North Iowa Community Action Organization, Inc. (NICAO)

HIPAA Policies and Procedures Manual

Board Approved Sept '03

North Iowa Community Action Organization, Inc.
HIPAA Policies and Procedures

General Definitions

Term	Definition
Business Associate (BA)	A person or entity who, on behalf of NICAO, and other than in the capacity of a workforce member: performs or assists in the performance of a function or activity that involves the use or disclosure of protected health information (PHI), or; provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.
Complaint	Any concern communicated by a person questioning any act or failure to act relating to an individual's rights to access to his/her health information, to maintain the privacy of his/her health information, to request restrictions on uses or disclosures of his/her PHI, to request confidential communications regarding his/her PHI, to request amendment of his/her PHI, or to receive an accounting of disclosures of his/her PHI.
Covered Entity (CE)	A health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form relating to any covered transaction.
Designated Record Set	A group of records maintained by or for a CE that is: the medical and billing records relating to an individual maintained by or for a health care provider; the enrollment, payment, claims adjudication, and case or medical management systems maintained by or for a health plan, or; used, in whole or in part, by or for a CE to make decisions about individuals. NICAO adopts HIPAA Academy recommendation (3.0) to define the designated record set as: personal data; medical history, physical exam, laboratory test orders, results and follow-up; treatment and special instructions; scheduled visits; informed consents; refusal of services; allergies and untoward reactions to drug(s) recorded in a prominent and specific location; billing, claim and payment records associated with payment for services, and any other information used by NICAO to make a medical decision.
Disclosure	The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
Health Oversight Agency	A governmental agency or authority, or a person or entity acting under a grant of authority from or a contract with such a public agency, including the employees or agents of the public agency, its contractors and those to whom it has granted authority, that is authorized by law to oversee the public or private health care system or government programs in which health information is necessary to determine eligibility or compliance.
Hybrid Entity	A single legal entity that is a CE that also conducts business that is not covered by HIPAA.
NICAO	When referred to in a policy statement, "NICAO" denotes the component of NICAO that is named in the "Applies To" statement of that policy.
Personal Representative	A person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person acting in *loco parentis* who is authorized under law to make health

	care decisions on behalf of an unemancipated minor, except where the minor is authorized by law to consent, on his/her own or via court approval, to a health care service, or where the parent, guardian or person acting in loco *parentis* has assented to an agreement of confidentiality between the provider and the minor.
Privacy Notice	The notice of privacy practices relating to an entity's use and disclosure of PHI that is mandated under HIPAA regulations for distribution to all individuals whose information will be collected by or on behalf of the entity.
Protected Health Information (PHI)	Individually identifiable information relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.
Psychotherapy Notes	Notes recorded in any medium by a mental health care provider who is a mental health professional documenting or analyzing the contents of conversation. The conversation can take place during counseling sessions that are private, group, joint, or family sessions. These notes are separated in some manner from the rest of the individual's medical record.
Public Health Authority	A governmental agency or authority, or a person or entity acting under a grant of authority from or a contract with such a public agency, including the employees or agents of the public agency, its contractors and those to whom it has granted authority, that is responsible for public health matters as part of its official mandate.
Treatment, Payment and Health Care Operations (TPO)	Includes all of the following: • *Treatment* means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care. • *Payment* means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collections activities, medical necessity determinations and utilization review. • *Health Care Operations* includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities.
Use	With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
Workforce Members	Employees, volunteers, trainees, contractors, temporary workers and other persons whose conduct, in the performance of work for NICAO, its offices, programs or facilities, is under the direct control of NICAO, office, program or facility, regardless of whether they are paid by the entity.

