pertinent technical and process requirements for firewall, intrusion detection, wireless, remote access, and internal and external scanning. McKesson developed the PCI Compliance Assistance Services to better support the needs of pharmacies that want to focus their energy on running the business and not on security and compliance.

PCI DSS SAQ Section	Partial List of Firewall and Security Technology Related PCI Requirements	McKesson SCG Option
1.1	Establish firewall and router configuration standards that formalize testing whenever configurations change; that identify all connections to cardholder data (including wireless); that use various technical settings for each implementation; and that stipulate a review of configuration rule sets at least every six months.	Provided
1.2	Build firewall and router configurations that restrict traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.	Provided
1.3	Prohibit direct public acess between the Internet and any system component in the cardholder data environment.	Provided
1.3.6	Firewall must have stateful inspection, also known as dynamic packet filtering.	Provided
8.3	Implement two-factor authentication for remote access to the network by employees, administrators, and third parties.	Provided
11.1	Test for the presense of wireless access points and detect unauthorized wireless access points on a quarterly basis.	Provided
11.2	Run internal and external vulnerability scans at least quarterly and after any significant change in the network.	Provided
11.2.1 (b)	Quarterly internal scan process must include rescans until passing results are obtained, or until all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.	Provided
11.2.1 (c)	Internal quarterly scans must be performed by a qualified internal resource(s) or qualified external third party.	Provided
11.4	Use network intrusion detection systems and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date.	Provided

The PCI Compliance Assistance Services address these and many other technical requirements of the PCI Self-Assessment Questionnaire. Having an SCG can automatically answer up to 50% of the questions.

Visit www.McKessonPCI.com or call 877.477.8269 Option 4 for help and resources