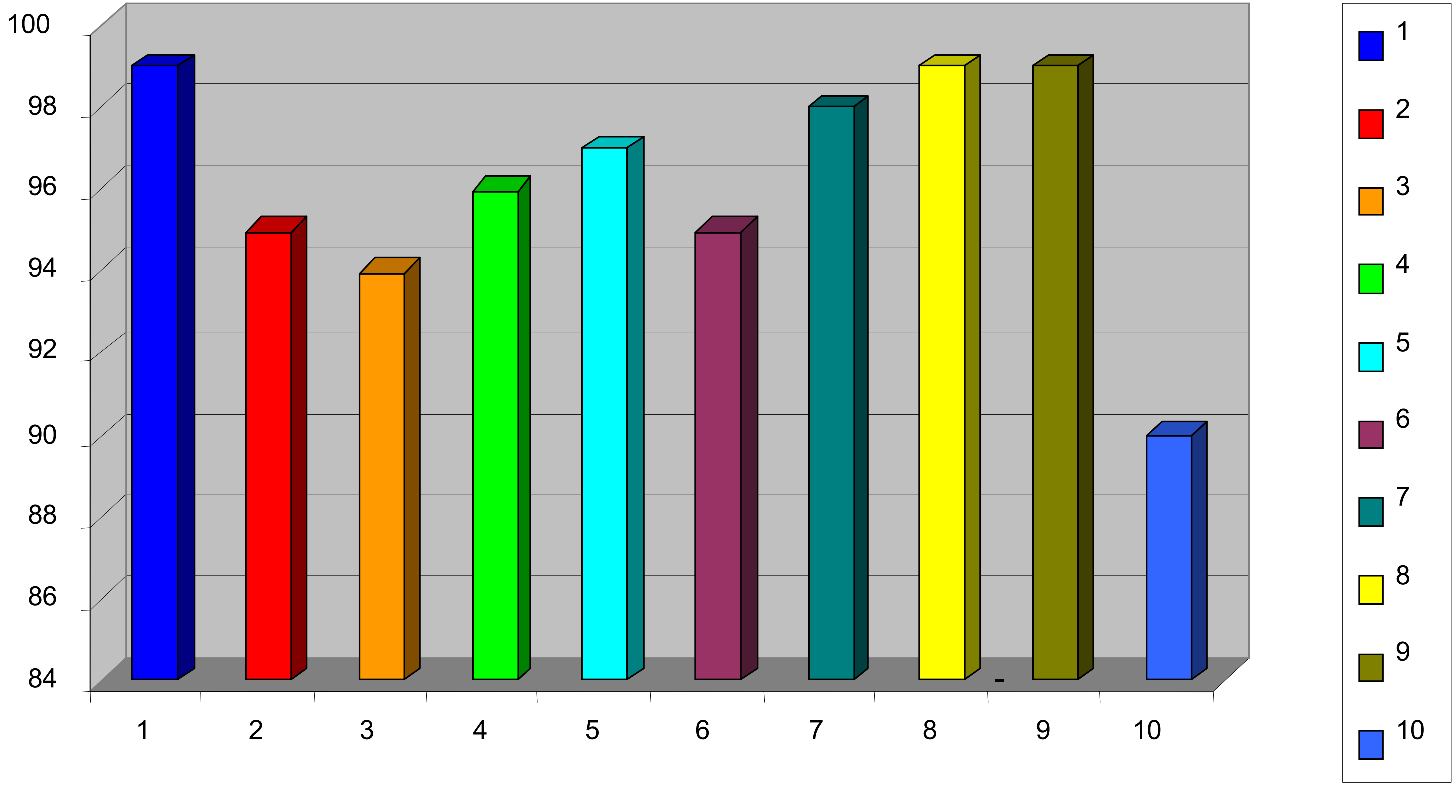
HIPAA Compliance – ISO17799

HIPAA Security & % Non-compliance



Security Policy

Business Continuity

Asset Classification & Control

Systems Dev & Maintenance

System Access Control

Personnel Security

Computer / Network Mgmt

Security Organization

Legal Compliance

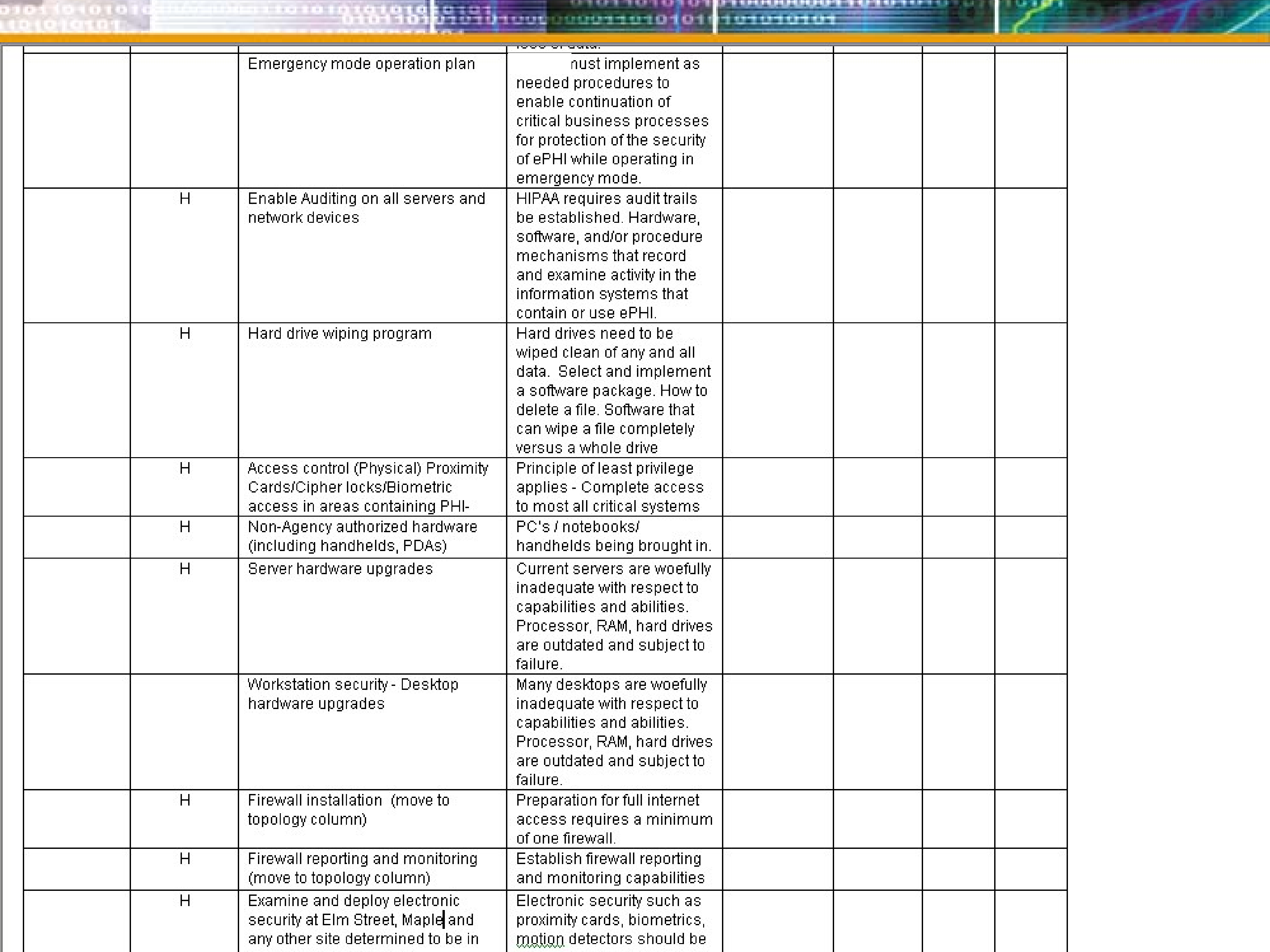
Physical / Environmental Security

-

RoadMap

Rank	Priority	Initiative Name	Description	Type	Exec Approved	Rank By Team	Start
(Numbered)	High Medium Low	HIPAA Security Requirement	Description of Need	Internal New Ongoing	(Funding available)		Q1, Q2, Q3, Q4
2	H	Access Control modifications (electronic)	Define and establish employee access controls on all critical systems and to the LAN as well as remote access and routers. Technical policies and procedures for information systems that maintain ePHI to allow access to only those persons or software programs that have been granted access rights as specified in the administrative safeguards section.	Ongoing	Yes	2	Q2
10	H	Unique user identification	Org. must assign a unique name and/or number for identifying and tracking user identity.	New	Yes	10	Q4
3	H	Emergency Access Procedure	Org. must establish and implement as needed procedures for obtaining necessary ePHI during an emergency.	Ongoing	Yes	3	Q2
4	H	Person or entity authentication	Org. must implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	Ongoing	Yes	4	Q2
7	H	Security Policy Development	Create and deliver corporate security policies	New	Yes	7	Q3
5	H	NT to 2000/2003 Upgrade	Begin planning for migration to Active Directory	New	No	5	Q4
11	HM	Windows 95, 98, NT to XP Upgrade/Licensing Compliance	Desktop upgrade to ensure security	New	No	11	Q104
8	H	Network Intrusion Detection / Host IDS	Implement IDS at critical access points	New	Yes	8	Q3
15	H	Create the Org. security team	Include staff from multiple sites	Ongoing	Yes	15	Q2
1	H	Define the Flow of PHI	Define the flow and restrict the flow	New	No	1	Q2

	M	Full IT documentation of processes, procedures, guidelines	Documentation of all activities within IT needs to be created				