Mapping of HIPAA Standards to NICAO Policies

	HIPAA Standard	NICAO Policy
164.502	General Ruse on Use & Disclosure (U & D)	HIP-00-004
	Minimum Necessary	HIP-00-004
		HIP-00-005
	U&D subject to agreed upon restriction	HIP-00-004
	U&D of de-identified data	HIP-00-004
	U&D to Business Associates	HIP-00-004
		HIP-00-006
	Deceased individuals	HIP-00-004
	Personal representatives	HIP-00-004
	Confidential communications	HIP-00-004
	U&D consistent with Notice	HIP-00-004
	U&D by whistleblowers	HIP-00-004
164.504	Health Care component	HIP-00-020
	Affiliated covered entities	Not applicable
	Business Associate contracts	HIP-00-006
	Requirements for group health plans	Not applicable
	Requirements for covered entities w/multiple covered functions	Not applicable
164.506	Permitted U&D	HIP-00-011
	Consent for U&D	HIP-00-011
164.508	Authorizations	HIP-00-011
		HIP-00-013
164.510	Facility directories	HIP-00-011
	U&D for involvement in individual's care and notification Purposes	HIP-00-011
164.512	U&D required by law	HIP-00-012
	U&D for public health activities	HIP-00-012
	U&D about victims of abuse	HIP-00-012
	U&D for health oversight activities	HIP-00-012
	U&D for judicial and administrative proceedings	HIP-00-012
	U&D for law enforcement	HIP-00-012
	U&D about decedents	HIP-00-012
	U&D for cadaveric organ, eye, or tissue donation purposes	HIP-00-012
	U&D for research purposes	HIP-00-012
	U&D to avert a serious threat to health or safety	HIP-00-012
	U&D for specialized government functions	HIP-00-012
	U&D for worker's compensation	HIP-00-012
164.514	De-identification of PHI	HIP-00-035
		HIP-00-036
	Minimum Necessary requirements	HIP-00-005

	Limited Date Set	HIP-00-035
	U&D for fundraising	HIP-00-025
	U&D for underwriting and related purposes	Not applicable
	Verification requirements	HIP-00-005
		HIP-00-030
164.520	Notice of Privacy Practices	HIP-00-007
164.522	Right of an individual to request restriction of U&D	HIP-00-009
	Confidential communications requirements	HIP-00-009
164.524	Access to PHI	HIP-00-009
164.526	Right to amend	HIP-00-009
164.528	Right to an accounting of disclosure of PHI	HIP-00-014
164.530	Personnel designations	HIP-00-003
	Training	HIP-00-003
	Safeguards	HIP-00-003
	Complaints to the covered entity	HIP-00-003
		HIP-00-010
	Sanctions	HIP-00-003
		HIP-00-010
	Mitigation	HIP-00-003
		HIP-00-010
	Refraining form intimidating or retaliatory acts	HIP-00-003
		HIP-00-010
	Waiver of rights	HIP-00-003
	Policies and procedures	HIP-00-003
	Documentation	HIP-00-003
		HIP-00-010
	Group health plans	Not applicable
164.532	Effect of prior authorizations	HIP-00-040
	Effect of prior contracts or other arrangements with business Associates	HIP-00-042
164.534	Compliance dates for initial implementation	HIP-00-001

HIP-00-001

Subject: HIPAA Policies and Procedures

Applies To: All covered healthcare components of NICAO

Purpose:
The purpose of this rule shall be to establish required policies and procedures for NICAO's compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and its implementing regulations.

Policy:
NICAO will comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Procedure:
NICAO offices, facilities, programs, and workforce members are directed to follow all applicable policies and procedures found in the NICAO HIPAA Policies and Procedures Manual maintained at NICAO Administrative Offices. Privacy Rule compliance is required by April 14, 2003.

Failure to comply with this rule and its reference documents may result in disciplinary sanctions as defined in policy HIP-00-002, Subject: Sanctions Policy found on page 6.

HIP-00-002

Subject: Sanctions Policy

Applies To: All covered healthcare components of NICAO

Purpose:

The purpose of this policy is to link the sanctions policy of North Iowa Community Action Organization to any failure to comply with HIPAA.

Policy:

NICAO policy is to comply with HIPAA. Any member of the NICAO workforce who fails to comply with HIPAA policies and procedures will be subject to progressive discipline and other sanctions.

Procedure:

- Failure to comply with NICAO HIPAA Policies and Procedures will result in progressive discipline according to Policy 716 of the NICAO Employee Personnel Policy Handbook dated October 1, 2003. (See page 78)

HIP-00-003

Subject: Administrative Requirements for Implementing HIPAA

Applies To: All covered healthcare components of NICAO

Purpose:

To issue instructions to all NICAO offices, facilities, programs and workforce members regarding NICAO's obligations relating to the implementation of the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. §§ 1320d-1329d-8, and regulations promulgated there under, 45 CFR Parts 160 and 164.

Policy:

Compliance Officer

NICAO's Compliance Officer is the Health Services Coordinator of the Family Health Center. The Compliance Officer will delegate HIPAA compliance tasks as needed.

Privacy Officer

NICAO's Privacy Officer is the Administrative Assistant of the Family Health Center. The Privacy Officer will further delegate HIPAA compliance tasks as needed.

Contact Person or Office

The Privacy Officer will be responsible for ensuring that complaints are received and resolved.

