Column1	Column2	Column3	Column4
Section	**Topic**	**Tech Tools Needed**	**Notes**
Introduction	**The importance of cybersecurity and compliance in the healthcare industry**		
	Overview of challenges for small healthcare organizations		
	State of the healthcare industry in 2023		
	Compliance vs Security		
	How does compliance work?		
The Cybersecurity Landscape	**Types of cyber threats small healthcare organizations may encounter**		
	Ransomware		
	Phishing		
	Insider Threats		
	Unsecured Devices		
	Third-Party Risks		
	Cybersecurity Processes and Best Practices		
10 Cybersecurity Requirements for SMB	**Tools and Technology Required for HIPAA**		
	Email Protection		
	Endpoint Protection		
	Access Management		
	Data Loss Prevention (DLP)		
	Asset Management		
	Network Management		
	Vulnerability Mangement		
	Incident Response		
	Medical Device Security		
	Cybersecurity Oversight & Governance		
Email Protection Systems	**Why email is a hotspot for cyber threats**		
	Key steps for establishing a robust email protection system		
	Phishing Risks and Prevention		
	Email Configuration and Training		
	Email Protection Systems		
	Email Encryption		
Endpoint Protection Systems	**Understanding endpoints and their vulnerabilities**		
	Measures to shield endpoints from threats		
	Basic Endpoint Protection		
	Device Encryption		
	Patching and End of Life		
Access Management	Controlling and monitoring access to critical information		
	Implementing best practices for access control		
	Managing Administrative Accounts		
	Shared Accounts- Don't Do It!		

	Multifactor Authentication or Single Sign-on		
	Terminating Access		
Data Protection and Loss Prevention	**The significance of safeguarding healthcare data**		
	Data Loss Prevention (DLP) vs Backups		
	DLP Options		
	DLP and Cloud Services		
	DLP Policies		
Asset Management	**Rationale for keeping track of organizational assets**		
	Techniques for comprehensive asset management		
	Procurement		
	Invetory		
	Decommissioning		
	Lost or Stolen Devices		
Network Management	**Foundations of maintaining a secure network**		
	Best practices for network protection and monitoring		
	Network Security practices		
	Network Segmentation		
	Intrusion Prevention		
	Network Monitoring		
	Physical Security and Guest Access		
Vulnerability Management			
	What is vulnerability management?		
	Tips for Implementing vulnerability management		
	Patching and Updating		
	Vulnerability Scans		
	Mitigated Risks		
Incident Response	**The role and importance of a fast and effective incident response**		
	Building a reactive incident response plan		
	Roles and Responsibilities		
	Challenges for the SMB		
	Types of incidents		
	Reporting and remediation		
Medical Device Security	**Addressing the unique vulnerabilities of network-connected medical devices**		
	Benefits and Risks		
	Practical steps for enhancing the security of medical devices		
	Best Practices		
	Challenges		

Cybersecurity Oversight and Governance	**The role of administrative oversight and documentation in compliance**		
	Structuring governance for optimum outcomes		
	The "Soft Side" of Compliance		
	Why security alone won't get you there		
Conclusion	**Recapping the essentials of cybersecurity and compliance for small healthcare organizations**		
	Reinforcing the need for a holistic, proactive approach		
	Benefits of Compliance		
Q&A Session	**Opportunity for attendees to clarify doubts, share experiences, or delve deeper into specific topics.**		
Note	Attendees are encouraged to bring their queries or specific challenges they face in their organization for a more interactive and productive Q&A session.		