Cloud Security

(800) 825-0224
advancedmd.com

SECURITY WITHOUT COMPROMISE.

ENSURE THE CONFIDENTIALITY, INTEGRITY & AVAILABILITY OF ALL DATA IN YOUR POSSESSION.

Run your practice with confidence of your data security. All AdvancedMD applications, information and records are stored in our managed cloud environment, giving you more freedom and security than what is possible with application service providers (ASP) and on-premises, client-server software applications. All our systems are scrutinized and safeguarded using the highest standards in security and encryption.

AdvancedMD offers free 2FA as an optional service to give you an extra layer of security that works in conjunction with the username and password by adding a second security code to your login verification that only you can access (such as receiving the code in your email account). We also offer a 2FA security code via an authenticator app on your smartphone.

We employ multiple layers of technical safeguards in our security. These include hardened network and operating systems, DMZs (multi-tiered firewalls and routers), intrusion detection systems (IDS), deep packet inspection (DPI) technologies, system policy and configuration management solutions, data loss prevention (DLP) technologies, secure, encrypted electronic communications, access, utilization, audit and event monitoring, logging and trend correlation, encryption of all transmitted information, network and application vulnerability scanning, application penetration testing, technical security assessments (internally and by 3rd parties), identity management, virus protection, and technical security training and awareness.

Technical Safeguards.

We employ multiple layers of technical safeguards in our security. These include hardened network and operating systems, DMZs (multi-tiered firewalls and routers), intrusion detection systems (IDS), deep packet inspection (DPI) technologies, system policy and configuration management solutions, data loss prevention (DLP) technologies, secure, encrypted electronic communications, access, utilization, audit and event monitoring, logging and trend correlation, encryption of all transmitted information, network and application vulnerability scanning, application penetration testing, technical security assessments (internally and by 3rd parties), identity management, virus protection, and technical security training and awareness.

Annual Risk Assessment.

Risk assessments are conducted at least yearly on the AdvancedMD infrastructure, business processes and other areas where ePHI could be disclosed. Findings from such assessments are used to make risk management decisions on how to reduce risk to an acceptable level. Risk assessment processes focus on areas of the business and technology operations where ePHI may be vulnerable to unauthorized access, disclosure, destruction or other loss of confidentiality, integrity or availability.

Results from risk assessments are grouped into findings that are then classified and categorized by level of risk. The determination of risk takes into account the information gathered and determinations made by analyzing the likelihood of a threat and the resulting impacts of a threat. Findings are then grouped into risk issues and are documented and tracked through to an acceptable remediation.

Business Continuity & Disaster Recovery.

AdvancedMD business continuity and disaster recovery programs include electronic hourly backups of all client data to offsite locations, backup verifications to ensure the integrity and recoverability of back up data, server clustering and redundant systems to the extent feasible, detailed business impact analysis and recovery strategies, crisis and incident command structures, BCP and DR plan testing and exercising, and emergency notification systems.

AdvancedMD