Training Requirements

NICAO and, as applicable, its offices, programs and facilities, must document the following training actions:

All NICAO employees and other workforce members must receive training on applicable policies and procedures relating to PHI as necessary and appropriate for such persons to carry out their functions within NICAO.

Each new workforce member shall receive the training as described above within a reasonable time after joining the workforce.

Each workforce member, whose functions are impacted by a material change in the policies and procedures relating to PHI, or by a change in position or job description, must receive the training as described above within a reasonable time after the change becomes effective.

Safeguards

Each office, program or facility of the agency must have in place appropriate administrative, technical, and physical safeguards to reasonably safeguard PHI from intentional or unintentional unauthorized use or disclosure.

Complaint Process
Each office, program or facility of the agency must have in place a process for individuals to make complaints about the entity's HIPAA policies and procedures and/or the entity's compliance with those policies and procedures, and must document all complaints received and the disposition of each complaint. See policy HIP-00-010, Subject: Complaint Process for Alleged Violations of Rights Relating to PHI found on page 27.

Sanctions
The Human Resources Office must have in place, must apply and must document application of appropriate sanctions against workforce members who fail to comply with HIPAA policies and procedures. (Note - there are exceptions for disclosures made by workforce members who qualify as whistleblowers or certain crime victims.)

Mitigation Efforts Required
Each office, program or facility must mitigate, to the extent practicable, any harmful effects of unauthorized uses or disclosures of PHI by the entity or any of its business associates.

Intimidating or Retaliatory Acts and Waiver of Rights Prohibited

Prohibition on Intimidating or Retaliatory Acts
Neither the agency nor any office, program, facility or workforce member shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of his/her rights or participation in any process relating to HIPAA compliance, or against any person for filing a complaint with the Secretary of the U.S. Department of Health and Human Services, participating in a HIPAA related investigation, compliance review, proceeding or hearing, or engaging in reasonable opposition to any act or practice that the person in good faith believes to be unlawful under HIPAA regulations as long as the action does not involve disclosure of PHI in violation of the regulations.

Prohibition on Waiver of Rights
No office, program, facility or workforce member of the agency shall require individuals to waive any of their rights under HIPAA as a condition of treatment, payment, enrollment in a health plan or eligibility for benefits.

Policies and Procedures
NICAO and, as applicable, its offices, programs and facilities must document the following actions relating to its policies and procedures:

> **Required Policies and Procedures:** NICAO shall design and implement policies and procedures to assure appropriate safeguarding of PHI in its operations to be followed by each office, program or facility, and all workforce members.

Changes to Policies and Procedures: NICAO must change its policies and procedures as necessary and appropriate to conform to changes in law or regulation. NICAO may also make changes to policies and procedures at other times as long as the policies and procedures are still in compliance with applicable law. Where necessary, the entity must make correlative changes in its Privacy Notice. NICAO may not implement a change in policy or procedure prior to the effective date of the revised Privacy Notice.

Documentation Requirements: NICAO and each of its offices, programs or facilities, must maintain the required policies and procedures in written or electronic form, and must maintain written or electronic copies of all communications, actions, activities or designations as are required to be documented hereunder, or otherwise under the HIPAA regulations, for a period of six (6) years from the later of the date of creation or the last effective date or such longer period that may be required under state or other federal law.

HIP-00-004

Subject: Management and Protection of Personal Health Information

Applies To: All covered healthcare components of NICAO

Purpose:

To issue instructions to all NICAO offices, facilities, programs and workforce members regarding the management and protection of individuals' health information.

Policy:

For details on specific requirements, refer to the appropriate policies in this manual as indicated by page reference. Generally, PHI shall not be used or disclosed except as permitted or required by law.

Notice of Privacy Practices Required

Individuals served must be given a Notice of Privacy Practices outlining the uses and disclosures of PHI that may be made, and notifying them of their rights and our legal duties with respect to PHI.

Permitted and Required Uses and Disclosures

PHI may be disclosed as follows:

- To the individual; see page 22, NICAO Policy HIP-00-009.
- To carry out TPO activities, within specified limits; see page 29, NICAO Policy HIP-00-011.
- Pursuant to and in compliance with a current and valid Authorization; see page 34, NICAO Policy HIP-00-013.
- In keeping with a Business Associate arrangement; see page 17, NICAO Policy HIP-00-006.
- As otherwise provided for in the HIPAA privacy regulations; see page 30, NICAO Policy HIP-00-012.

Minimum Necessary

Generally, when using or disclosing PHI, or when requesting PHI from another entity, reasonable efforts must be made to limit the PHI used or disclosed to the minimum necessary to accomplish the purpose of the use/disclosure; see page 13, NICAO Policy HIP-00-005.

