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 Media Protection Policy

REVIEWED AND APPROVED BY: CIHA Executive Committee

EFFECTIVE DATE: 5/25/2023

LAST REVIEWED: 5/25/2023

PURPOSE:

The purpose of the Cherokee Indian Hospital Authority (CIHA) Media Protection 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 *Media Protection Policy* has been developed to ensure the confidentiality, integrity, and 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 MP-1]

Note MP = Acronym used by NIST for Media Protection

CIHA shall implement and maintain a Media Protection 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 Media Protection Policy* shall include preventive and timely cybersecurity maintenance activities that consist of:

- Development, documentation, dissemination, implementation, and maintenance of a media protection policy and procedural guidelines;

- Only authorized personnel shall be allowed access to media;

- Authorized personnel shall be approved through a documented and formalized user provisioning process;

- Media marking shall be assigned and affixed distribution limitations and applicable security attributes;

- Media storage shall be in secure location at all times;

- Transportation of media;

- Media sanitization and disposal;

- Testing of sanitization equipment and procedures;
- Application of non-destructive sanitization techniques;
- Restrictions on use of media, such as USB flash drives and external, portable hard disk drives.

DEFINITIONS:

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.

Media

Physical devices or writing surfaces onto which information is recorded, stored, or printed within an information system.

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.

<u>Media Protection Policy and Procedural Guidelines</u>

[NIST MP-1]

<u>Internal Controls:</u>
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 media protection process and the family of media protection security controls. The media protection 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 Media Protection principles established in NIST, "Media Protection" control guidelines, as the official standards for this security domain. The "MP" designator identified in each control represents the NIST-specified identifier for the Media Protection 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 Media Protection 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 media protection 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.

Media Access

[NIST MP-2]

CIHA restricts user access to digital and non-digital media to only authorized individuals by using CIHA-defined security measures. Using discretion, CIHA may restrict the use of media in environments that process Highly Restricted data through:

a. Security controls, which shall be implemented to protect the CIA of data contained on media (throughout the media's life and disposal) from unauthorized disclosure and modification;

b. Access controls, which shall include physical protection of and accountability for removable storage media, minimizing the risk of damage to its stored data, unauthorized access, theft, and software licensing violations;

c. Risk assessment, which aids in selecting the type of media and associated information within it that requires restricted access;

d. System owners, who must document policies and procedures about access to restricted media, personnel who are authorized to access this media, and the specific measures taken to restrict it;

e. Documentation of the processes required to ensure the protection of the information of the access restricted media and the information on the media from authorized access. This includes, but is not limited to, backup media (e.g., digital media or disks or non-digital media);

f. Personnel - they must use only CIHA approved devices to store Restricted or Highly Restricted data. Personally owned removable devices (e.g. thumb drives, jump drives, external hard drives) must not be used on the CIHA network and for storing non-public data:

   i. All removable storage media must be encrypted using FIPS 140-3 (and subsequent versions) approved encryption algorithms (e.g. AES-256), unless the CIHA CISO or designee has classified the data as public. This includes, but is not limited to, devices such as thumb/flash drives, external/removable hard drives, compact disks, etc.;

   ii. All removable storage devices must be isolated and scanned for malware prior to use on the CIHA network. Autorun capabilities should be deactivated to reduce any risk of malware leak;

   iii. Any detected malware must be removed from the removable storage devices. The removable storage devices must then be verified to ensure that it is safe for use on the CIHA network.

Using Data Loss Prevention (DLP):
CIHA must use all preventive measures to ensure that the CIA of data remains intact. Data Loss Prevention (DLP) technologies offer automated ways to protect confidential data from being transmitted external to the CIHA network without approval and using encryption technologies. CIHA must employ automated tools to monitor internally or at network boundaries for unusual or suspicious transfers or events regarding the following data types:

a. Personally Identifiable Information (PII);

b. State and Federal Tax Information (FTI);

c. Protected Health Information (PHI);

d. Payment Card Industry (PCI) Data Security Standard DSS;

e. Social Security Administration (SSA) Provided Information;

f. Attorney-Client Communications.

