NORTH IOWA COMMUNITY ACTION HIPAA SECURITY POLICIES

Table of Contents

Administrative Safeguards

Physical Safeguards

Technical Safeguards

HIPAA Security Program

Policy #: 101

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to provide reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability (CIA) of information assets by protecting those assets from unauthorized access, modification, destruction, or disclosure.

North Iowa Community Action Organization (NICAO) will maintain a HIPAA Security Program that complies with core business objectives as well as applicable state and federal regulations. This program as described by NICAO's security policies and supporting plans and procedures, will clearly state the objectives, responsibilities, and enforcement requirements of NICAO.

The purpose of the NICAO HIPAA Security Program is to:

- Establish policies, procedures, plans, and standard tools to secure information in compliance with state and federal security requirements, using minimum levels of industry standards.
- Support NICAO and its mission to provide continuity of service to customers.
- Maintain trust with customers and stakeholders through the practice of good stewardship of information assets.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

The Scope is defined as all types of sensitive information, including all sensitive information, created by, received, or held by HIPAA covered NICAO. This information will be protected in any form including, but not limited to paper, electronic, or oral. HIPAA covered NICAO, as a hybrid organization, includes the components listed below.

As a Provider of Health Care

Designated Health Care Provider Components of NICAO

These areas of NICAO are subject to HIPAA regulations and penalties:

- Family Health Center
- Executive Director of NICAO

Internal Business Associates of NICAO Health Care Components of the Family Health Center:

- Fiscal Operations
- Human Resources
- Management Information Systems
- Board of Directors

As a Flexible Savings Health Plan

Designated Health Plan Components of NICAO

These areas of NICAO are subject to HIPAA regulations and penalties:

- Human Resources
- Executive Director of NICAO

Internal Business Associates of NICAO Health Care Components of the Flexible Savings Health Plan:

- Fiscal Operations
- Management Information Systems
- Board of Directors

NICAO will implement safeguards determined to be reasonable and appropriate to protect its information assets to maintain the confidentiality, integrity, and availability (CIA) of those assets.

Policies, plans, and procedures created in support of this HIPAA Security Program address at a minimum:

- Administrative safeguards
- Physical safeguards
- Technical safeguards

In addition, all security policies, and procedures shall be reviewed and evaluated (based on any environmental and operational changes) on an annual basis by the Information Security Officer and team.

Responsibilities:

All individuals, groups, and organizations identified in the scope of this policy are responsible for:

- Compliance with all NICAO HIPAA Security Policies.

The NICAO Information Security Officer, as defined by, Assigned Security Responsibility Policy, is responsible for:

- The development, implementation, and maintenance of NICAO HIPAA Security Policies.
- Working with employees to develop procedures and plans in support of the HIPAA Security Policies.
- The retention of documentation required by the regulation for 7 years from the effective date.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

Procedures developed in support of the HIPAA Security Program will address (but are not limited to):

- Information system activity review
- Workforce clearance
- Termination
- Security incident handling
- Access authorization, establishment, and modification
- Contingency operations procedures
- Physical access control and validation procedures
- Updating maintenance records
- Workstation use
- Media disposal and re-use
- Accountability
- Data backup and storage procedures
- Emergency access
- Automatic logoff

Risk Analysis Policy

Policy #: 102

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to conduct an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information held by the organization.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will conduct an accurate and thorough assessment of risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information, including EPHI. Such risk analysis activities will be conducted at least once per year and must result in a comprehensive Risk Analysis Report that summarizes the risks, vulnerabilities to the confidentiality, integrity and availability of sensitive information. This report must also identify recommended safeguards and prioritize all such risks and vulnerabilities.

Responsibilities:

The Information Security Officer is responsible for coordinating all activities associated with risk analysis. All involved employees who assist with risk analysis activities will be trained in appropriate security compliance requirements and NICAO's security policies with the objective that they understand their responsibilities and duties to reduce the risk of security violations.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

Risk is defined as the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence.

All risk analysis activities shall be organized into three phases. These phases are:

- Phase I: Documentation Phase
- Phase II: Risk Assessment Phase
- Phase III: Safeguards Determination Phase

The minimal activities that NICAO will conduct in each phase are as follows:

Phase I: Documentation Phase

- Identify what sensitive information is collected
- Identify systems with sensitive information
- Document the purpose of these systems
- Document the flow of sensitive information

Phase II: Risk Assessment Phase

- Identify vulnerabilities and threats to sensitive information
- Describe the risks
- Identify controls
- Describe the level of risk

Phase III: Safeguards Determination Phase

- Recommend safeguards for sensitive information

- Determine residual risk to sensitive information

The results of all identified risk analysis activities along with the safeguard and other recommendations must be summarized with supporting documentation in a risk analysis report.

A risk analysis report shall be compiled on a periodic basis and at minimum, annually.

Risk Management Policy

Policy #: 103

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement security measures sufficient to reduce risks and vulnerabilities to a **reasonable and appropriate level** to comply with impacted regulations.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with impacted regulations.

Responsibilities:

The Information Security Officer has the responsibility to:

- Ensure that appropriate risk analysis covering, at a minimum, all sensitive information are performed at a frequency of at least once a year
- Approve risk mitigation plans, risk prioritization, and the elimination or minimization of risks
- Facilitate timely actions, decisions and remediation activities

The Information Security Officer must be supported by NICAO managers to identify and prioritize risks to sensitive information. Risk management is an essential management function at NICAO.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce the risk to an acceptable level.

Risk management related activities are essential to help identify critical resources needed to support NICAO and the likely threat to all such resources.

The principal goal of NICAO's risk management policy is to protect the organization, especially its sensitive information, and its ability to perform its mission.

The objective of performing risk management is to enable NICAO to accomplish its mission by:

- Better securing systems that store, process or transmit sensitive information.
- Enabling management to make well-informed risk management decisions to justify the expenditures that are a part of the IT and other budgets.
- Assisting management in authorizing or evaluating systems on the basis of supporting documentation resulting from the performance of risk management.