Deceased Individuals

NICAO will continue to follow these policies and procedures for any PHI it holds pertaining to deceased clients.

Personal Representatives

A person acting in the role of personal representative must be treated as the individual regarding access to relevant PHI unless:

- The individual is an unemancipated minor, but is authorized to give lawful consent, or may

obtain the health care without consent of the personal representative, and minor has not requested that the person be treated as a personal representative, or the personal representative has assented to agreement of confidentiality between the provider and the minor;

- There is a reasonable basis to believe that the individual has been or may be subjected to domestic violence, abuse or neglect by the personal representative or that treating that person as a personal representative could endanger the individual, and, in the exercise of professional judgment, it is determined not to be in the best interests of the individual to treat that person as a personal representative.

Agreed Upon Restrictions

An individual has a right to request a restriction on any uses or disclosures of his/her PHI, though a covered entity need not agree to the requested restriction, and cannot agree to a restriction relating to disclosures required under law (i.e. disclosures to the U. S. Secretary of Health and Human Services for HIPAA enforcement purposes). See page 22, NICAO Policy HIP-00-009.

Confidential Communications

An individual has a right to request to receive communications of PHI by alternative means or at alternative locations, and reasonable requests must be accommodated. See page 13, NICAO Policy HIP-00-005.

Accounting for Disclosures

An individual has a right to an accounting of disclosures of his/her PHI for up to a six (6) year period. See page 36, NICAO Policy HIP-00-014.

De-identified PHI

Health information may be considered not to be individually identifiable in the following circumstances:

- A person with appropriate knowledge and experience with generally acceptable statistical and scientific principles and methods determines that the risk is very small that the information could be used, alone or with other reasonably available information, to identify the individual who is the subject of the information; or
- The following identifiers of the individual (and relatives, employers or household members) is removed (also referred to as the Safe Harbor Method):
  - names;
  - information relating to the individual's geographic subdivision if it contains fewer than 20,000 people;
  - elements of dates (except year) directly related to the individual, and all ages and elements of dates that indicate age for individuals over 89, unless aggregated into a single category of age 90 and older;
  - telephone numbers;
  - fax numbers;
  - email addresses;
  - social security numbers;

- medical record numbers;
- health plan beneficiary numbers;
- account numbers;
- certificate or license numbers;
- vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- biometric identifiers;
- full face photographic images;
- and any other unique identifying number, characteristic or code.

Complaint Process:

Each office, program or facility of NICAO must have in place a process for individuals to make complaints about the entity's HIPAA policies and procedures and/or the entity's compliance with those policies and procedures. See page 27, NICAO Policy HIP-00-010.

Documentation:

Each office, program or facility of NICAO must maintain written or electronic copies of all policies and procedures, communications, actions, activities or designations as are required to be documented under this manual for a period of six (6) years from the later of the date of creation or the last effective date or such longer period that may be required under state or other federal law.

HIP-00-005

Subject: Minimum Necessary Standard

Applies To: All covered healthcare components of NICAO

Purpose:

To issue instructions to all NICAO offices, facilities, programs and workforce members regarding NICAO's obligations relating to the HIPAA requirement to use, disclose or request only the minimum amount of protected health information (PHI) necessary to accomplish the intended purpose of the use, disclosure or request.

Policy:

The North Iowa Community Action Organization Inc., and its offices, facilities, programs and workforce members, will make reasonable efforts to ensure that the minimum necessary protected health information (PHI) is disclosed, used, or requested. Exceptions to the minimum necessary requirement include:

- disclosures to the individual who is the subject of the information;
- disclosures made pursuant to an authorization;
- disclosures to or requests by healthcare providers for treatment purposes;
- disclosures required for compliance with the standardized HIPAA transactions;
- disclosures made to HHS pursuant to a privacy investigation;
- disclosures that are otherwise required by the HIPAA regulations or other law.

Procedure:

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of the organization.

- Reasonable efforts will be made to limit each PHI user's access to only the PHI that is needed to carry out his/her duties. These efforts will include internal staff-to-staff use and external disclosure of PHI. See the table included with this policy.
- For situations where PHI use, disclosure, or request for information occurs on a routine and recurring basis protocols have been developed to assure that the PHI disclosed will be limited to the amount of information reasonably necessary to achieve the purpose of the use, disclosure or request. Universal Service Agreements have been reviewed to ensure that the PHI being released meets this Minimum Necessary standard.
- For non-routine disclosures (other than pursuant to an authorization - for instance to accrediting bodies, insurance carriers, research entities, funeral homes, etc.) criteria as outlined on page 15 & 16 has been adopted for review by NICAO staff to limit the information disclosed to that which is reasonably necessary to accomplish the purpose for which disclosure is sought. A request may be presumed to be limited to the minimum necessary if the request is from another CE, or is from a public official or a professional for the purpose of providing services to the CE, and the request states that the PHI requested is the minimum necessary.