Media Marking
[NIST MP-3]

Media should be marked for multiple purposes, including:

a. All data must be labeled to reflect its classification. Recipients of information must maintain an assigned internal and external label and protect the information;

b. If data or systems contain multiple classifications, then the highest classification shall appear on the label. Data labeling may be automated where technically configurable or performed manually;

c. CIHA must label removable media (e.g., CDs, DVDs, diskettes, external hard drives, and flash drives) and any information system output that contains FTI (e.g., reports, documents, data files, back-up tapes);

d. The following table summarizes labeling requirements for different classes of data:

Table 1. Risk Classification for Data Label Requirements

Media	Classification		
	Low Risk	**Medium Risk (Restricted)**	**High Risk (Highly Restricted)**
Electronic Media Email/Text Recorded Media CD/DVD/USB (Soft Copy)	No Label Required	• Creation Date • External and Internal Labels • Email – Beginning of Subject Line • Physical Enclosure – Label	• Creation Date • External and Internal Labels • Email – Beginning of Subject Line • (See IRS 1075 Publication for Additional Marking Requirements for FTI)
Hard Copy	No Label Required	• Each Page if Loose Sheets • Covers (Front and Back) and Title Page, if Bound	• Each Page if Loose Sheets • Covers (Front and Back) and Title Page, if Bound
Web Sites	No Label Required	• Internal Website Only • Each Page Labeled “RESTRICTED” on Top and Bottom of Page	• Internal Website Only • Each Page Labeled “HIGHLY RESTRICTED” on Top and Bottom of Page

Data Classification:
All data must be classified into one (1) of three (3) classes:

- Low Risk;
- Medium Risk (Restricted);
- High Risk (Highly Restricted).

The classifications determine the level of security that must be placed around the data. The data creator or steward is responsible for labeling the classification of risk for information correctly. The three (3) classes are identified by the following definitions and criteria:

- **Low Risk**
  Data or systems that are open to public inspection, according to state and/or federal law, or is readily available through public sources. By default, data is Low Risk unless it meets the requirements for a higher classification.

- **Medium Risk (Restricted)**
  Any data or systems that are breached or disclosed to an unauthorized person is in violation of state and/or federal law. Medium Risk may also be referred to as Restricted.

  The following types of data must be classified as Medium Risk, at minimum. This is not a complete list and is subject to legislative changes:

  - **CIHA Employee Personnel Records**
    These records include information that is confidential, and unauthorized discussion, disclosure, and/or dissemination of this confidential applicant/employee information is prohibited;

  - **Security Features**
    Information that describes security features of electronic data processing systems, information technology systems, telecommunications networks, or electronic security systems, including hardware or software security, passwords, or security policies procedures, processes, configurations, software, and codes is confidential;
  - **Sensitive Public Security Information:**
    Sensitive public security information includes information containing specific details of public security plans and arrangements or the detailed plans and drawings of public buildings and infrastructure facilities. Plans to prevent or respond to terrorist activity, to the extent such records set forth vulnerability and risk assessments, potential targets, specific tactics, or specific security or emergency procedures, the disclosure of which would jeopardize the safety of governmental personnel or the general public or the security of any governmental facility, building, structure, or information storage system, are also sensitive public security information.

  By law, information relating to the general adoption of public security plans and arrangements and budgetary information concerning the authorization or expenditure of public funds to implement public security plans and arrangements, or for the construction, renovation, or repair of public buildings and infrastructure facilities are not sensitive public security information and should be classified as Low Risk.

- **High Risk (Highly Restricted)**
  Data, if breached or disclosed to unauthorized users, has the potential to cause great harm or damage to personnel or institutions. High Risk information can only be disclosed under very specific conditions, if at all. State and/or federal law or other requirements often include specific guidelines for protecting High Risk data and systems. High Risk data and systems may also be referred to as Highly Restricted. High Risk data includes the following:

  a. **Personal Information and Personally Identifiable Information (PII)**
  Under state law, personal information is a person's first name or first initial and last name **in combination** with other identifying information. Identifying information is defined as the following:

  i. Social security or employer taxpayer identification numbers;
  ii. Driver's license, state identification card, or passport numbers;
  iii. Checking account numbers;
  iv. Savings account numbers;
  v. Credit card numbers;
  vi. Debit card numbers;
  vii. Personal Identification (PIN) Code;
  viii. Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names;
  ix. Digital signatures;
  x. Any other numbers or information that can be used to access a person's financial resources;
  xi. Biometric data;
  xii. Fingerprints;
  xiii. Passwords;
  xiv. Parent's legal surname prior to marriage;

The following table summarizes the PII and Sensitive PII (**Note:** The table is not exhaustive):

Table 2. Personally Identifiable Information and Sensitive Personally Identifiable Information

