MedMal DIRECT
Insuring a Healthy Practice

THE HIPAA SECURITY RULE

SECURITY STANDARDS MATRIX (APPENDIX A OF THE SECURITY RULE)

ADMINISTRATIVE SAFEGUARDS			
STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS (R) = Required (A) = Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)		
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Health Care Clearing Functions	(R)
		Access Authorization	(A)
		Access Establishment & Modification	(A)
Security Awareness & Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedures	(A)
		Application and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)		
Business Contracts & Other Arrangements	164.308(b)(1)	Written Contract / Other Arrangement	(R)
PHYSICAL SAFEGUARDS			
STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS (R) = Required (A) = Addressable	
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control & Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)		
Workstation Security	164.310(c)		
Device and Media Controls	164.310(d)(1)	Disposal	(R)
		Media Re-Use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

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

MedMal DIRECT
Insuring a Healthy Practice

THE HIPAA SECURITY RULE

TECHNICAL SAFEGUARDS			
STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS (R) = Required (A) = Addressable	
Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	164.312(b)		
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person to Entity	164.312(d)		
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)
ORGANIZATIONAL REQUIREMENTS			
STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS (R) = Required (A) = Addressable	
Business Contracts or Other Arrangements	164.314(a)(1)	Business Associate Contracts	(R)
		Other Arrangements	(R)
Requirements for Group Health Plans	164.314(b)(1)	Implementation Specifications	(R)
POLICIES, PROCEDURES & DOCUMENTATION REQUIREMENTS			
STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS (R) = Required (A) = Addressable	
Policies and Procedures	164.316(a)		
Documentation	164.316(b)(1)	Time Limit	(R)
		Availability	(R)
		Updated	(R)