- Use/disclosure of the entire medical record should not be made unless use/disclosure of the entire record is specifically justified as the amount reasonably necessary to accomplish the purpose of the use or disclosure.
- All NICAO Workforce Members will be trained regarding this policy within 60 days of employment and annually thereafter.
- Questions regarding these procedures should be directed, in writing, to the NICAO Privacy Officer for resolution: NICAO Privacy Officer, 300 15th St NE, Mason City, IA 50401.

Protocol:

When PHI use, disclosure, or request for information occurs on a routine and recurring basis, except for TPO as defined in HIP-00-011, the NICAO Family Health Center staff will respond as follows:

- The Privacy Officer, Compliance Officer, or licensed staff member must provide approval for a staff member to share the information.
- The approved staff member must limit the amount of information reasonably necessary to achieve the purpose of the use, disclosure, or request.
- The following information must be documented in the patient's chart:
    - Name of the entity requesting the information
    - The listing of the information shared by the NICAO staff verbally and/or in written form
    - The date the information was shared
    - Signature of staff providing the information

Minimum Necessary Standard

Requested by	Signature Required	Signed by	Procedure	Required Charge
Accrediting Agencies(DPH)	No	N/A	May view copies and/or release copies as requested	No
Attorney/legal Aid (acting in the interest of the Patient) If lawsuit pending against NICAO	Yes	Patient or legal guardian of person	May view chart, release copies as requested, forward copies to Legal Consultant if lawsuit pending.	No
Bureau of Disability Determination	Yes	Person or legal guardian of person	One copy without charge.	No
Coroners Office	Yes	Signed release by coroner, deputy coroner or representative of either.	Release copies as requested.	No
Court Order	Yes	Judge	Release copies as requested. (Fax copy of Court Order to NICAO)	No
Department of Health	No	N/A	Release communicable information to report communicable disease.	No
Family Member	Yes	Patient or legal guardian of deceased patient	Release copies as requested.	No
Employer	Yes	Person or legal guardian of person	Release copies as requested.	No
Executor of Estate	Yes	Signed release by executor or administrator of estate of a deceased patient (copy of Court appointment must be provided)	Release copies of information necessary to administer the estate	No
Funeral Home	No	N/A	Release only time, date of death and attending physician. Do not release diagnosis.	No
General Hospital/Clinic/Nursing Home (non-emergency, scheduled appointment)	Yes	Must attempt to acquire signature of person or legal guardian of person	May view and/or release copies as requested	No
Insurance Carriers	No	NA	Release copies as requested	No

Law Enforcement (Secret Service, FBI, Iowa State Highway Patrol)	Yes	Must attempt to acquire signature of person or legal guardian of person	Release copies as requested.	No
Parole/Probation Officer	Yes	Person or legal guardian of person	Release copies as requested.	No
Client	Yes	Client or legal guardian of person	Release copies as requested unless access specifically is restricted in a client's treatment plan for clear treatment reasons.	No
Client/Client's representative for filing SS disability benefits	Yes	Person or legal guardian of person	One copy without charge.	No
Private Physician/Provider	Yes	person or legal guardian of person	Release copies as requested.	No
Prosecutors Office	Yes	Person or legal guardian of person	Release copies as requested.	No
Research Person	Dependant	Upon type of research being conducted	Defer to Executive Committee for direction	No
Selective Service	Yes	Patient or legal guardian of person	Release copies as requested	No
Social Security Administration	Yes	Person or legal guardian of person	One copy without charge.	No
Subpoena (From Court or Administrative Body)	No	N/A	Notify Attorney/Agency of need for Court Order or signed authorization (Fax copy of Subpoena to Legal Consultant)	No
Veterans Administration	Yes	Patient or legal guardian of person	Release copies as requested for continuity of care	No

HIP-00-006

Subject: Business Associate Contracts

Applies To: All covered healthcare components of NICAO

Purpose:

To issue instructions to all NICAO offices, facilities, programs and workforce members regarding the necessity for and the required content of agreements with business associates (including in some cases other governmental entities) relating to the business associate's receipt and use of protected health information (PHI) from or on behalf of NICAO, its offices, facilities, programs or workforce members.

