CONSENTRY NETWORKS SUPPORT MATRIX

FOR HIPAA SUBPART C STANDARDS

HIPAA Subpart C Standards	Sections	Specifications [R] Required, [A] Addressable	ConSentry Support
Administrative Safeguards			
Security Management Process Implement policies and procedures to prevent, detect,contain, and correct security violations.	164.308 (a)(1)	Risk Analysis [R] Risk Management [R] Sanction Policy [R] Information System Activity Review [R]	The ConSentry solution allows for the creation of security or application/data access policies on a per user or per group basis. The product will monitor the adherence to these policies for every LAN port connected on the network. Flexible reports show the adherence to policies as well as violations.
Workforce Security Authorize, supervise and manage employee access	164.308(a)(3)	Authorization/Supervision [A] Workforce Clearance Procedure[A] Termination Procedures [A]	The ConSentry solution features either active or passive authentication to identify users group membership and access privileges as they log into the network. Access to patient data can be controlled to only those users who have approval to view the data. When employees are terminated, their access privileges can be revoked in the central identity storage system and the ConSentry solution will learn in real time of these changes.
Information Access Management Isolate clearinghouse functions and control access to protected health information	164.308(a)(4)	Isolate Health Care Clearinghouse Functions [R] Access Authorization [A] Access Establishment and Modification [A]	The Consentry solution effectively 'firewalls' access on a per user basis. The solution does not require network design modification in order to establish physical segmentation of users. No matter where users log in from, their appropriate access policies are enforced at the port level.
Security Awareness Training Provide updates, guard against malware, monitor logins and manage passwords	164.308(a)(5)	Security Reminders [A] Protection from Malicious Software [A] Log-In Monitoring [A] Password Management [A]	The ConSentry solution can control the spread of malware in milliseconds, rapidly identifying and stopping malware propagation, thereby preventing network meltdown.

HIPAA Subpart C Standards	Sections	Specifications [R] Required, [A] Addressable	ConSentry Support
Security Incident Response Identify, respond to, mitigate and document security incidents	164.308(a)(6)	Response and Reporting [R]	The ConSentry solution provides detailed real time event visualization and one-click remediation to block the effects of malicious activity. Integrated historical reports provide long term trend analysis and documentation of security events.
Technical Safeguards			
Access Control Track users, ensure emergency availability and encrypt data	164.312(a)(1)	Unique User Identifier [R] Emergency Access Procedure [R] Automatic Logoff [A] Encryption and Decryption [A]	The ConSentry solution leverages an organization's existing user identity solution and binds user name to IP and MAC address so that users can be tracked as to where they go and what applications they use. ConSentry enforces the appropriate access policies based on user or group identity policies.
Audit Controls Record and examine system activity	164.312(b)	Implement audit mechanisms [R]	ConSentry can track and log access to restricted information and send suspect traffic to a network sniffer for detailed investigation and forensics.
Integrity Authenticate that health data has not been altered	164.312(c)(1)	Mechanism to Authenticate [A]	ConSentry can provide audit trails on a per user basis [identified by user name, not just machine name] on all access to restricted information.
Person or Entity Authentication Implement procedures to verify identity prior to granting access	164.312(d)	Procedures to Verify Identity [R]	The ConSentry solution integrates tightly with a Network Access Control architecture without requiring upgrades. ConSentry will authenticate the user prior to network access, confirm identity with existing identity databases, ensure that the host machine meets the appropriate security levels, and only then grant access to only the applications and services for which the person is authorized.
Transmission Security Shield electronic transmissions from improper modification	164.312(e)(1)	Integrity Controls [R] Encryption [A]	The solution ensures that only authorized users [identified by user name, not just machine name] have access to restricted information.

CONSENTRY NETWORKS

ConSentry Networks
1690 McCandless Drive
Milpitas CA 95035

Phone 408.956.2100 **Fax** 408.956.2199
Toll-Free 866.841.9100
Email info@consentry.com
www.consentry.com