Cherokee Indian Hospital Authority

The Mission of the Cherokee Indian Hospital is to be the provider of choice for the community by providing accessible, patient and family centered quality healthcare with responsible management of the Tribes resources.

TITLE: CIHA Awareness and Training Policy

REVIEWED AND APPROVED BY: CIHA Executive Committee

EFFECTIVE DATE: 4/18/2023

LAST REVIEWED: 4/18/2023

PURPOSE:

The purpose of the Cherokee Indian Hospital Authority (CIHA) Awareness and Training Policy is to provide a security framework that ensures the protection of the CIHA information systems, technology devices, and data from unauthorized access, loss, or damage while supporting the organization's business-driven needs and meeting compliance with North Carolina State departments, including the North Carolina Department of Information Technology (NCDIT), the North Carolina Department of Health and Human Services (NCDHHS), and NC Medicaid. The information may be:

- Verbal;
- Digital; and/or
- In hardcopy form.

The information may also be:

- Individually controlled or shared;
- Stand-alone or networked;
- Used for administration, research, marketing, or other purposes.

In support of the purpose, this *Awareness and Training Policy* has been developed to ensure the confidentiality, integrity, availability (CIA), privacy, and security of the information assets of CIHA through the establishment of safeguards to prevent theft, abuse, and misuse while exceeding State departments' compliance requirements.

Failure to comply with this Policy may subject the CIHA workforce (refer to the Definition section for further description and delineation of CIHA Workforce) to potential penalties and disciplinary action that may include termination of employment or contract.

STAFF GOVERNED BY THIS POLICY:

This Policy applies to all:

- CIHA workforce;
- CIHA vendors or subcontractors, who process, store, transmit, and have connectivity to the Information Technology (IT) infrastructure.

POLICY:

[NIST AT-1]

Note AT = Acronym Used by NIST for Awareness and Training

CIHA shall implement and maintain an Awareness and Training Policy in compliance with National Institute of Standards and Technology (NIST) and State departments. This Policy shall be reviewed annually or more frequently as federal, state, and tribal laws, rules, or regulations are modified and updated as necessary.

The *CIHA Awareness and Training Policy* shall include preventive and timely maintenance activities that consist of:

- Development, documentation, dissemination, implementation, and maintenance of an awareness and training policy and procedural guidelines;
- Security awareness training requirements;
- Insider threat training requirements;
- Individual responsibility for using, configuring, and/or maintaining information systems;
- Security training records.

DEFINITIONS:

Access to Organizational Information Systems

Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., non-local access).

Chief Executive Officer (CEO)
The Chief Executive Officer (CEO) is the executive sponsor for CIHA who provides direction on major hospital policies, including, but not limited to, strategic, financial, risk management, infrastructure, regulatory, and governance issues. The CEO is responsible for delegation of tasks needed to ensure CIHA information security (IS) and cyber risks are managed through an appropriate governance committee. The CEO shall also ensure that both strategic and operational processes are empowered and supported. The CEO will monitor progress on all major initiatives.

Chief Information Officer (CIO)
The Chief Information Officer (CIO) is responsible for CIHA's overall information technology strategy and operations. The CIO delegates responsibility for information technology strategy and information technology operations activities, as appropriate. The CEO authorizes the CIO to pursue appropriate activities and actions which help achieve the strategy and operations objectives consistent with this Policy.

Chief Information Security Officer (CISO)
The Chief Information Security Officer (CISO) is responsible for ensuring that CIHA information is protected. The CISO will delegate responsibility to steadfast individuals for approving and reviewing access rights to information. The CISO is responsible for ensuring that CIHA's security objectives are achieved. The CEO authorizes the CISO to pursue appropriate activities and actions that are consistent with this Policy, which contribute to achieving CIHA's security objectives.

CIHA Workforce
CIHA workforce includes all full-time or part-time CIHA staff/personnel/agents/employees (i.e., contractors, volunteers, interns, trainees, students, contract employees/workers, other third parties, guests), non-employees, and other persons/individuals whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

National Institute of Standards and Technology (NIST)
NIST is one of the nation's oldest physical science laboratories. NIST provides technology, measurement, and standards for the smallest to the largest technologies. CIHA has adopted the Cyber Security Framework (CSF) provided by NIST, which provides guidance on how to prevent, detect, and respond to cyberattacks.

Procedural Guidelines
Guidelines for developing operational procedures.

PROCEDURAL GUIDELINES:
CIHA ensures that all applicable users follow the procedural guidelines for purposes of complying with CIHA policies.

