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	___	___	___	___	___	___

	Doing it Now	In the future	Not Needed	Too Expensive	Does not Apply	Don't Know
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	_____	_____	_____	_____	_____	_____

	Doing it Now	In the future	Not Needed	Too Expensive	Does not Apply	Don't Know
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:_____	⎯⎯	⎯⎯	⎯⎯	⎯⎯	⎯⎯	⎯⎯