Risk management consists of three phases:

- Phase I: Risk Assessment
- Phase II: Risk Mitigation
- Phase III: Evaluation and Assessment (Residual Risk)

The activities that NICAO will conduct in each phase are as follows:

Phase I: Risk Assessment

- System characterization
- Threat identification
- Vulnerability identification
- Safeguard analysis
- Likelihood determination
- Impact analysis
- Risk determination
- Safeguard recommendations
- Results documentation

Phase II: Risk Mitigation

- Prioritize actions
- Evaluate recommended safeguard options
- Conduct cost-benefit analysis
- Select safeguards
- Assign responsibility
- Develop safeguard implementation plan
- Implement selected safeguards

Phase III: Evaluation and Assessment (Residual Risk)

- Evaluate safeguards deployed
- Evaluate security policies

Sanction Policy

Policy #: 104

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose of this policy is to apply appropriate sanctions against workforce members who fail to comply with the security policies or procedures of NICAO.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will ensure all members of its workforce comply with the Security Policies of the organization as well as state and federal regulations such as HIPAA and the HITECH Act by applying sanction and disciplinary actions appropriate for the breach of policy.

Responsibilities:

All individuals identified in the scope of this policy are responsible for:

- Compliance with any sanction that is applied to them under this policy

The NICAO Information Security Officer is responsible for:

- Reviewing reported security incidents and violations of security policy and levying, based on the gravity of the breach, appropriate sanctions upon the workforce member

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will appropriately discipline employees and other workforce members for any violation of any security policy or procedure to a degree appropriate for the gravity of the violation. These sanctions include, but are not limited to, re-training, verbal and written warnings and immediate dismissal from employment.

In addition, workforce members who knowingly and willfully violate state or federal law for improper use or disclosure of a patient’s information are subject to criminal investigation and prosecution or civil monetary penalties. NICAO and members of the NICAO workforce will not intimidate or retaliate against any workforce member or patient that reports the incident.

In addition, NICAO will:

- Record all disciplinary actions taken, provide a copy to the employee, and file the original with Human Resources.
- Investigate all security incidents or violations and mitigate to the extent possible any negative effects of the incident in a timely manner.
- NICAO will ensure all sanctions in this policy are consistent with Human Resources policies.

Information System Activity Review Policy

Policy #: 105

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will clearly identify all critical systems that process sensitive information. NICAO will implement security procedures to regularly review the records of information system activity on all such critical systems that process sensitive information.

Responsibilities:

The Information Security Officer will clearly identify:

- The systems that must be reviewed.
- The information on these systems that must be reviewed and the appropriate review method.
- The types of access reports that are to be generated.
- The security incident tracking reports that are to be generated to analyze security violations.
- The individual(s) responsible for reviewing all logs and reports.

When determining the responsibility for information review, a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will clearly identify all critical systems that process sensitive information. NICAO will implement security procedures to regularly review the records of information system activity on all such critical systems that process sensitive information.

The information that will be maintained in audit logs and access reports including security incident tracking reports must include as much as possible, of the following, as reasonable and appropriate:

- User IDs
- Dates and times of log-on and log-off
- Terminal identity, IP address and/or location, if possible
- Records of successful and rejected system access attempts

NICAO will attempt wherever reasonable, appropriate, and technically feasible to record:

- Who (Unique User ID), did
- What action (Read, write, edit, delete, print, etc.), to
- What data (Server, DB, instance, table, row, field),
- When (Enterprise wide timestamp), and from
- Where (Terminal ID, IP address, local or remote access)

Safeguards must be deployed to protect against unauthorized changes and operational problems including:

- Alterations to the message types that are recorded
- Log files being edited or deleted

Assigned Security Responsibility Policy

Policy #: 106

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose of this policy is to identify the security official who is responsible for the development and implementation of the policies and procedures required by the HIPAA Security Rule 164.308(a)(2).

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will assign final responsibility of security to one individual who will be referred to as the “Information Security Officer.”

Responsibilities:

All individuals, groups, and organizations identified in the scope of this policy are responsible for:

- Supporting and providing assistance to the Information Security Officer whenever necessary when the Information Security Officer is acting in the role described under the policy section.

The NICAO Information Security Officer, as defined by the Assigned Security Responsibility Policy, is responsible for all aforementioned responsibilities described in the policy section.

The Executive Director is responsible for:

- Duly appointing a capable Information Security Officer and replacing that person if they are not able to fulfill their responsibilities or are no longer affiliated with the organization.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will assign final responsibility of security to one individual who will be referred to as the “Information Security Officer.” This individual’s ultimate goal is to protect the confidentiality, integrity, and availability (CIA) of critical information assets at NICAO and to ensure compliance with applicable regulations.

Responsibilities of the Information Security Officer include (but are not limited to):

- Ensuring all policies, procedures, and plans required by regulations are developed, implemented, and maintained as necessary.
- Monitoring changes in legislation that may affect NICAO and its security position.
- Monitoring changes and advances in technology that may affect NICAO and its security position.
- Performing technical and non-technical evaluations or audits on security processes in order to find and correct weaknesses and guard against potential threats to security.
- At the direction of the Executive Director, acting as an internal consultant and potentially as an external spokesperson for NICAO in all issues related to security.
- Ensuring a system for reporting and responding to security incidents (as well as violations of regulations) is in place and functioning.
- Delivering, on an ongoing basis, security awareness training to all members of the workforce.

If the Information Security Officer is not able to meet the requirements of this policy, or is no longer affiliated with the organization, NICAO will assign these responsibilities to a new Information Security Officer.

Authorization and/or Supervision Policy

Policy #: 107

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement procedures for the authorization and/or supervision of workforce members who work with sensitive information or in locations where it may be accessed.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will implement security safeguards to ensure that all members of the workforce, who have access to sensitive information, including operations and maintenance employees, are authorized and supervised appropriately.

Responsibilities:

The Information Security Officer is responsible for ensuring the implementation of requirements related to the Authorizations and/or Supervision Policy. The activities may include:

- Supervision of some members of the workforce
- Proper access authorizations on the basis of job roles or functions
- Clearance procedures
- Maintenance of access authorization records

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will implement security safeguards to ensure that all members of the workforce who have access to sensitive information:

- Need the access they have;
- Have the access they need;
- Understand the limits of access to sensitive information
- Understand how to authenticate themselves to the system or application

NICAO will determine and assign managers who shall in turn determine what members of the workforce shall have access to sensitive information.