Policy:

Generally, the covered entity may disclose PHI to a BA, or allow a BA to create or receive PHI on the entity's behalf, if the entity first obtains adequate assurance that the BA will appropriately safeguard the PHI. This requirement does not apply with respect to:

- disclosures made to a provider concerning the individual's treatment, or;
- disclosures made to a governmental agency for purposes of public benefit eligibility or enrollment determinations where such agency is authorized by law to make these determinations

The covered entity must document these assurances through a written agreement.

Determining When to Create a BAC

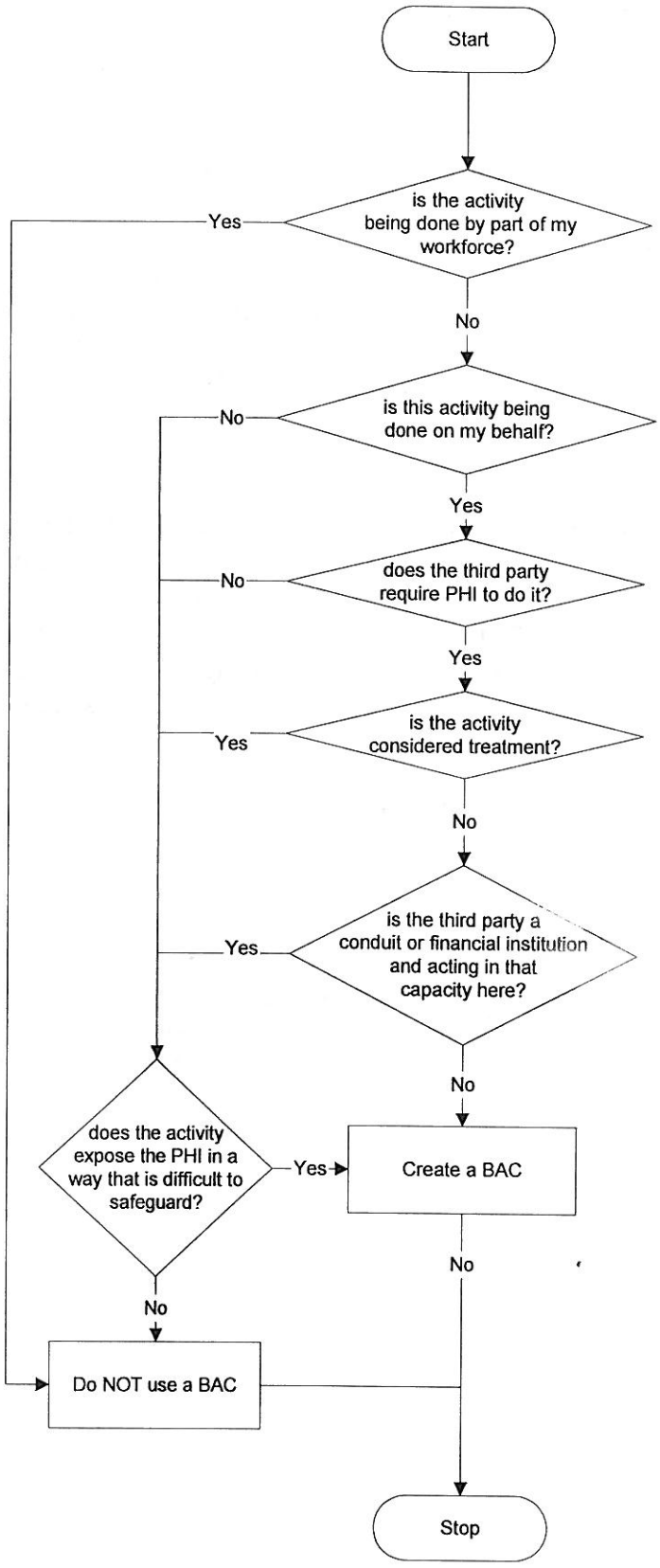
The flowchart that follows provides guidance on when to create a BAC or similar agreement as described above. The same process is to be applied when NICAO is acting as a BA and is using a subcontractor to conduct a task that requires PHI or exposes PHI to disclosure.

Do we need a BAC with this third party?

Step 1: Identify each process - a third party may be doing more than one thing for you. One activity may require a BAC. Others might not.

Step 2: From your perspective, walk through the flowchart to determine the need for a BAC.

Step 3: Repeat for each process with this third party.



Content Requirements

The agreement between the covered entity and the BA must meet the following requirements, as applicable:

- Establish permitted and required uses or disclosures of PHI that are consistent with those authorized for the entity, except that the agreement may permit the BA to use or disclose PHI for its own management and administration if such use or disclosure is required by law or the BA obtains reasonable assurance that the confidentiality of the PHI will be maintained
- Provided that the BA will:
  - Not use or disclose the PHI except as authorized under the agreement or required by law
  - Use safeguards to prevent unauthorized use or disclosure
  - Report unauthorized uses or disclosures to the entity
  - Pass on the same obligations relating to protection of PHI to any subcontractors or agents
  - Make PHI available for access by the individual or his/her personal representative, in accordance with relevant law and policy
  - Make PHI available for amendment, and incorporate any approved amendments to PHI, in accordance with relevant law and policy
  - Make information available for the provision of an accounting of uses and disclosures in accordance with relevant law and policy
  - Make its internal practices, books and records relating to its receipt or creation of PHI available to the Office of the U.S. Secretary of Health and Human Services for purposes of determining the entity's compliance with HIPAA regulations
  - If feasible, return or destroy all PHI upon termination of contract; if any PHI is retained, continue to extend the full protections specified herein as long as the PHI is maintained
  - Authorize termination of the agreement by the entity upon a material breach by the BA; this element of the agreement may be omitted if the BA is another governmental entity and the termination would be inconsistent with the statutory obligations of the entity or the BA

Oversight Responsibilities

If the entity knows of a pattern or practice of the BA that amounts to a material violation of the agreement, the entity must attempt to cure the breach or end the violation, and if such attempt is unsuccessful, terminate the agreement, if feasible, and, if not, report the problem to the Office of U.S. Secretary of Health and Human Services.

HIP-00-007

Subject: Provision of Privacy Notice

Applies To: All covered healthcare components of NICAO

Purpose:

To issue instructions to all NICAO offices, facilities, programs and workforce members regarding the provision of a notice of privacy practices to all patients and clients.

Policy:

Generally, an individual has a right to receive a written notice of the uses and disclosures of his/her Protected Health Information (PHI) that may be made by or on behalf of a Covered Entity (CE), and of the individual's rights and the CE's legal duties with respect to his/her PHI.

Content Requirements

The notice of privacy practices must be written in plain language and must contain the following elements:

- The following statement in a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY".

- A description, including at least one example, of the types of uses and disclosures that the CE is permitted to make for purposes of treatment, payment and health care operations, with sufficient detail to place an individual on notice of the uses and disclosures permitted or required

- A description of each of the other purposes for which the CE is permitted or required to use or disclose PHI without an individual's consent or authorization, with sufficient detail to place an individual on notice of the uses and disclosures permitted or required;

- A statement that other uses or disclosures will be made only with the individual's written authorization, and that the authorization may be revoked in accordance with the policy on authorizations;

- A statement describing contacts such as: to contact the individual for appointment reminders, treatment alternatives, or other health related benefits.

- A statement of the individual's rights with respect to his/her PHI, and a brief description of how the individual may exercise those rights, including: the right to request restrictions on certain uses/disclosures of PHI, and the fact that the CE does not have to agree to such

restrictions; the right to receive confidential communications of PHI; the right to inspect and copy PHI; the right to amend PHI; the right to receive an accounting of disclosures of PHI, and; the right to receive a paper copy of the privacy notice (each of the above in accordance with relevant policies);

- A statement of the CE's duties with respect to PHI, including statements: that the CE is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy policies; that the CE is required to abide by the terms of the currently effective privacy notice, and; that the CE reserves the right to change the terms of the notice and make the new notice provisions effective for all PHI maintained, along with a description of how the CE will provide individuals with the revised notice;

- A statement that individuals may complain to the CE and to the Secretary of the U.S. Department of Health and Human Services about privacy rights violations, including a brief statement about how a complaint may be filed and an assurance that the individual will not be retaliated against for filing a complaint;

- The name, or title, and telephone number of the person or office to contact for further information;

- The effective date of the notice, which may not be earlier than the date printed or published.

Revisions to Notice

NICAO will promptly revise and distribute the privacy notice whenever there is a material change to the uses or disclosures, the individual's rights, the CE's legal duties, or other privacy practices described in the notice. Except when required by law, a material change to any term may not be implemented prior to the effective date of the notice reflecting the change.

Provision of Notice

NICAO facilities and programs must provide individuals with the notice, and obtain the individual's written acknowledgement of receipt, or document attempts to obtain such acknowledgement, no later than the date of the first service delivery. The receipt of acknowledgement will be maintained in the medical record. Additionally, the notice in effect (original notice or any subsequent revisions) must be prominently posted and copies must be available for individuals to take at any service delivery sites.