Awareness and Training Policy and Procedural Guidelines
[NIST AT-1]
Internal Controls:
All CIHA information assets must meet the required security controls defined in this Policy that are based on NIST. This Policy addresses CIHA's requirements, which will be used to implement the awareness and training process and the family of awareness and training security controls. The awareness and training process is required to ensure that all information systems are designed and configured using controls sufficient to safeguard CIHA's information systems. CIHA has adopted the Awareness and Training principles established in NIST, "Awareness and Training" control guidelines, as the official standards for this security domain. The "AT" designator identified in each control represents the NIST-specified identifier for the Awareness and Training control family.

CIHA develops, documents, disseminates, implements, and maintains this Policy, as it applies to all covered personnel involved in the acquisition, development, operation, and cybersecurity maintenance of information systems, technology devices, and supporting infrastructure. This Policy:

i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
ii. Requires that the Awareness and Training procedures include the necessary controls to facilitate the implementation of this Policy.

Policies and procedures are a critical component of CIHA's system of internal controls, which helps to ensure that all personnel have a clear understanding of roles, responsibilities, acceptable uses, and other important information that relates to awareness and training in accordance with information security's best practices. As such, policies and procedures relating to the stated criteria herein are to be reviewed and updated on an annual basis to ensure that their overall adequacy and sufficiency meets CIHA's needs.

Literacy Training and Awareness
[NIST AT-2]
CIHA management must provide any required local information security training and track the completion of all required training in a training completion log or system. CIHA shall provide information relevant to effective information security practices to workforce in a timely manner.

On at least a quarterly basis, CIHA management shall receive input from information security staff on the effectiveness of information security measures and recommended improvements. Training requirements include the following:

a. A handbook or summary of information security policies, which shall be formally delivered to and signed by covered persons before beginning work;
b. Formal information technology security training appropriate for work responsibilities on a regular basis and whenever a workforce member's work responsibilities change;
c. Managers must delay covered personnel access to Restricted or Highly Restricted data until initial training is complete;
d. When a workforce member changes jobs, his/her information security needs must be reassessed, and any new training on procedures or proper use of information-processing facilities shall be provided as a priority;
e. All contractors and other third parties shall have provisions in their contracts with CIHA that sets forth the requirement that they must comply with all CIHA information security policies;
f. Training on social engineering and how to detect it and respond to it;
g. Training on the acceptable use of CIHA resources;
h. Annually recurring information security awareness training in support of information security awareness program objectives must be completed by all workforce (which includes all consultants and vendors) with access to CIHA information assets) that is appropriate for work responsibilities;
i. Management must revoke logical access to systems and services if a workforce member fails to complete required annual training. Failure to complete required training within the renewal date shall result in either disciplinary action or a loss of access to systems until such time as the training has been completed;
j. Workforce members on extended medical leave are exempted from this requirement until such time that they return to the workplace;
k. Managers must ensure that covered workforce members remain in compliance with required training;
l. Long-term contractors and other third parties with contracts ending within thirty (30) days of an annual training deadline are exempted from completing annual training.

Literacy Training and Awareness – Insider Threat
[NIST AT-2(2)]

Insider threat training shall include how to communicate workforce concerns and the prevention, detection, and response regarding potential indicators of insider threats through appropriate CIHA channels in accordance with established organizational policies and procedures.

Potential indicators and possible precursors of insider threat can include behaviors, such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow workforce members, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices.

Role-Based Training

[NIST AT-3]

The extent of security-related training shall reflect the person's individual responsibility for using, configuring, and/or maintaining information systems. CIHA shall provide training to users and technical staff in critical areas of cybersecurity, including vendor-specific recommended safeguards.

a. Role-based security-related training shall be provided before authorizing a person's access to a system and before that person is allowed to perform his/her assigned duties, when required by system changes;
b. Training in cybersecurity threats and safeguards, with the technical details to reflect the workforce member's responsibility for configuring and maintaining information security, is required;
c. Annual re-occurring training shall be provided thereafter;
d. Technical staff responsible for information system security will receive training in the following areas:
    i. Server and personal computer (PC) security engagement;
    ii. Packet-filtering techniques implemented on routers, firewalls, etc.;
    iii. Intrusion detection and prevention;
    iv. Software configuration, change, and patch management;
    v. Virus prevention/protection procedures;
    vi. Business continuity practices and procedures;
    vii. Additional education for information security professionals and jobs requiring expertise in security will be provided as needed through formal external courses and certification programs.

Training Records

[NIST AT-4]

CIHA shall document and monitor individual information system security training activities, including basic security awareness training and specific information system security training. Individual training records shall be retained for a period of ten (10) years.