HIPAA Security Checklist for Healthcare Providers - Self-Evaluation Checklist

Individual Authentication of Users	Doing it Now	In the future	Not Needed	Too Expensive	Does not Apply	Don't Know
Unique individual identifier for each user	_____	_____	_____	_____	_____	_____
Automatic logoff after specified time	_____	_____	_____	_____	_____	_____
Change passwords often (enforced by system)	_____	_____	_____	_____	_____	_____
System generates random password	_____	_____	_____	_____	_____	_____
Weak passwords not allowable	_____	_____	_____	_____	_____	_____
System stores password encrypted	_____	_____	_____	_____	_____	_____
Uniform User ID across organization	_____	_____	_____	_____	_____	_____
Incentives to reduce key account sharing	_____	_____	_____	_____	_____	_____
Single-use or token based passwords	_____	_____	_____	_____	_____	_____
Token card plus password or PIN	_____	_____	_____	_____	_____	_____
Biometric (fingerprint, retinal scan, etc.)	_____	_____	_____	_____	_____	_____
Caller-ID verification of remote location	_____	_____	_____	_____	_____	_____
Telephone callback for remote users	_____	_____	_____	_____	_____	_____
Different security for terminals in different locations	_____	_____	_____	_____	_____	_____
Comply with Orange Book C2 or better	_____	_____	_____	_____	_____	_____
Account canceled when employee leaves	_____	_____	_____	_____	_____	_____
Emergency access procedures for forgotten password	_____	_____	_____	_____	_____	_____
Policies and procedures in place for Authentication	_____	_____	_____	_____	_____	_____
Policies and procedures strictly enforced (even fines)	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____

Access Controls	Doing it Now	In the future	Not Needed	Too Expensive	Does not Apply	Don't Know
Access control list for each file or database	_____	_____	_____	_____	_____	_____
Access control lists UserID based	_____	_____	_____	_____	_____	_____
Role based access profiles	_____	_____	_____	_____	_____	_____
Access overrides for emergencies	_____	_____	_____	_____	_____	_____

Simple access control (All or nothing)	_____	_____	_____	_____	_____	_____
Gross granularity control (Screen based, or application based)	_____	_____	_____	_____	_____	_____
Medium granularity control (Record based, or role based algorithm)	_____	_____	_____	_____	_____	_____
Fine granularity control (Field based, or UserID based algorithm)	_____	_____	_____	_____	_____	_____
Multiple parameters (e.g. UserID, role, physical location, function, etc.)	_____	_____	_____	_____	_____	_____
Policies and procedures in place for Access Control, and to determine legitimate need	_____	_____	_____	_____	_____	_____
Policies and procedures strictly enforced (even fines)	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____

Monitoring of Access	Doing it Now	In the future	Not Needed	Too Expensive	Does not Apply	Don't Know
System imposed audit trails	_____	_____	_____	_____	_____	_____
Software controlled audit trails	_____	_____	_____	_____	_____	_____
Transaction log audit trail	_____	_____	_____	_____	_____	_____
File level audit trail	_____	_____	_____	_____	_____	_____
Record level audit trail	_____	_____	_____	_____	_____	_____
Field level audit trail	_____	_____	_____	_____	_____	_____
Write or change data audit trail	_____	_____	_____	_____	_____	_____
Read, display, print data audit trail	_____	_____	_____	_____	_____	_____
Automatic display of "last access" to the next user, to allow self-audit by all users.	_____	_____	_____	_____	_____	_____
Periodic management reports of exceptions	_____	_____	_____	_____	_____	_____
Periodic management reports of all access	_____	_____	_____	_____	_____	_____
Internal periodic audit of audit trails	_____	_____	_____	_____	_____	_____
Policies and procedures in place for Access Monitoring, to detect misuse and violations	_____	_____	_____	_____	_____	_____
Policies and procedures strictly enforced (even fines	_____	_____	_____	_____	_____	_____
External/independent audit of audit trails	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____

Other:_____	_____	_____	_____	_____	_____	_____

Physical Security and Disaster Recovery	Doing it New	In the future	Not Needed	Too Expensive	Does not Apply	Don't Know
Secure computer room	_____	_____	_____	_____	_____	_____
Secure access to displays and printers	_____	_____	_____	_____	_____	_____
Network security, no external network access	_____	_____	_____	_____	_____	_____
Secure destruction of printouts, floppies, etc.	_____	_____	_____	_____	_____	_____
Secure destruction of obsolete equipment	_____	_____	_____	_____	_____	_____
Burglar alarm monitored by Police	_____	_____	_____	_____	_____	_____
Secure backup, storage and retrieval	_____	_____	_____	_____	_____	_____
Multiple backup storage sites	_____	_____	_____	_____	_____	_____
Disaster recovery plan in place	_____	_____	_____	_____	_____	_____
Disaster recovery plan periodically tested	_____	_____	_____	_____	_____	_____
Emergency data access assured in case of disaster	_____	_____	_____	_____	_____	_____
Data content integrity assured	_____	_____	_____	_____	_____	_____
Operations recoverability	_____	_____	_____	_____	_____	_____
Non-disruption of critical functions	_____	_____	_____	_____	_____	_____
Policies and procedures in place for Physical Security and Disaster Recovery	_____	_____	_____	_____	_____	_____
Policies and procedures strictly enforced (even fines)	_____	_____	_____	_____	_____	_____
Security maintained 100% in disaster recovery mode	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____