PII includes:	
Name, Email Address, Home Address, and Telephone Number	
Sensitive PII includes:	
If stand-alone:	**If paired with the above identifiers:**
Social Security Number (SSN)	Citizenship or Immigration Status
Employer Taxpayer Identification Numbers	Position Descriptions and Performance Plans Without Ratings
Driver’s License or State ID Number	Medical Information
Passport Number	Ethnic or Religious Affiliation
Alien Registration Number	Sexual Orientation
Financial Account Numbers (banking, credit, debit, etc.), or any other numbers or information that can be used to access a person’s financial resources	Account Passwords
Biometric Identifiers	Last 4 Digits of SSN
Personal Identification (PIN) Code.	Date of Birth
Digital Signatures	Criminal History
Biometric Data	Mother’s Maiden Name
Fingerprints	Electronic Identification Numbers
Passwords	Internet Account Numbers or Internet Identification Names

b. **State and Federal Tax Information** (FTI)
FTI is any return or return information received from the Internal Revenue Service (IRS) or secondary source, such as from the Social Security Administration (SSA). FTI includes any information created by the recipient that is derived from tax return or return information;

c. **Payment Card Industry (PCI) Data Security Standard (DSS)**
PCI DSS applies to the transmission, storage, or processing of confidential credit card data. This data classification includes credit card magnetic stripe data, card verification values, payment account numbers, personal identification numbers, passwords, and credit/debit card expiration dates;

d. **Personal Health Information (PHI)**
PHI is confidential individually identifiable information relating to the past, present, or future health status of an individual, including mental health information. This information is protected under the same controls as Health Insurance Portability and Accountability Act (HIPAA) of 1996 and state laws that address the storage of confidential state and federal personally identifiable health information that is protected from disclosure;

e. **Social Security Administration (SSA) Provided Information**
Information that is obtained from the SSA can include a Social Security number verification indicator or other PII data.

The following table summarizes the three (3) data classifications [Low Risk, Medium Risk (Restricted), and High Risk (Highly Restricted)]:

Table 3. Description and Types for Risk Classifications

	Risk Classification		
	Low Risk	**Medium Risk (Restricted)**	**High Risk (Highly Restricted)**
Description:	Information not specifically made confidential by state and/or federal law	Information made confidential by state and/or federal law, including the possibility of when it is combined with other data	Information made confidential by state and/or federal law that has the potential to cause great harm or damage to personnel or institutions if breached or disclosed to unauthorized users
Types:	• Information on publicly-accessible websites • Routine correspondence, email, and other documents.	• CIHA Personnel Records • Security Features • Sensitive Public Security Information	• PII • PCI DSS • PHI • State and FTI • SSA Provided Information • Attorney-Client Communications

System Risk Classification:

All systems must be classified into one (1) of these three (3) classes:

- Low Risk System;
- Medium Risk System;
- High Risk System.

These classifications are determined by the level of security that must be placed around the systems. A system receives a risk classification based on the data stored, processed, transferred, or communicated by the system and the overall risk of unauthorized disclosure. System Classifications for Risk are as follows:

a. **Low Risk System**
   Systems that contain only data that is public by state and/or federal law or directly available to the public via such mechanisms as the Internet. Desktops, laptops, and supporting systems used by CIHA are considered Low Risk systems unless they store, process, transfer, or communicate Medium Risk or High Risk data.

   Low Risk systems must maintain a minimum level of protection (e.g. passwords and data at rest restrictions) as outlined in the *CIHA Access Control Policy*. Low risk systems are also subject to state laws and may require legal review to ensure that only public data is released in response to a public records request.

   Low Risk systems that contain websites with high visibility are often a target of opportunity for compromise and defacement, and these types of breaches can potentially pose significant risk to CIHA. In addition, an unauthorized user may be able to gain access to a higher classified system.
b. **Medium Risk System**
   Stores, processes, transfers, or communicates Medium Risk data or has a direct dependency on a Medium Risk system. Any system that stores, processes, transfers, or communicates PII is classified as a Medium Risk system, at minimum.
c. **High Risk System**
   Stores, processes, transfers or communicates High Risk data or has a direct dependency on a High Risk system.