	H	Incident Response	Develop Incident Response procedures and reporting				
	M	Problem Management	Develop Problem Management procedures				
	M	Configuration Control	Develop Configuration Control procedures				
	M	Change Management	Develop Change Management procedures				
	M	Release Management	Develop Release Management procedures				
6	H EXTERNAL L INTERNAL	Email Encryption – Transmission security.	Select and install - Software to examine email and other electronic information traversing CHCS networks. CHCS must implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Since PHI does flow in this manner, security measures must be implemented that ensure electronically transmitted ePHI is not improperly modified without detection until disposed of. Also, mechanisms to encrypt ePHI whenever deemed appropriate must be implemented.	Ongoing	Yes	6	Q2-4
9	H	Anti-Virus on all servers	Add anti-virus to critical systems	Ongoing	No	9	Q3
	M	Computer Room Physical Security	Install card access with auditing				
	H	Windows 2000 / 2003 Server (security)	Establish security standards for Windows 2000				
	H	Create a Business Continuance, Disaster Recovery Plan for IT	HIPAA requires these plans be in place and periodically updated and tested – procedures to restore any				



			loss of data.				
		Emergency mode operation plan	nust implement as needed procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.				
	H	Enable Auditing on all servers and network devices	HIPAA requires audit trails be established. Hardware, software, and/or procedure mechanisms that record and examine activity in the information systems that contain or use ePHI.				
	H	Hard drive wiping program	Hard drives need to be wiped clean of any and all data. Select and implement a software package. How to delete a file. Software that can wipe a file completely versus a whole drive				
	H	Access control (Physical) Proximity Cards/Cipher locks/Biometric access in areas containing PHI-	Principle of least privilege applies - Complete access to most all critical systems				