Protection of Remote Access Points and Protection of External Electronic Communications	Doing it Now	In the future	Not Needed	Too Expensive	Does not Apply	Don't Know
Firewall for Internet access	_____	_____	_____	_____	_____	_____
Encrypted Virtual Network for Internet users	_____	_____	_____	_____	_____	_____
Limit use of the Internet to USA remote sites	_____	_____	_____	_____	_____	_____

Healthcare data available to external network	_____	_____	_____	_____	_____	_____
Strong encryption required for Internet and Extranet users	_____	_____	_____	_____	_____	_____
Authentication and Digital signatures required for Internet and Extranet users	_____	_____	_____	_____	_____	_____
Dial-in protections (e.g. Caller-ID, callback, encryption)	_____	_____	_____	_____	_____	_____
Mobile access (laptop/handheld) physical protection and data encryption	_____	_____	_____	_____	_____	_____
Healthcare data over Infrared or Radio links encrypted and authenticated	_____	_____	_____	_____	_____	_____
Control IP addresses, prevent IP spoofing	_____	_____	_____	_____	_____	_____
Periodic verification / maintenance of security measures	_____	_____	_____	_____	_____	_____
Policies and procedures in place for protection of remote / external access	_____	_____	_____	_____	_____	_____
Policies and procedures strictly enforced (even fines)	_____	_____	_____	_____	_____	_____
Periodic user training on required procedures	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____

Software Discipline	Doing it Now	In the future	Not Needed	Too Expensive	Does not Apply	Don't Know
Virus checking all files	_____	_____	_____	_____	_____	_____
Virus checking electronic mail	_____	_____	_____	_____	_____	_____
Control or restrict user software	_____	_____	_____	_____	_____	_____
Control PC software loading	_____	_____	_____	_____	_____	_____
Network software periodic census	_____	_____	_____	_____	_____	_____
Version control / Change control in use	_____	_____	_____	_____	_____	_____
Policies and procedures in place for assurance of software discipline	_____	_____	_____	_____	_____	_____
Policies and procedures strictly enforced (even fines)	_____	_____	_____	_____	_____	_____
Periodic user training on required procedures	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____

System Assessment	Doing it Now	In the future	Not Needed	Too Expensive	Does not Apply	Don't Know
Run anti-intrusion programs	_____	_____	_____	_____	_____	_____
Vulnerability evaluation	_____	_____	_____	_____	_____	_____
Stay up on CERT alerts	_____	_____	_____	_____	_____	_____
Avoid or update obsolete technologies	_____	_____	_____	_____	_____	_____
Network software periodic census	_____	_____	_____	_____	_____	_____
Version control / Change control in use	_____	_____	_____	_____	_____	_____
Policies and procedures in place for system self-assessment evaluation	_____	_____	_____	_____	_____	_____
Policies and procedures strictly enforced (even fines)	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____

Monitoring of Integrity of Data	Doing it Now	In the future	Not Needed	Too Expensive	Does not Apply	Don't Know
Document integrity checking system	_____	_____	_____	_____	_____	_____
Digital signatures applied to documents	_____	_____	_____	_____	_____	_____
Monitor integrity of backup media	_____	_____	_____	_____	_____	_____
Encrypt/sign database contents	_____	_____	_____	_____	_____	_____
Checksum or signature protection of critical files	_____	_____	_____	_____	_____	_____
Policies and procedures in place for monitoring integrity of data	_____	_____	_____	_____	_____	_____
Policies and procedures strictly enforced (even fines)	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____

Organizational Practices	Doing it Now	In the future	Not Needed	Too Expensive	Does not Apply	Don't Know
Scalable confidentiality and security procedures	_____	_____	_____	_____	_____	_____
Security / confidentiality committees	_____	_____	_____	_____	_____	_____
Designation of an information security officer in the organization	_____	_____	_____	_____	_____	_____
Education and training programs for all employees, medical staff, agents and	_____	_____	_____	_____	_____	_____

contractors.						
Organizational sanctions for violation of policies and procedures	_____	_____	_____	_____	_____	_____
Improved patient authorization forms for disclosure of health information	_____	_____	_____	_____	_____	_____
Patient access to audit logs	_____	_____	_____	_____	_____	_____
Awareness training for all personnel, including management	_____	_____	_____	_____	_____	_____
Periodic security reminders. User education	_____	_____	_____	_____	_____	_____
Written security policies and documentation	_____	_____	_____	_____	_____	_____
Signed statement by all employees regarding confidentiality of records	_____	_____	_____	_____	_____	_____
Defined escalation procedures, including contact names and numbers, for security issues	_____	_____	_____	_____	_____	_____
Personnel clearance procedure	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____
Other:_____	_____	_____	_____	_____	_____	_____