<u>Media Storage</u>
[NIST MP-4]
CIHA shall ensure the proper storage of data and information files for which they are responsible by doing the following:

a. Protecting and backing up stored data so in the event accidental or unauthorized deletion or misuse occurs, a restoration can occur;
b. Meeting all applicable statutory and regulatory requirements for data retention, destruction, and protection;
c. Protecting CIHA information by complying with the Retention of Records and Reports section of the *CIHA Compliance Plan*;
d. Ensuring encryption keys are properly stored (separate from data) and available, if needed, for later decryption. CIHA shall use encryption authorized by the CIHA CISO when using it to protect data;
e. Establishing change management procedures for the emergency amendment of data that occurs outside normal software functions and procedures;

f. Properly documenting and approving all emergency data amendments or changes and meeting all applicable statutory and regulatory requirements;
g. Physically controlling and securely storing media containing FTI;
h. Protecting information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures;
i. Requiring the encryption of data stored on secondary devices [devices that retain copies of data stored on primary data storage devices (i.e., backups)] to protect the highest level of information contained therein;
j. Storing only the minimum of public data necessary to adequately perform business functions. Sensitive or confidential data that is not needed for normal business functions, (e.g., the full contents of a credit card magnetic strip or a credit card PIN) should not be stored.

Media Archival:
CIHA shall consult with the CIHA CISO to select archival media that protects the integrity of the stored data for as long as the data are archived. In addition, the following data archiving requirements must be met:

a. When archiving data associated with legacy systems (systems that are no longer being used in operations), CIHA shall provide a method for accessing that data;
b. Classification of the back-up media so that the individual encountering the archive can determine the sensitivity of the data;
c. Storage of back-up media shall be maintained in a secure location, preferably at an off-site facility;
d. All back-up media shall be physically secured from theft and destruction:
    i. Migrating data to another system or archiving data shall be in accordance with the Retention of Records and Reports section of the *CIHA Compliance Plan*.

Media Transport

[NIST MP-5]

All CIHA users must observe the requirements for transferring or communicating information based on its risk, which are defined in the following table. Data stewards or assigned representatives may designate additional controls to further restrict access to further protect information; criteria to be followed includes:

a. Access to data shall be granted only after a business need has been demonstrated and approved by the data steward;
b. CIHA must use transmittals or an equivalent documented tracking method to ensure FTI and other Restricted or Highly Restricted data reaches its intended destination;
c. All media shall be transported by secured courier or other delivery method which can be accurately tracked;
d. Management approval shall be obtained before moving any media from a secure area;
e. Inventory logs of all media shall be maintained properly, and an inventory of these logs shall be performed at least quarterly.

The following table provides authorized methods for the transfer or communication of data, and the asterisks within the table are explained after:

Table 4. Risk Classification by Method of Transfer or Communication

Method of Transfer or Communication	**Risk Classification**		
	Low Risk	**Medium Risk (Restricted)**	**High Risk (Highly Restricted)**
Copying	No Restrictions	Permission of Data Custodian Advised	Permission of Data Custodian Advised
Storage	Encryption Optional	Encryption or Physical Access Control Required** No External Cloud Storage***	Encryption Required No External Cloud Storage***
Fax	No Restrictions	Encryption Required	Encryption Required
Electronic Mail	Encryption Optional	Encryption Required	Encryption Required
Spoken Word*	No Restrictions	Reasonable Precautions to Prevent Inadvertent Disclosure	Active Measures to Control and Limit Information Disclosure to as Few Personnel as Possible
Log Tracking Process	No Restrictions	Data Custodian is Required to Include Audit Trails for All Access and Destruction of Information	Data Custodian is Required to Include Audit Trails for All Access and Destructions of Information (See IRS 1075 Publication for Additional Storage Requirements for FTI)
Granting Access Rights	No Restrictions	Data Custodian or Designee Only	Data Custodian or Designee Only
Post (Mail)	No Restrictions	Physical Access Control	Physical Access Control (See IRS 1075 Publication for Additional Storage Requirements for FTI)
Release to a Third Party	Third Party Must be an Authorized User and Have a Job-Related Need****	Third Party Must be an Authorized User and Have a Job-Related Need****	Third Party Must be an Authorized User and Have a Job-Related Need****

* "Spoken Word" is defined as transmission over telephone or mobile phone, voicemail, answering machine, and face-to-face communication.

** Any mobile or portable computing devices such as, smart phones, and portable storage devices [e.g., compact disks (CDs), digital video disks (DVDs), and flash drives] that are used to conduct CIHA's business, must use FIPS-140-3 (and subsequent versions) validated encryption to protect all PII and confidential information that is stored on the device from unauthorized disclosure. It is highly recommended that physical locations with weak access controls, such as satellite offices, deploy full-disk encryption of Restricted and Highly Restricted data.