Workforce Clearance Procedure

Policy #: 108

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement procedures to determine that the access of a workforce member to sensitive information is appropriate.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO shall require that effective personnel screening processes be applied to allow a range of implementation, from minimal procedures to more stringent procedures, based on the results of the risk analysis performed.

Responsibilities:

The Information Security Officer is responsible for ensuring the implementation of the requirements of the Workforce Clearance Procedure.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO requires that effective personnel screening processes are applied, from minimal procedures to more stringent procedures, based on the job functions of the individual and the results of the risk analysis performed.

Application and resume information must be validated. This includes validation of information such as:

- Reference checks for the employers identified in the resume or employment application.
- Academic credentials identified in the resume or employment application.
- Criminal background checks.

All procedures will be consistent and in coordination with Human Resources Policies.

Termination Procedure

Policy #: 109

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement procedures for quickly, securely and completely terminating access to sensitive information when the employment of a workforce member ends.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will terminate access to all systems and facilities when any member of the workforce has been terminated or no longer requires access to information or facilities in order to perform their assigned job function.

Responsibilities:

The Information Security Officer is responsible for ensuring that all activities identified in the Termination Procedure occur.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

Any termination of a workforce member must immediately result in the Human Resources (HR) and the Information Technology (IT) departments coordinating their activities to ensure:

- Password access is immediately revoked;
- Access to all systems and applications is revoked;
- The workforce member is removed from any systems or applications that processed sensitive information;
- Any keys and IDs provided to the workforce member during their employment are returned, and
- The workforce member is not provided access to their desk or office or, if provided, the access is limited and carefully supervised.

If listed items cannot be returned to NICAO for any reason, compensatory controls must be implemented. Termination of access will be verified and segregation of duties will be applied to ensure immediate and complete termination of all access including electronic and physical.

Human Resources may conduct an exit interview and document any issues or concerns related to the workforce member.

Access Authorization Policy

Policy #: 110

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement policies and procedures for granting access to sensitive information, for example, authorization required to access a workstation, transaction, program, process or other mechanism.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO shall implement policies and procedures for granting access to sensitive information including authorization required to access a workstation, transaction, program, process or other mechanism.

Responsibilities:

The Information Security Officer is responsible for:

- Ensuring the implementation of the Access Authorization Policy.
- Reviewing the access rights of individuals to ascertain that they are aligned with the individual’s job duty or function.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO shall determine and assign data owners for all sensitive information and the data owner shall ultimately determine which members of the workforce shall have authorization to access sensitive information.

Each individual’s job description must be reviewed to determine their:

- Individual user access
- The security group that this individual belongs to

The principle of least privilege and separation of duties shall be factors that influence the access rights granted to an individual or an entity.

The fundamental principal of “need to know” will be applied within NICAO to determine access privileges.
Access to sensitive information will be granted only if that individual has a legitimate business need for the information. Reasonable efforts will be made to limit the amount of information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Access Establishment and Modification Policy

Policy #: 111

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will create and maintain Access Control Lists (ACLs) and other access control-related capabilities to ensure that access is limited to approved rights.

Responsibilities:

The Information Security Officer is responsible for:

- Ensuring the implementation of the Access Establishment and Modification Policy.
  Reviewing the access rights of individuals to ascertain that they are aligned with the individual job function.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

Access shall be:

- Granted according to documented procedures;
- Limited to that access which is required to perform the assigned job function;
- Thoroughly documented,
- Periodically reviewed by assigned managers, and
- Modified as required by job function or business need.

A regular review shall be conducted to ensure that access rights for each individual or entity are consistent with established policies and job functions.

Security Reminders Policy

Policy #: 112

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement and ensure that periodic security reminders are distributed to all members of the workforce.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will periodically send out security reminders to all members of the workforce.

Responsibilities:

The Information Security Officer is responsible for periodically sending out security reminders to members of the workforce.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

The security reminders shall reflect security awareness concerns and issues that have the potential to compromise the confidentiality, integrity or availability of sensitive information.

The security reminders may also communicate new or on-going security activities and initiatives.

Protection from Malicious Software Policy

Policy #: 113

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement procedures for guarding against, detecting, and reporting malicious software.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will deploy malicious software identification, prevention, and removal technology at the perimeter of its network, on all servers (including email servers), and on individual end-user systems.

Responsibilities:

The Information Security Officer is responsible for:

- Ensuring that malicious software checking programs are installed both on the perimeter of the network and on individual end-user systems.
- Identifying all critical systems and network components that are vulnerable to malicious software.
- Implementing malicious software checking capability on all such identified systems.

Members of the workforce are responsible for:

- Not configuring or introducing any modifications to systems or applications to prevent the execution of malicious software checking programs.
- Immediately contacting the Information Security Officer or respective manager by phone or in person, not by email, if there are any indications of a threat or malicious software infection.
- Participating in all security awareness training programs and applying the knowledge in preventing, detecting, containing and eradicating malicious software.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will:

- Subscribe to updates to malicious software checking programs.
- Ensure that updates are being received and applied on a daily basis.
- Conduct security training that will include information on:
  - Potential harm that can be caused by malicious software.
  - Prevention of malicious software such as viruses.
  - Steps to take if malicious software such as a virus is detected.

Log-In Monitoring Policy

Policy #: 114

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement procedures for monitoring log-in attempts and reporting discrepancies.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will configure all critical components that process, store or transmit sensitive information to record log-in attempts, both successful and unsuccessful, as well as automatic lock out and reporting after three failed attempts.

Responsibilities:

The Information Security Officer is responsible for:

- Ensuring the implementation of the Log-in Monitoring Policy.
- Identifying all critical systems that will record log-in attempts, both successes and failures.
- Ensuring the regular monitoring of these logs by authorized individuals.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

- The security awareness training must include information about the importance of monitoring log-in success or failure.
- The information provided must address the steps for checking last log-in information.

Password Management Policy

Policy #: 115

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement procedures for creating, changing and safeguarding passwords.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will implement procedures and training to ensure that all members of the workforce, including privileged users and IT administrators, create secure, complex passwords, modify those passwords on a periodic and regular schedule, and safeguard their passwords appropriately.

Responsibilities:

The Information Security Officer is responsible for:

- Ensuring the implementation of the Password Management Policy.
- Authorized the periodic and/or random password cracking or guessing and requiring any identified passwords to be changed by the user.

Members of the workforce are responsible for:

- Not sharing their passwords.
- Treating all passwords as sensitive, confidential information.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO requires that:

- All production system-level passwords must be part of the Information Security Officer’s administered global password management database.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where the Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of “public,” “private,” and “system,” and must be different from the passwords used to log in interactively. A keyed hash must be used where available (for example, SNMPv2).

Users must select strong passwords.

Strong passwords have the following characteristics:

- At least eight characters in length
- A mixture of letters, numbers, and symbols
- Changed according to a schedule set by the Security Officer
- Different from the previous 4 passwords
- Not contain the user’s User ID

Poor, weak passwords have the following characteristics:

- Less than eight characters

- A word found in a dictionary (English or foreign)
- A common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software
    - Birthdays and other personal information such as addresses and phone numbers
    - Word or number patterns (e.g., aaabbb, qwerty, zyxwvuts, 123321, etc.)
- Any of the above spelled backwards
- Any of the above preceded or followed by a digit (for example, secret1, 1secret)

Systems that authenticate must require passwords of users and must block access to accounts if more than three unsuccessful attempts are made.

Other than IT related issues, the following password guidelines must be followed:

- Don’t reveal a password over the phone.
- Don’t reveal a password in an email message.
- Don’t talk about a password in front of others.
- Don’t hint at the format of a password, like, "my family name."
- Don’t reveal a password on questionnaires or security forms.
- Don’t share a password with family members.
- Don’t reveal a password to co-workers.

If someone demands a password, refer them to this document or have them contact the Information Security Officer.

The “Remember Password” feature of applications such as Internet Explorer, Google Chrome or operating systems such as Windows must not be used.

Every effort should be made to maintain the confidentiality of all passwords.

Response and Reporting Policy

Policy #: 116

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to NICAO, and document security incidents and their outcomes.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will:

- Identify, research, and respond to any suspected security incidents;
- Mitigate, to the extent practicable, any harmful effects of any suspected or actual security incidents; and
- Maintain appropriate documentation for all security incidents.

Responsibilities:

The Information Security Officer is responsible for:

- Training all members of the workforce on appropriate reporting of security violations.
- Determining if the security incident is "serious" or "non-serious" and the appropriate level of response to the security incident. All such responses must be in accordance with established policies and procedures.
- At a minimum, the Information Security Officer and/or his/her team must immediately consider a response that includes:
    - Disconnecting the affected system from the network (should not remove power from the system)
    - Determining if the incident is accidental or intentional
    - Identifying all system-related information such as:
        - Hardware address
        - System name
        - IP address
        - Sensitive data processed by the system
        - Applications installed on the system
        - Location of the system

Completing a Security Incident Report for each security incident with as much information as possible about the following:

- Contact information of the person reporting the incident (name, phone, address, email)
- Date and time of the incident
- Detailed description of the incident
- Any further information, such as unusual activities or individuals associated with the incident

The Information Security Officer and other members of management are jointly responsible for:

- Mitigating to the extent possible, any harmful effects of security procedures.
- Deciding when it is appropriate to contact law enforcements officials about a security incident that has been characterized as serious.
- Leading activities that bring NICAO into compliance with regulatory requirements.

Members of the workforce are responsible for:

- Immediately reporting any and all suspected violations of information security to the Information Security Officer. All incident reporting and response activities must be conducted strictly on a need-to-know basis.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):
If the security incident construes a breach of EPHI, please immediately take the following steps.

This policy requires addressing the following seven steps:

1. Prepare for a security incident.
2. Detect and report security incidents.
3. Assemble the incident response team.
4. Limit further damage.
5. Gather evidence.
6. Fix the damage.
7. Analyze the incident.

Data Backup Plan

Policy #: 117

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to establish and implement procedures to create and maintain retrievable exact copies of sensitive information in the event of equipment failure or damage.

To ensure the NICAO has a dependable backup for data recovery in the event of equipment failure or damage.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will

- Create and maintain exact, retrievable copies of sensitive information.
- Ensure that sensitive data is backed up on a regular basis so as to minimize the loss of data in the event of an incident or disaster.
- Ensure that backup media is periodically tested to ensure suitable quality and reliable data restoration.

Responsibilities:

The Information Security Officer will be responsible for implementing the requirements of the Data Backup Plan.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

In developing the backup schedule, the Information Security Officer will consider factors such as:

- What data (systems, files, directories, and folders) should be backed up?
- How frequent are backups done?
- Who is responsible/ authorized to retrieve the media?

Disaster Recovery Plan

Policy #: 118

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to establish and implement as needed procedures to restore any loss of data.

A Disaster Recovery Plan applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. A disaster recovery plan refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency.

A Disaster Recovery Plan provides a blueprint to continue business operations in the event that a catastrophe occurs. The disaster recovery plan must include contingencies for the period of time of the disaster and until the recovery plan can be completely implemented. The price for not developing a disaster recovery plan is that NICAO may find it difficult to continue to be in business or potentially suffer a significant loss.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will develop and maintain a Disaster Recovery Plan. The Information Security Officer will ensure the development of a Disaster Recovery Plan document.

Responsibilities:

The Information Security Officer will be responsible for implementing the requirements of a Disaster Recovery Plan.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will assign final responsibility of security to the Information Security Officer.

The Information Security Officer is to ensure the development of a Disaster Recovery Plan document. This document includes the following sections:

1. Purpose: a statement describing the goal of the disaster recovery plan.
2. Scope: identifies the specific locations/sites and critical systems that are a part of the Disaster Recovery Plan.
3. Assumptions: identifies the foundation that the plan is based on.
4. Team: identifies the Team lead for the activity as well as members of the IT organization and others that will be involved in the disaster recovery process.
5. Notification: establishes the formal communication required to contact members to alert them of the incident.
6. Damage assessment and reporting: describes the process of analyzing the extent of damage to systems and sites and includes reports that identify recommendations for management.
7. Activation: describes the process to start disaster recovery activities.
8. Recovery operations: describes the steps to recover critical systems and applications at the recovery site. This section would include information on data recovery based on the backed up data in the Data Backup Plan.
9. Return to normal operations: describes the procedures for the full recovery of all data and a complete return to normal processing of all business functions.

Emergency Mode Operation Plan

Policy #: 119

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to establish and implement as needed procedures to enable continuation of critical business processes for protection of the security of sensitive information while operating in an emergency mode, as defined below.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO Information Security Officer must identify the levels of emergencies and associated responses. The Information Security Officer must develop specific components of the Emergency Mode Operations Plan.

Responsibilities:

The Information Security Officer will be responsible for implementing the requirements of an Emergency Mode Operation Plan.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

The Information Security Officer must identify the levels of emergencies and associated responses. This may be based on the magnitude of the incident or disaster. For example:

- Level 1 Emergency may relate to a loss of business function or a specific part of a location/site.
- Level 2 Emergency may be based on an incident impacting multiple business functions or multiple locations/sites.
- Level 3 Emergency may be based on a significant disruption to several business functions or substantial damage at one or more locations/sites.

The specific components of an Emergency Mode Operation Plan must include:

- Identification of crisis management team members throughout the organization who will address strategic response of the organization in an emergency.
- Identification of support team members who will address tactical response of the organization in an emergency.
- Identification of a command center or other specifically designated facility to be utilized during emergency mode operation.
- Process for acquisition of additional human resources with applicable skill sets if current human resources are geographically restricted.
- Procedures and checklists to provide for the orderly transition and restoration of normal business operations (e.g., moving from the impacted site to the alternate site).
- Coordination of available critical facilities for alternate processing and business workspace for continuing operations in the event of an emergency.
- Communication plan for internal employees as well as external business partners and other stakeholders that addresses essential issues (e.g., operational status, Human Resources, and financial concerns).
- Procedures to ensure that health and safety issues are addressed.

Testing and Revision Procedures

Policy #: 120

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement procedures for periodic testing and revision of contingency plans.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will ensure that all contingency plans are tested and revised, as necessary, on a periodic basis.

Responsibilities:

The Information Security Officer will be responsible for implementing the requirements of Testing and Revision Procedures.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

Testing and revision procedures are procedures for processing of periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary. These written testing and feedback mechanisms are the keys to successful testing.

The Information Security Officer must ensure that procedures for testing and revision need to address the following:

- Sufficient awareness and training of all personnel on how to react in the event of a disaster or other business interruption.
- Validation of the Disaster Recovery and Emergency Mode Operation Plans to ensure that processes and procedures are effective.
- Identification of weaknesses in the Disaster Recovery and Emergency Mode Operation Plans and procedures to mitigate identified weaknesses.
- Procedures to ensure that the Disaster Recovery and Emergency Mode Operations Plans remain current and active.
- Procedures that test interdependencies among critical business processes, applications, and systems.
- Procedures that test the adequacy of equipment in place to fulfill the Disaster Recovery and Emergency Mode Operations Plans.
- Periodic updates and testing of all procedures and components of the Disaster Recovery and Emergency Mode Operation Plans.

Applications and Data Criticality Analysis

Policy #: 121

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to assess the relative criticality of specific applications and data in support of other contingency plan components.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO shall assess the relative criticality of applications and data to support the Disaster Recovery & Emergency Mode Operations Plans.

The relative criticality shall be documented and approved by executive management in order to establish the priority of recovery capabilities and activities.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the requirements of Applications and Data Criticality Analysis.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO should assess the “critical” areas of the business, which would include:

- Critical business functions
- Critical infrastructure
- Critical sensitive information or records

Evaluation Policy

Policy #: 122

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to perform a technical and non-technical evaluation that establishes the extent to which NICAO's HIPAA Security Policies and Procedures meet the requirements of impacted regulations.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will evaluate the technical and non-technical implementations of its HIPAA Security Policies.

This evaluation will be completed on a regular basis, at least annually, and in response to environmental or operational changes affecting the security of sensitive information.

The evaluation will determine the effectiveness of, and adherence to, NICAO policies as well as to ensure compliance with U.S., State and Federal regulations.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the requirements of this policy.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will evaluate the technical and non-technical implementations of its HIPAA Security Policies and Procedures at least annually, as well as when any of the following events occur:

- There is a change to any state or federal regulation that may affect the NICAO HIPAA Security Policies;
- There is a new state or federal regulation that may affect the policies;
- There has been a significant breach of security or other security incident within NICAO, and/or
- Any other time the Information Security Officer feels there is a need to evaluate the HIPAA Security Policies at NICAO.

Should a policy or procedure be found to be ineffective, missing, or otherwise flawed, NICAO will:

- Amend (or add) the policy or procedure in a timely manner, and
- Communicate the new policy or procedure to the affected workforce members and ensure that they understand the changes.

Business Associate Agreement and Other Arrangements Policy

Policy #: 123
Version #: 1.0
Effective Date: 05/15/18

Purpose:

The purpose is to obtain satisfactory assurances that the Business Associate will appropriately safeguard all sensitive information in accordance with applicable regulations.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will identify all organizations that process sensitive information on behalf of NICAO as well as all organizations for which NICAO collects, processes, or transmits sensitive information. All such business partners will require the implementation of a Business Associate Agreement(s) executed by NICAO.

NICAO will execute a Business Associate Agreement (BAA) with all Business Associates of NICAO, and will further require any subsequent Business Associates to execute a similar agreement.

Responsibilities:

The Information Security Officer will:

- Review all Business Associate Agreements and modify them as necessary to ensure compliance with this standard.
- Review the flow of sensitive information to identify all possible organizations that access sensitive information and may be required to execute a BAA or other legal agreement to ensure compliance with the applicable regulations.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

Each organization that provides data transmission of protected health information to NICAO (or its Business Associate) and that requires access on a routine basis to such protected health information or each vendor that contracts with NICAO to offer a personal health record to patients as part of its electronic health record, is required to enter into a Business Associate Agreement with NICAO.

NICAO will establish the flow of sensitive information to all outside entities and identify how such information is transmitted, and the requirements for processing sensitive information at the business associate site.

NICAO will review all existing BAAs and ensure that all such agreements are modified with Addendums or revised for compliance with impacted regulations.

The termination of an agreement with the Business Associate must result in return or destruction of all sensitive information by the Business Associate.

Business Associates must train all members of their workforce that process or come into contact with sensitive information. This training must include awareness of the requirements of the appropriate regulation as well as information about the business associate’s security policies and procedures.

NICAO must have the right to audit the Business Associate in the event of violations related to its sensitive information.

NICAO must reserve the right to take “reasonable steps” including canceling the BAA without penalty.

If the Business Associate intends to process or transmit NICAO sensitive information outside the United States of America then NICAO will be informed of specific details related to such processing or transmission and reserves the right to not authorize any such flow of sensitive information.

Business Associates must comply with HIPAA standards:

- 164.308-Administrative Safeguards;
- 164.310-Physical Safeguards;
- 164.312-Technical Safeguards;
- 164.316-Policies and procedures and documentation requirements and
- 164.504(e)-Uses and disclosures: Organizational requirements

Business Associates must comply with all applicable HITECH regulations.

A Business Associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify NICAO of such breach within 72 hours of its discovery. Such notice shall include the identification of each patient whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach.

A Business Associate may not receive compensation in exchange for any protected health information without authorization from patient. (Except for Public Health Activities, Research, Treatment, Health Care Operations, Exchanges with Business Associate, with patient, or as otherwise determined by the Secretary of Health and Human Services.)

NICAO may account for their own disclosures of patient information and then provide the name and contact information of the Business Associate for additional disclosure details. If requested by the patient, the Business Associate must account for their disclosures under a separate cover.

Contingency Operations Policy

Policy #: 201

Version #: 12.0

Effective Date: 05/15/18

Purpose:

The purpose is to establish and implement as needed procedures that allow facility access in support of restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will develop contingency operation procedures to facilitate access for emergency response.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the Contingency Operations Policy.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will develop contingency operation procedures to address emergency response.

These procedures will include:

- Notification
- Evacuation
- Equipment tests
- Training
- System shutdown

For example, the area of emergency notification procedures would include activities such as:

- Contacting managers as required.
- Evacuate the building if required.
- Conduct a damage assessment.
- Create a damage assessment report and communicate to senior management.
- Determine if the damaged site can be repaired and used.
- Establish time objectives for activities.

Facility Security Plan

Policy #: 202

Version #: 12.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will develop a Facility Security Plan to safeguard facilities and premises from unauthorized physical access, tampering or theft including the equipment present in all such facilities.

All equipment that collects, stores, processes, or transmits electronic personal health information will be protected from unauthorized access at all times.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the requirements of the Facility Security Plan. The Information Security Officer is responsible for reviewing and updating the plan as necessary.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will develop a Facility Security Plan with the objective of safeguarding facilities and premises from unauthorized physical access, tampering or theft including the equipment present in all such facilities.

The Facility Security Plan must define the security perimeter of all buildings and sites. Further, the plan should ensure that all external doors are adequately secured against unauthorized access by installing locks or other access control devices.

Controls need to be deployed to protect against theft or other damage to the extent possible.

Access Control and Validation Procedures

Policy #: 203

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control access to software programs for testing and revision.

To ensure that employees are able to access the information that is appropriate and required in their positions and that all patient information remains confidential.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will configure facility access controls to validate all access by members of the workforce to facilities and systems. Access controls will be enforced to ensure that the only access to sensitive information is by authorized members of the workforce.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the requirements of the Access Control and Validation Procedures.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will develop procedures for receiving and escorting visitors. Visitors must complete an entry in the visitor log book at the reception desk and be escorted to appropriate areas inside the facility.

Maintenance Records Policy

Policy #: 204

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will document all repairs and modifications to the facility that could affect the confidentiality, integrity, or availability of EPHI. All records will be securely retained for a time period as dictated in the NICAO's document retention policy.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the Maintenance Records Policy.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary action. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

The Information Security Officer will identify and document changes related to the hardware components essential to security. Security modifications made to physical components of a facility by outside vendors will be documented in the visitor log book and securely stored.

Workstation Use Policy

Policy #: 205

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access sensitive information.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will ensure that workstations and other computing devices are being used for work related purposes only.

All NICAO workstations will be utilized in a secure, approved manner, by authorized personnel only, and in such a way that the confidentiality, integrity, and availability of EPHI are not jeopardized.

NICAO will ensure that access is not permitted to NICAO workstations by individuals that are not authorized members of the NICAO workforce.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of this policy.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

Workstations and other computing devices that are owned or operated by NICAO are to be used for work-related purposes only. This includes, but is not limited to, Internet and Web access as well as the use of email at NICAO.

Workforce members should not expect any level of personal privacy as their activities, emails, files, and logs may be viewed at any time by the Information Security Officer or other members of management in support of this and other policies and procedures. NICAO may revoke the access rights of any individual at any time in order to protect or secure the confidentiality, integrity, and availability of sensitive information or to preserve the functionality of electronic information systems.

NICAO will implement reasonable and appropriate measures to secure its computing devices used to access sensitive information. These measures will include, but are not limited to the following:

- All user and administrator accounts must be protected by some form of authentication.
- All users accessing NICAO's computing devices must have and use a unique user ID.
- Procedures must be maintained that implement security updates and software patches in a timely manner.
- Procedures must be maintained that require users to run an up-to-date anti-virus program on all computing devices at NICAO.
- All unnecessary and unused services (or ports) must be disabled.
- Measures must be taken to physically protect computing devices located in public areas and devices located in public areas will be situated as to block unauthorized viewing and/or will have screen savers that black out the screen. These computers will also have screen savers that automatically activate following a brief period of inactivity.

Workstation Security Policy

Policy #: 206

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement physical safeguards for all workstations that access sensitive information and to restrict access to only authorized users.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will implement physical safeguards for all workstations that access sensitive information to restrict access to authorized users only.

Responsibilities:

All individuals identified in the scope of this policy are responsible for:

- Using NICAO computing devices for work-related purposes only.
- Following all procedures implemented by the Information Security Officer related to this policy.

The NICAO Information Security Officer is responsible for:

- Maintaining procedures required to support this policy, and
- Supporting and ensuring compliance by workforce members

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

All members of the workforce will be trained on the appropriate and authorized use of workstations as part of the security awareness training.

Workstations will be positioned such that the monitor screens and keyboards are not within view of unauthorized individuals.

Users will log off prior to leaving their workstations. Users will store any written passwords in secure locations only. Under no circumstances will any password information be posted on the workstation or accessible anywhere in its vicinity.

Workstations must be labeled to identify function and location and assist with compliance with access control procedures.

Workstations must:

- Ensure the confidentiality of sensitive information.
- Employ a password-protected screen saver and/or workstation locking mechanism when the workstation is unattended.
- Ensure routine back up of all critical data.
- Require virus scanning of media prior to use.

Users of workstations must:

- Properly log off their workstation at the end of the business day.
- Only use approved software on NICAO systems.
- Use workstations and software in accordance with contract agreements and copyright laws.

Disposal Policy

Policy #: 207

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement policies and procedures to address the final disposition of sensitive information and/or the hardware or electronic media on which it is stored.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will ensure that its inventory database is appropriately updated upon the disposal of components containing sensitive information.

NICAO will ensure that the disposal of all sensitive information is conducted securely and that the destruction of the information is permanent.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the requirements of the Disposal Policy.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will:

- Ensure that prior to disposal, data on hardware or electronic media will be securely overwritten or physically destroyed and that such steps taken will be documented.
- Ensure that the data is permanently and securely destroyed in such a manner that it cannot be reassembled or recovered by any process currently available.
- Ensure that this procedure is consistent with NICAO Fiscal Policies.

Media Re-Use Policy

Policy #: 208

Version #: 12.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement procedures for removal of sensitive information from electronic media before the media are made available for re-use.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will ensure that all electronic media including hard disk drives, optical media, USB keys, memory cards, or any other electronic or portable media has been cleaned of all sensitive data prior to any re-use.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the requirements of the Media Re-use Policy.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will ensure that:

- The inventory database is appropriately updated upon the re-use of media components containing sensitive information.
- Prior to re-use that the media is securely overwritten and that such action is verified and documented.
- The previous label on such media that is to be overwritten is removed and destroyed.

Accountability Policy

Policy #: 209

Version #: 12.0

Effective Date: 05/15/18

Purpose:

The purpose is to maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will ensure that a record is maintained to identify movements of sensitive information including all related hardware and devices.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the requirements of the Accountability Policy.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will ensure that the inventory database is maintained to identify movements of sensitive information including all related hardware and devices.

The movement of hardware, electronic media and devices includes the receipt, removal, storage and/or disposal of sensitive information systems. Such information will also include the identity of responsible persons associated with the movement.

The NICAO Information Security Officer shall periodically verify that the records are accurate and are being maintained by all members of the workforce.

Data Backup and Storage Policy

Policy #: 210

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to create a retrievable, exact copy of sensitive information, when needed, prior to the movement of equipment.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will determine when backups are needed and this will be done prior to the movement of any required systems collecting, storing, processing, or transmitting sensitive information.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the Data Backup and Storage Policy.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will:

- Determine when backups are needed and this will be done prior to the movement of any required systems.
- Make an exact, retrievable copy of the data.
- Test the copy of the data to make sure the copy of the data is exact and retrievable.
- Store the backed up data in a secure location and ensure that the appropriate access controls are implemented to only allow authorized access to all such data.

Unique User Identification Policy

Policy #: 301

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to assign a unique name and/or number for identifying and tracking user identity.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will ensure that each individual who accesses sensitive information, such as EPHI, will be granted some form of unique user identification.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the requirements of the Unique User Identification Policy.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

Each individual that is authorized to access sensitive information, such as EPHI, will be granted some form of unique user identification.

At no time will any workforce member allow anyone else to use their unique ID. Likewise, at no time will any workforce member use anyone else's ID.

NICAO will develop a standard convention for assigning unique user identifiers. NICAO will maintain a secure record of unique user identifiers assigned. NICAO will minimize the use of generic accounts.

NICAO will seek to create unique, individual accounts for privileged access with similar access rights so that activities may be tied to a single individual.

Emergency Access Procedure

Policy #: 302

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to establish and implement authorized access to sensitive information during an emergency.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will establish an Emergency Access Procedure for gaining properly authorized access to sensitive information, such as EPHI, during an emergency.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the Emergency Access Procedure.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will establish an Emergency Access Procedure for gaining properly authorized access to sensitive information, such as EPHI, during an emergency.

Extraordinary care in safeguarding and documenting the use of the information must be exercised during this procedure. The configuration of emergency access controls will be consistent with approved authorizations.

NICAO will identify the necessary sensitive information that would need to be obtained during an emergency.

NICAO will test the emergency access controls to ensure availability and the appropriate restrictions. In the event of an emergency, a record will be maintained of systems accessed by unique individuals.

Automatic Logoff Policy

Policy #: 303

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will:

- Maintain procedures for Automatic Logoff of systems that contain sensitive information after a period of inactivity.
- Configure all systems that support automatic logoff to require logoff after a predetermined period of time. If systems do not support automatic logoff capabilities, NICAO will request those capabilities from the appropriate vendor and document all vendor responses.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the Automatic Logoff Policy.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will maintain procedures for automatic logoff of systems that contain sensitive information after a period of inactivity.

The length of time that a user is allowed to stay logged on while idle will depend on the sensitivity of the information that can be accessed from that computer and the relative security of the environment that the system is located.

NICAO will periodically inspect systems to ensure that the automatic session logoff capability is configured correctly.

If systems do not support automatic logoff capabilities, NICAO will request those capabilities from the appropriate vendor and document all vendor responses in writing.

Encryption and Decryption Policy

Policy #: 304

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement a mechanism to encrypt and decrypt sensitive information.

The Encryption Policy is intended to assist employees of NICAO in making a decision about the use of encryption technologies as a method of protecting data stored on systems that process sensitive information.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will:

- Identify systems that require sensitive information to be encrypted.
- Identify members of the workforce, processes, and devices that require encryption capabilities and will implement those capabilities and test their proper functioning.
- Provide only encryption keys to members of the workforce whose job role requires knowledge of encryption keys.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the Encryption and Decryption Policy.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will:

- Identify members of the workforce who require encryption capabilities.
- Balance the challenge of protecting “data at rest” against the increase in security technology complexity and administrative overhead including performance considerations and usability.
- Test encryption and decryption capabilities of products and systems to ensure proper functionality.
- Review the viability of securing critical database, file servers, and sensitive information on mobile devices.

Audit Controls Policy

Policy #: 305

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use sensitive information.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will:

- Identify critical systems that require event auditing capabilities.
- Define the events to be audited on all such systems.
- Protect all collected logs from alteration or destruction.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the Audit Controls Policy.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will identify critical systems that require event auditing capabilities.

NICAO will define the events to be audited on all such systems. At a minimum, event auditing capabilities will be enabled on all systems that process, transmit, and/or store sensitive information. Events to be audited may include, and are not limited to, logins, logouts, and file accesses, deletions and modifications.

Audits may be conducted to:

- Ensure confidentiality, integrity, and availability of sensitive information.
- Investigate possible security incidents and ensure conformance to NICAO security policies.
- Monitor user or system activity where appropriate.

NICAO will ensure the protection of all audit reports and log files. NICAO will review the usage of software and application tools to review audit files.

When requested, and for the purpose of performing an audit, any access needed will be provided to authorized members of NICAO security team. This access may include:

- User level and/or system level access to any computing or communications device.
- Access to information (electronic, hardcopy, and so on) that may be produced, transmitted, or stored on NICAO equipment or premises.
- Access to work areas (labs, offices, cubicles, storage areas, and so on).
- Access to interactively monitor and log traffic on NICAO networks.

NICAO will protect all collected logs from improper alteration or destruction even by NICAO privileged users such as Administrators or ROOT accounts. NICAO logs should seek to follow “Write Once, Read Many” standards so that they cannot be altered once they are written.

Mechanism to Authenticate Sensitive Information Policy

Policy #: 306

Version #: 12.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement electronic mechanisms to corroborate that sensitive information has not been altered or destroyed in any unauthorized manner.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will:

- Review the use of digital signature and/or checksum technology to corroborate that sensitive information has not been altered or destroyed in any unauthorized manner.
- Evaluate the need for and use of encryption to maintain the integrity of sensitive information.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of the requirements of the Mechanism to Authenticate Sensitive Information Policy.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will establish a baseline of information to compare future data integrity checks against. This includes checking actual file and directory contents and attributes against baseline information.

Person or Entity Authentication Policy

Policy #: 307

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement procedures to verify that the person or entity seeking access to sensitive information is the one claimed.

This policy sets a minimum acceptable level of authentication for users or entities at NICAO.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will evaluate authentication mechanisms to verify that a patient, system, or process is who they claim to be.

Responsibilities:

All individuals identified in the scope of this policy are responsible for:

- Using, as instructed, any authentication method required by the Information Security Officer.
- Abiding by all requirements set forth for the protection of passwords at NICAO.

The NICAO Information Security Officer is responsible for:

- Evaluating and implementing strong (two-factor) authentication solutions when appropriate, while giving preference to high-risk users as described below.
- Ensuring the password administration options of all software packages are set to reflect the password requirements outlined above.
- Monitoring compliance of the workforce with this policy and responding to any security incidents which may arise from it.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO recognizes that the use of passwords as an authentication method is inherently insecure and intends to use strong authentication solutions for workforce members that have access to sensitive information where reasonable and appropriate. Strong authentication solutions use a combination of two or more factors (described above) when granting or denying access; such as the presence of a smart card (something you have) combined with a PIN (something you know).

NICAO will evaluate emerging strong authentication technologies on a periodic basis and implement them when one is found that is:

- Technically sound and useable
- Financially reasonable
- Meets business objectives

NICAO will give strong authentication preference to users that pose a higher risk to the organization. High risk users include (but are not limited to):

- Users that have administrator rights to systems that contain sensitive information.
- Users that connect to the network remotely.
- Users that have portable computing devices that may be carried off the premises.

All workforce members that use passwords will make efforts to keep those passwords safe and secure.

Integrity Controls Policy

Policy #: 308

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement security measures to ensure that electronically transmitted sensitive information is not improperly modified without detection until disposed of.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will:

- Maintain integrity controls to ensure the validity of information transmitted over the network infrastructure.
- Implement measures to ensure that sensitive information is not improperly modified without detection until disposed of by an authorized member of the workforce.

Responsibilities:

The Information Security Officer will be responsible for ensuring the implementation of Integrity Controls Policy.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will:

- Maintain integrity controls to ensure the validity of information transmitted over the network infrastructure.
- Identify the information transmitted over open and other networks for such data integrity is a requirement. This information includes, but is not limited to EPHI.
- Determine the types of integrity controls to implement to secure sensitive information transmitted over public and other external networks.

Encryption Policy

Policy #: 309

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement a mechanism to encrypt sensitive information whenever deemed appropriate.

The Encryption Policy is intended to assist employees of NICAO when making a decision about purchasing or developing software and other systems that make use of encryption technologies as a method of protecting “data in motion.”

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will evaluate the need for and use of encryption to maintain the confidentiality and integrity of sensitive information being transmitted over a network.

Responsibilities:

All workforce members are responsible for:

- Understanding and following all security related policies and procedures related to encryption.

The Information Security Officer is responsible for:

- Ensuring all workforce members understand and follow security related policies and procedures related to encryption.
- Evaluating and implementing financially reasonable email encryption solutions.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO shall protect “data in motion” by implementing a combination of solutions that may include Virtual Private Networks (VPNs), Secure Sockets Layer (SSL) and other technologies. NICAO key length requirements will be reviewed annually and upgraded as technology allows. All keys generated will be securely escrowed.

NICAO will:

- Identify systems that require sensitive information to be encrypted for the purpose of transmission.
- Identify members of the workforce who require encryption capabilities for transmission purposes.
- Test encryption and decryption capabilities of products and systems to ensure proper functionality.

Policies and Procedures Standard

Policy #: 401

Version #: 1.0

Effective Date: 05/15/18

Purpose:

The purpose is to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of impacted regulations.

Scope:

This policy applies to HIPAA covered NICAO in its entirety, including all workforce members, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, or temporary workers. Further, the policy applies to all HIPAA covered NICAO devices, systems, networks, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

NICAO will ensure the development of all policies and procedures required by the regulations.

Responsibilities:

The Information Security Officer will be responsible for ensuring the development of NICAO's HIPAA Security Policies and Procedures.

Compliance:

Failure to comply with this or any other Security Policy will result in disciplinary actions as per the Sanction Policy-104. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s):

NICAO will:

- Ensure the development of all policies and procedures required by the regulations.
- Ensure that all members of the workforce, including managers, are trained on NICAO HIPAA Security Policies.
- Ensure that the policies and procedures are updated on a regular basis.