Effective Date: 12/24/2019
Review Date: 5/24/2022
Revised Date:

North Sound Behavioral Health Administrative Services Organization, LLC

Section 4000 - Information Systems: Incident Response Plan (IRP)

Authorizing Source: HCA Contract
Approved by: Executive Director Date: 5/24/2022 Signature:

POLICY #4024.00

SUBJECT: INCIDENT RESPONSE PLAN (IRP)

PURPOSE

In compliance with §164.308(a)(6)(i) – (ii), and State Contract OCIO requirements, North Sound Behavioral Health Administrative Services Organization (North Sound BH-ASO) has implemented procedures to identify and respond to non-disaster security incidents to protect all confidential information, including protected health information (PHI). With reference to the NIST 800-61, Rev. 2 Incident Handling Procedures, this IRP includes processes that will ensure the timely and effective handling of information technology security incidents. This includes elevation to the Emergency Mode Operations and/or Business Continuity and Disaster Recovery (BCDR) plans, and whether to engage additional notification procedures.

PROCEDURE

Incident Response Team

The North Sound BH-ASO HIPAA Security Officer (or assignee) will convene a security incident response team after performing an initial analysis, after a potential threat is identified. The response team will include the HIPAA Privacy Officer and other members of the IS/IT team. Depending on the nature and severity of the incident, additional staff may be assigned.

Incident Prevention

Reducing the impact of security incidents is handled through workforce training that includes Relias (or other LMS) training modules, routine security reminders sent via email or discussed during meetings, and other training resources that will be made available, such as the North Sound BH-ASO Intranet website.

Incident Detection

Information technology workforce members will monitor network, server, workstation, and information-flow behavior using firewall email threat alerts, syslog server alerts, SFTP logs, web and network server logs, backup logs, security system access logs, and various network automated status alerts sent via email and text. These emails are briefly reviewed and archived by the Security Officer and/or the Information Technology (IT) team as they come in multiple times daily, watching for service failures or other deviations from preferred baselines.

Incident Containment and Correction

Workforce members will report security incidents to the HIPAA Privacy and Security Officers. If the incident demands a timelier response, workforce members will notify the Security Officer and / or the IT team to report an incident affecting information security. To determine the effectiveness of this Incident Response Plan (IRP) and identify key areas for improvement based on lessons learned, the response team will utilize the weekly IS and IT stakeholder meetings for post incident reviews, and the annual IRP review. Additional review meetings may be scheduled as necessary.

The Information Technology Manager will analyze the incident and:

1. Determine whether an incident has occurred;
2. Evaluate what information is at risk of being compromised;

3. Ascertain what users' services are affected;
4. Ascertain what network services are affected; and
5. Make the determination whether to recommend to the HIPAA Privacy Officer to use the Breach Notification Protocol. This includes timely notification to *all* contracted business partners, vendors and delegates accordingly. In the event of a release of Category 3 or above data, the North Sound BH-ASO will follow the state breach notification statute RCW 42.56.590 regarding personal information.

If the IT Manager determines that an incident could affect other users or services, then containment will follow the initial analysis and include:

1. Identifying affected systems and services;
2. Identifying whether workforce credentials are compromised or at risk;
3. Isolating the affected system(s), service(s) or credentials from the affected user(s) and from the network if possible, to preserve forensics;
4. Considering additional systems that are at risk of being compromised;
5. Considering engaging external-vendor computer forensic services;
6. Understand and report the impact to appropriate business function managers; and
7. Directing the evaluation of any automated tools that failed to detect the incident.

Once the security incident effects have been isolated, the IT Department will eradicate the incident:

1. Remove, if possible, all like-vectors (e.g. phishing emails, malware, etc.) from other systems; and
2. Wipe or reimage workstations or servers as appropriate.

After systems, services or credentials no longer pose a threat to the greater information, the IT Department will recover affected systems, services or credentials and may:

1. Reload systems or restore services from backups as required.
2. Create new credentials while existing accounts are further analyzed.
3. Update firewalls or other network security appliances (e.g. IPS) to prevent incident reoccurrence.
4. Scan affected systems after restored to ensure no additional vulnerabilities are present.

The HIPAA Security Officer will record all incidents onto the North Sound Behavioral Health Administrative Services Organization HIPAA Program Security Incident Log, and perform post-incident work that includes:

1. Confirming whether information confidentiality, integrity or availability was compromised and if the Breach Notification Protocol applies;
2. Determining whether a security violation has occurred;
3. Reviewing policy and training materials; and
4. Implementing appropriate changes to policy and train the workforce as applicable to reduce the risk of incident reoccurrence.

Business Associate Incident Management
The HIPAA Security Officer and Privacy Officer will review delegate Business Associate (BA) reported security incidents. Corrective action, to include terminating the BA service contract, may be performed by the HIPAA Privacy Officer. North Sound BH-ASO will notify all contracted business contacts of any service disruptions that affect their data.

Incident Retention
The HIPAA Security Officer will retain a record of all security incidents for six years from resolution. North Sound BH-ASO BCDR and IRP plans are stored securely offsite in the event of an emergency where the building was to become inaccessible for any reason.

REFERENCES

4022.00 Business Continuity Disaster Recovery (BCDR)
North Sound BH-ASO Business Continuity and Disaster Recovery (BCDR) Plan

ATTACHMENTS
None