	H	Non-Agency authorized hardware (including handhelds, PDAs)	PC's / notebooks/ handhelds being brought in.				
	H	Server hardware upgrades	Current servers are woefully inadequate with respect to capabilities and abilities. Processor, RAM, hard drives are outdated and subject to failure.				
		Workstation security - Desktop hardware upgrades	Many desktops are woefully inadequate with respect to capabilities and abilities. Processor, RAM, hard drives are outdated and subject to failure.				
	H	Firewall installation (move to topology column)	Preparation for full internet access requires a minimum of one firewall.				
	H	Firewall reporting and monitoring (move to topology column)	Establish firewall reporting and monitoring capabilities				
	H	Examine and deploy electronic security at Elm Street, Maple and any other site determined to be in	Electronic security such as proximity cards, biometrics, motion detectors should be				

	M	Review and harden all vendor contracts (IBM verbal agreement for 48 hours)	Ensure response times and deliverables meet Org requirements for uptime. Tie this to the DRP and BCP.				
	H	Workstation Use - User/desktop security	Deploy strong passwords, screen savers, automatic inactivity timeouts in applications and periodic password changes. No password sharing.				
	H	Review porting PC-based applications	Centralized control in an enterprise database (DB2 – SQL-Server)				
	H	Complete topology review	In preparation for enterprise Internet access (network, security devices, DNS, DMZ, etc.)				
	H	Security Training	Org needs to implement a security awareness and training program for all members of its workforce (including management).				
	H	Risk analysis / Risk management	Org must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI. Org must implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with security standards (ISO17799 used)				
	H	Sanction Policy	Appropriate sanctions against workforce members who fail to comply with Org security policies and procedures must be applied.				
	H	Information System Activity Review	Org must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.				