

HIPAA SECURITY TABLE OF CONTENTS
Part 1. General Security
1.1 – General Security Controls Policy
Part 2. Administrative Safeguards
2.1 - Security Management Process
2.2 - Risk Analysis & Assessment
2.3 – Risk Management
2.4 – Sanctions
2.5 – Information System Activity Review
2.6 – Security Officer
2.7 – Workforce Authorization
2.8 – Workforce Clearance
2.9 – Workforce Termination
2.10 – Information Access Management
2.11 – Security Awareness and Training
2.12 – Security Reminders
2.13 – Protection from Malicious Software
2.14 – Log-In Monitoring
2.15 – Password Management
2.16 – Security Incident Procedure - Response and Reporting
2.17 – Contingency Plan Overview
2.18 – Data Backup Plan
2.19 – Disaster Recovery Plan
2.20 – Emergency Mode Operation Plan
2.21 – Testing and Revision Procedures
2.22 – Applications and Data Critical Analysis
2.23 – Evaluation
2.24 – Business Associate Contracts/Written or Other Arrangement
Part 3. Physical Safeguards
3.1 – Facility Access Controls
3.2 – Contingency Operations
3.3 – Facility Security Plan
3.4 – Access Control and Validation Procedure
3.5– Maintenance Records
3.6– Workstation Use
3.7 – Workstation Security
3.8 – Device and Media Controls
3.9 – Device and Media Disposal
3.10 – Device and Media Controls – Media Re-use
3.11 – Device and Media Controls - Accountability
3.12 – Device and Media Controls – Data Backup and Storage
Part 4. Technical Safeguards
4.1 – Access Control - Unique User Identification
4.2 – Access Control - Emergency Access Procedure
4.3 – Access Control - Automatic Logoff
4.4 – Access Control - Encryption and Decryption
4.5 – Audit Controls
4.6 – Integrity - Authenticate Electronic Information
4.7 – Person or Entity Authentication
4.8 – Transmission Security - General, Integrity Controls, Encryption

Part 5. Organizational Requirements
5.1 – Business Associate Contracts
Part 6. Documentation Requirements
6.1 – Policies & Procedures, Time Limit, Availability and Updates
Part 7. Logs, Forms, Schedules (Separate Binder)
1. Access to PHI Log: See Privacy Manual
2. Detailed Systems Configurations / Log
3. Training Attendance Log: See Privacy Manual
4. Access Termination Form
5. Audit Controls Checklist
6. Business Associate Database Log
7. Back Up and Password Policy Log
8. Device Malfunction / Work Order Log
9. Disaster Procedures Form
10. Emergency Call List
11. Emergency Plan Test
12. Facility Maintenance and Repair Record
13. Hardware Control Log
14. Hardware / Software Relocation Log
15. Incident Report Form - Security
16. Media Destruction, Disposal, & Re-use Form
17. User Name and Password Control Log
18. Security Access Request / Authorization Form
19. Security and Confidentiality Acknowledgement
20. Software Control Log
21. User Identification Form
22. Vendor Contact Form
23. Visitors Log