MedMal DIRECT
Insuring a Healthy Practice

COMPREHENSIVE CYBERSECURITY CHECKLIST

SECURITY MEASURE	DESCRIPTION	IN PLACE	PLANNED DATE	COST
Hardware Inventory & Tracking	Inventory tagging of all IT equipment and logging.			
Software Inventory	List of all software with versions used.			
Managed Professional Anti-Virus	Professional grade anti-virus.			
Monthly Patching with Report	Review to ensure all security patches are applied.			
Monitored Network	Real-time review of network activity and network.			
Development of Security Profiles	Security settings for equipment.			
Disabling of USB Drives	Disabling of USB drives to prevent unauthorized downloads or uploads of data.			
Admin Privileges to Install Software	Disable ability for staff to install software.			
Business Grade Firewall	Professional grade firewall. SonicWALL TZ210 or better.			
Intrusion Detection & Prevention	Software to defend against known attacks on firewall.			
Penetration Reporting	Review of intrusion attempts.			
Unified Threat Management Device	Added security device to prevent malware.			
Domain Controller	Server used to control security settings on workstations and ability to add Terminal Services.			
File Integrity Checking Tools	Tools used to make sure files have not been altered.			
Network Hardening with Report Server	Removal of unnecessary services, changing of default passwords, and additional measures to secure devices.			
Firewall				
Quarterly Security Reviews	To prevent “decay” of Hardening Process			
Training	Yearly HIPAA Security Rule training required.			
Web Content Filtering	Restricting access to web sites.			
Blacklist / Whitelist	Restricting or granting access to web sites.			
Spam Filtering	Additional scanning of emails and attachments			
Data Backup with Monitoring	On-Site			
Data Backup with Monitoring	Off-Site			
Audit Log Monitoring	User activity monitored for unusual or suspicious activity.			
Server/Firewall/EHR				
Controlled Access	User privileges, restriction of administrative accounts			
Two Factor Authentication	Using two factors to identify an individual.			
Encryption - Server	Special method of locking files that turns text into cyber text.			
Encryption - Workstations				
Encryption - Backup				
Encryption – Mobile Devices				
Vulnerability Scanning	Internal scans to determine known vulnerabilities.			
Penetration Testing	Review network security from outside the network.			
Remediation of Results	Update system after vulnerability and penetration scans.			
Follow-Up Scanning & Testing	Re-scan network to ensure updates in place & working.			

MedMal Direct Insurance Company
76 South Laura Street - Suite 900 - Jacksonville, FL 32202
RiskManagement@MedMalDirect.com - MedMalDirect.com