*** No external cloud storage is allowed unless explicitly authorized by the CIHA CISO.

**** Authorized users who are granted access to CIHA Information Systems per the *CIHA Access Control Policy*. Restricted information is only available to authorized personnel requiring access to the information as part of their job responsibilities per the *CIHA Access Control Policy*. Note: Third party access to federal data may be restricted through federal mandates.

Media Sanitization

[NIST MP-6]

Media must be sanitized in accordance with NIST Special Publication 800-88 revision 1 (and subsequent revisions), *Guidelines for Media Sanitization*. These sanitization methods ensure data is not unintentionally disclosed to unauthorized users. Media containing Highly Restricted data shall be sanitized prior to disposal, the release out of CIHA control, or the release for reuse using CIHA-approved sanitization techniques in accordance with applicable federal and/or CIHA policies and guidelines. The baseline for sanitizing media is shown in the following table:

Table 5. Risk Classification for Media Sanitization

Sanitization	**Risk Classification for Media Sanitization**		
	Low Risk	**Medium Risk (Restricted)**	**High Risk (Highly Restricted)**
	Not Required (Recommended)	Mandatory	Mandatory

Media Sanitization – Review, Approve, Track, Document, and Verify:
[NIST MP-6(1)]
CIHA shall protect data confidentiality and integrity through proper sanitization and disposal of obsolete equipment, as well as protect information by using secure software sanitization and disposal techniques.
All sanitization and disposal of records must be in accordance with federal and/or state laws, any CIHA program retention schedules, and NIST Special Publication 800-88 revision 1 (and subsequent revisions), *Guidelines for Media Sanitization.*

Though there are no specific restrictions for the sanitization and disposal of Low Risk data, shredding is generally recommended as a best practice. The following table summarizes sanitization and disposal methods for the three (3) data classifications.

Table 6. Risk Classification for Media Disposal

Sanitization	Risk Classification for Media Sanitization		
	🟩 Low Risk	🟨 Medium Risk (Restricted)	🟥 High Risk (Highly Restricted)
	No Restrictions (Optional)	Shredding, Degaussing, or Secure Disposal	Shredding, Degaussing, or Secure Disposal

Media Sanitization - Equipment Testing
[NIST MP-6(2)]
CIHA must test sanitization equipment and procedures quarterly to verify that the intended sanitization method is functioning as designed.

Media Sanitization - Nondestructive Techniques
[NIST MP-6(3)]
CIHA must apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to any information systems containing data deemed essential to CIHA. Because such storage devices can often contain malware, it is important to utilize an approved software solution for scanning the device before it is allowed to execute any commands on information systems.

Nondestructive techniques include, but are not limited to, endpoint protection (i.e. antivirus software).

Media Use

[NIST MP-7]

CIHA shall ensure that security controls are in place to protect the CIA of CIHA's data stored on information system storage media (throughout the storage media's life and disposal):

a. Access controls shall include physical protection of and accountability for removable storage media, minimizing the risk of damage to its stored data, unauthorized access, theft, and software licensing violations;

b. Any connection to non-CIHA-owned information system storage media, mobile devices, or computers to a CIHA-owned resource is prohibited, unless connecting to a guest network or guest resources. This prohibition, at CIHA's discretion, does not apply to an approved vendor who provides operational IT support services under contract;

c. The use of sanitation-resistant media that does not support sanitization commands (or if supported, the interfaces are not supported in a standardized way across these devices) is prohibited for use with Highly Restricted data. Sanitation-resistant media include, for example, compact flash, embedded flash on boards and devices, solid state drives, and USB removable media;

d. The *CIHA Internet and Electronic Mail Acceptable Use Policy* and Sec. 4.13. Use of phone, mail and office systems of the *CIHA Personnel Manual* shall define the proper use of information assets and include critical technologies, such as remote access technologies, removable electronic media, laptops, tablets, smartphones, email usage, and Internet usage.

Aggregation and Commingling:

Commingling of different risk classifications of data on the same media is prohibited. All attempts must be made to ensure that there is a physical separation of the different data types within the same media. When deemed impossible, the data must be classified and labeled appropriately to the highest classification level with the most stringent security controls implemented.

When data with different classifications is aggregated and summarized, the highest classification within the aggregated data must be applied to all of it.

CIHA shall prohibit the use of portable storage devices in CIHA information systems when such devices have no identifiable owner. By requiring portable storage devices to have identifiable owners (e.g., individuals, organizations, or projects), the risk of using technologies that have no identifiable owner is reduced, which allows CIHA to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion).