DATABANK
Data Center Evolved™

# HIPAA HOSTING CHECKLIST

Pivotal Elements for Protecting the Security and Privacy of Electronic Protected Health Information (ePHI)

## PHYSICAL ACCESS CONTROLS

### Facility Access Controls

- Restricted Parking/Premises
- Restricted Access to the Facility
- Signs for Data Center Identification
- Guard or Attendant at Entrance
- Valid Government Photo ID for Visitors
- Sign-in/Sign-out Process
- Restricted Access Signage
- Escort Policy Required for Visitors and Vendors

### Data Center Access Controls

- Restricted Access to the Data Center
- Biometric Access Requirement
- Unique Access ID for Each Employee
- Process For Granting/ Revoking Access
- Reconciliation of Staff with Access

### Data Center Access and Monitoring

- Monitoring of Access
- Digital Log of Door Accesses
- Electronic Visitor Logs
- Camera Placement at All Door Access Points, Aisles, and Cages

### Data protection

- Shredder Availability (Not applicable to Colo or Managed services environment)
- Server/Comm Cabinets Secured
- Network Cables and Sockets Secured

## LOGICAL ACCESS CONTROLS

### Data Protection (continued)

- Complete Separation Between Each Customer Environment
- Separate & Defined Server Roles
- Access Control and Logging for All Access to Servers with ePHI
- Firewall Between Public/ Private Zones
- Production Change Management
- Incident/Problem Management Program
- Security Incident Response Plan
- Risk Management

### Documented Policies/Controls

- Access Control
- Password Management
- Firewalls
- Virus Protection
- Data Classification
- Encryption
- Retention
- Destruction

## NETWORK ACCESS CONTROLS

### Firewall

- Dedicated Firewall for Every Environment
- Cisco ASA Firewalls
- Firewall Redundancy
- VPN Tunnels
- Remote Access
- Dual Factor Authentication
- IPSEC Tunnels
- INGRESS and EGRESS Filters

### Network

- Private VLAN
- DMZ Zone for Public Services
- Internal Zone for Private Server

### Intrusion Prevention

- Intrusion Prevention Service (IPS)
- Prevention of “Phone Home Bots”
- DDoS Mitigation (optional)
- Offload of SSL Traffic
- Web Application Firewalls for OWASP 10

### Enterprise: Anti-virus

- Enterprise-Grade Anti-Virus
- Host-Based Intrusion Prevention
- Centralized Reporting
- Abnormal Process Logging

## MANAGED HOSTING

### Business Checklist

- Will Sign a HIPAA BAA
- Utilize Data Encryption (optional)
- Cyber Insurance Coverage
- Onsite and Offsite Backups
- Vulnerability Management and Logging
- Security, Incident, Training, and HR Policies
- SSAE 18 SOC 2 Type II
- Audit Support (1 Hr Annually)
- All Staff Trained in HIPAA
- Security Awareness Training

### Managed Hosting Checklist

- Monitoring
- Patching
- Backups
- Recovery
- Security
- 24/7 Tech Support
- Customer Portal