Effective Date: 10/22/2019
Review Date: 10/22/2019
Revised Date: 10/2/2019

North Sound Behavioral Health Administrative Services Organization, LLC

Section 4000 - Information Systems: Vulnerability and Risk Analysis

Authorizing Source: HCA Contract
Approved by: Executive Director Date: 10/22/2019 Signature:

POLICY #4003.00

SUBJECT: VULNERABILITY AND RISK ANALYSIS

POLICY

At least annually, or whenever significant changes occur on the network, the North Sound Behavioral Health Administrative Services Organization (North Sound BH-ASO) Security Officer, IT Administrator (or assignee) shall conduct periodic vulnerability scans from both inside and outside of the network. In addition, at least every three (3) years, North Sound BH-ASO will conduct a HIPAA Risk Assessment.

Internal Scans

When conducting internal scans, at a minimum, the following shall be done:

1. System user testing
    a. Randomly choose a current system user
    b. Make a copy of their profile
    c. Make attempts to access various network resources such as:
        i. Directories where the user does not have access
        ii. System tools that affect configuration of network resources
    d. Attempt to log on to resources that the user does not have access to log on to
    e. Attempt to bypass firewall settings
    f. Attempt to access potentially malicious files. Currently, most workstations are configured to not execute certain file types (e.g., .vbs, .js, etc.) but rather point to a warning document located on the network.
2. Verify that various security and system logs are appropriately logging scan events.
3. Document any vulnerabilities found and propose solutions if necessary.
4. Rectify as applicable vulnerabilities found

This is by no means meant to be an exhaustive list of the internal scans that will be conducted. Rather it is to establish a minimum of what shall be done. Additional items will be scanned as technology and system resources change, and as new threats are discovered. These additional items scanned will be documented as a part of the report generated from the internal scans.

External Scans

When conducting external scans, at a minimum, the following shall be done:

1. Firewall testing
    a. Utilize various external resources to probe the firewalls to see what ports are open.

b. Attempt to gain access to network resources via open ports.

2. Test to ensure protection mechanisms are protecting North Sound BH-ASO mailboxes by blocking potentially malicious attachments to email messages.
3. Test if able to bypass firewalls to gain access to internal network resources.
4. Verify that various security and system logs are appropriately logging scan events.
5. Document any vulnerabilities found and propose solutions if necessary.
6. Rectify as applicable vulnerabilities found.

This is by no means meant to be an exhaustive list of the external scans that will be conducted. Rather it is to establish a minimum of what shall be done. Additional items will be scanned as technology and system resources change, and as new threats are discovered. These additional items scanned will be documented as a part of the report generated from the internal scans.

Periodic testing includes penetration tests, vulnerability assessments and system code analysis. Whenever a new server, workstation, device or application is to be added to the network, a vulnerability assessment of that system or application will be conducted.

HIPAA Risk Assessment

North Sound BH-ASO will conduct a Security Assessment to review and assess the effectiveness of the HIPAA security program. This test will be conducted ***at least once every three years***. This Assessment shall be conducted by an outside auditor or organization independent of North Sound BH-ASO IT staff.

ATTACHMENTS

None