UDOH HIPAA Security Policies

Policy #	Type	Policy Title
13.01	Security	Information Security Strategy
13.02	Security	Security Management Process
13.03	Security	Risk Analysis & Risk Management
13.04	Security	HIPAA Security Oversight
13.05	Security	Information System Activity Review
13.06	Security	Workforce Security
13.07	Security	System Access
13.08	Security	Information Access Management
13.09	Security	Security Reminders
13.10	Security	Protection from Malicious Software
13.11	Security	Log-In Monitoring
13.12	Security	Security Incident Procedures
13.13	Security	Response and Reporting
13.14	Security	Contingency Plan
13.15	Security	Data Backup Plan
13.16	Security	Disaster Recovery Plan
13.17	Security	Emergency Mode Operation Plan
13.18	Security	Testing and Revision Procedures
13.19	Security	Applications and Data Criticality Analysis
13.20	Security	Evaluation
13.21	Security	Business Associate Agreements
13.22	Security	Facility Access
13.23	Security	Contingency Operations
13.24	Security	Facility Security Plan
13.25	Security	Access Control and Validation Procedures
13.26	Security	Maintenance Records
13.27	Security	Device and Media Controls
13.28	Security	Destruction, Disposal, and Reuse of PHI Media
13.29	Security	Accountability
13.30	Security	Data Backup and Storage
13.31	Security	Access Control
13.32	Security	Emergency Access Procedure
13.33	Security	Encryption and Decryption Policy
13.34	Security	Audit Controls
13.35	Security	Integrity
13.36	Security	Mechanism to Authenticate Sensitive Information
13.37	Security	Transmission Security
13.38	Security	Integrity Controls
13.39	Security	Encryption
13.40	Security	Policies and Procedures Standard
13.41	Security	Documentation Standard
13.42	Security	Information Classification
13.43	Security	Network Security

13.44	Security	Email Security
13.45	Security	Remote Access
13.46	Security	Portable Devices
13.47	Security	VPN
13.48	Security	Wireless Security
13.49	Security	Wireless IP Phones
13.50	Security	Social Media Policy
13.51	Security	Cell Phone and Smartphone Policy