Pre-Assessment Checklist for HIPAA Security Compliance

The following information is required as part of the process to certify compliance with emerging standards for electronic data security, as a part of DHHS' ongoing certification process for the U.S. Department of Health and Human Services' Health Insurance Portability and Accountability Act (HIPAA).

Please provide the following information to the best of your ability, involving other resources within your group as necessary to complete this documentation. Information from this document will be used to plan the assessment process for your group, so providing accurate information can greatly shorten the amount of time spent assessing your level of security compliance.

Point of Contact

Please provide the contact information (name, phone number, email address, etc) of the individual who will be the point of contact for HIPAA coordination within your division. If an additional individual will be coordinating specifically with the HIPAA Security efforts, please include information for that individual as well.

Name:		
Job Title:		
Email Address:		
Phone number:		
Office Address:		

Network Locations, Nodes, and Connections

Per location please identify the total number of nodes (servers, workstations, etc) and the types of connections (Internet, Remote, and third party/business partner).

Physical Location	No. of Nodes	Types of Connections

Types of Network Nodes

Please list the total number of each type of platform and the version or versions in use within your infrastructure. These are platforms that are physically located on the network.

Platform	Numbers	Version(s) In Use
DOS, Windows 3.x , 9x, ME		
NT/Windows 2000		
Unix (HP, Sun, Linux, etc.)		
Mainframes (VMS, etc.)		
Apple/Mac		
Novell		
Other (specify)		
Other (specify)		

Applications In Use

Please list the applications (web server, ftp server, etc), versions, and total numbers of those applications employed on your infrastructure.

Application	Version	Total No.
Web		
FTP (File Transfer Protocol)		
NFS (Network File System)		
SMTP (Email)		
DNS (Domain Name Service)		
RAS (Remote Access Service)		
Database		
Data Imaging Applications (Ghost)		
Instant Messenger Applications (AOL, MSN, Yahoo)		
Desktop Firewalls		
Other (Specify)		
Other (Specify)		

Network Perimeter Devices In Use (routers, firewalls, etc.)

Please identify the type and total number of routers (Cisco, Bay Networks, etc), firewalls (Check Point FireWall-1, Gauntlet, Cisco PIX, etc.) and VPN solutions employed within your infrastructure.

Device Type	Version	Total No.
Routers		
Firewalls		
VPN Solution		
Other (specify)		

Special Devices/Applications In Use

Please identify the type and total number of any other devices or applications not covered elsewhere, such as Personal Digital Assistants (PDA), Wireless devices and/or protocols, Laptops, personally used backup devices (e.g. read/writeable CD-ROM).

Device/ Application	Description	Total No.

Documentation

Asset List	Please use the provided forms attached to provide all necessary information on servers located within the network. If these servers are vital to daily business please make a notation on the form stating this.
General Network Information	Please attach a diagram or drawing of your network.

Network Information

External Network

(Duplicate this page as needed)

Registered IP Address Range(s):	
Registered Domain Name(s):	
Firewall in Use?	Y / N
Firewall IP Address:	
Firewall Hostname:	
Brand and Version of Firewall:	
Hardware/OS Platform of Firewall:	
Authorized Incoming Services:	**Server IP(s) Authorized for these (or 'any'):**
HTTP:	
FTP:	
Telnet:	
SSH:	
SMTP:	
DNS:	
Other (specify):	
Other:	
Other:	
Other:	
Other:	
Virtual Private Networks in Use?	Y / N
Implementation:	Hardware / Software
Manufacturer and version:	
Encryption in Use:	Y / N
Implementation:	Hardware / Software
Manufacturer and/or version:	

Internal Network

(Duplicate this page as needed)

Internal IP Address(es) in Use:		
Internal Protocol(s) in Use:	TCP/IP	Y / N
	NetBEUI/NetBIOS	Y / N
	IPX	Y / N
	SNA	Y / N
	Apple Talk	Y / N
	Banyan/Vines	Y / N
	Encryption (e.g. IPSEC)	Y / N
	LDAP	Y / N
	Other (Specify)	Y / N
NT Domains in Use	Y / N	
NT Domain Name(s):		
Novel NDS Tree in Use	Y / N	
Novell NDS Tree Name(s):		
SNMP Communities in Use:	Y / N	
SNMP Community Name(s):		
Allowed Outgoing Protocols (or 'any' if all):		
Encryption in Use:	Y / N	
Implementation:	Hardware / Software	
Manufacturer and/or version:		

Remote Access/Dial-in

Phone Number Ranges in Use:		
Modem Bank(s) in Use:	Y / N	
Modem Bank Phone Numbers in Use:		
Desktop Modem(s) in Use:	Y / N	
Modem Phone Numbers in Use:		
Remote access solutions in Use:	Y / N	
		PCAnywhere
	Other (Specify)	
Remote Management in Use:	Y / N	
	Other (Specify)	

Third Party Connections (Data Centers, Business partners, Application Service Providers (ASP))

Third Party Connection(s) into Network?	Y / N
Name of Third Party:	
Purpose of Connection:	
Address of Gateway to Third Party:	

Name of Third Party:	
Purpose of Connection:	
Address of Gateway to Third Party:	
Name of Third Party:	
Purpose of Connection:	
Address of Gateway to Third Party:	
Name of Third Party:	
Purpose of Connection:	
Address of Gateway to Third Party:	
Name of Third Party:	
Purpose of Connection:	
Address of Gateway to Third Party:	

Critical System List

(Duplicate this page as needed)

Host Name:	
IP Address:	
Platform:	
Protocol:	
Device Type (specify hardware/model)	
Server:	Switch:
Firewall:	Router:
Mainframe:	Other:
Accessible from Outside?	Y / N
Purpose:	
Physical Location:	
Services Running:	
FTP	HTTP
TELNET	SMTP
TFTP	SSH
DNS	OTHER(Specify)
OTHER	OTHER
OTHER	OTHER
OTHER	OTHER