The privacy notice will also be prominently posted on the NICAO web site and available electronically from the web site.

Documentation Requirements

NICAO will retain copies of notices issued for a period of at least six years from the later of the date of creation or the last effective date and each facility and program will retain documentation of individual's acknowledgement of receipt, or refusal to acknowledge receipt, of the privacy notice for a period of at least six years.

HIP-00-009

Subject: Individuals' Rights Related to Protected Health Information (PHI)

Applies To: All covered healthcare components of NICAO

Purpose:

To issue instructions to all NICAO offices, facilities, programs and workforce members regarding NICAO's obligations relating to individual's rights relating to access to and use/disclosure of their protected health information (PHI).

Policy:

Right to Access PHI

Individuals have a right to access and obtain a copy of their PHI and any information in their designated record set except as set forth below:

- **Denial of Access without a right of review:** Access may be denied where:
  - Information was compiled in anticipation of litigation;
  - Information was collected in the course of research that includes treatment of the individual and the individual agreed to a suspension of the right of access during the research period;
  - Access can be denied in accordance with the Clinical Laboratory Improvements Amendments of 1988 (CLIA) or the Privacy Act (5 USC 552a).

- **Denial of Access with a right of review:** Access may be denied, though denial is subject to review where:
  - Access is determined by a licensed professional to be likely to endanger life or physical safety of the individual or another person; and such determination is documented.
  - Access is requested by a Personal Representative and a licensed professional determines that such access is reasonably likely to cause substantial harm to the individual or another person.

- **Right of Review:** If the basis for denial of access gives a right of review, the individual has a right to have the denial reviewed by another licensed professional who did not participate in the original denial decision. Such review must be complete within a reasonable period of time, and the NICAO facility or program must promptly: (i) provide the individual with notice of the reviewer's decision, and (ii) comply with the determination to provide or deny access.

- **Timely Review:** The covered entity must act on a request for access no later than thirty (30) days after receipt unless the time period is extended as permitted below:
  - If the information to be accessed is not maintained or accessible on-site, the covered entity must

act on the request no later than sixty (60) days after receipt.
- If the covered entity is unable to act on the request for access within the applicable 30 or 60 day period, it may extend the time for response by no more than thirty (30) days, provided that, within the original allotted time period, the covered entity gives the individual written notice of the reasons for the delay and the date by which a responsive action will be taken.

- **Provision of Access:** The covered entity must provide the individual with access to the information in the form or format requested if it is readily producible in such form or format, or in a readable hard copy or other form or format as mutually agreed to, either by arranging for a convenient time and place for inspection and copying, or mailing the information at the individual's request.
  - If the information is maintained in more than one place, the information need only be produced once in response to a current request for access.
  - The covered entity may provide a summary of the information in lieu of providing access, or may provide an explanation of the information to which access is provided if the individual, in advance, agrees.
  - The covered entity will follow existing North Iowa Community Action Organization Inc. corporate Policies and Procedures when imposing a fee for copying information.

- **Denial of Access:** The covered entity must provide a timely, written denial of access to the individual, written in plain language, explain the basis for the denial, and any applicable right of review, and describe how the individual may complain to the covered entity (including name or title of contact, and phone number) or the U.S. Secretary of Health and Human Services.
  - To the extent possible, the individual must be given access to any information requested after excluding the information for which covered entity has grounds for denying access.
  - If the covered entity does not maintain the information for which access has been requested, but knows where it is maintained, the covered entity must inform the individual where to direct the request for access.

- **Documentation:** The covered entity must document and retain for six years from the date of its creation the designated record sets subject to access and the names or titles of persons responsible for receiving and processing requests for access.

Right to Request Restrictions on Uses/Disclosures of PHI, And To Request Confidential Communications

- **Requests for Restrictions on Uses/Disclosures:** The covered entity must permit an individual to request that the covered entity restrict uses and disclosures of PHI made for Treatment, Payment, or Healthcare Operations (TPO) or disclosures to family or others involved in the individual's care, though the covered entity does not have to agree to the restriction requested.
  - If the covered entity agrees to the requested restriction(s), it must document the agreed upon restriction in writing, and abide by the restriction unless the individual is in need of emergency treatment, the information is needed for the treatment, and the disclosure is to another provider only for purposes of such treatment. The covered entity must request that the provider

agree not to further disclose the PHI.
- The covered entity cannot agree to a restriction that prevents uses or disclosures permitted or required to the individual, or where the use or disclosure does not require the individual's permission.
- The covered entity may terminate an agreed upon restriction if the individual so agrees, as documented in writing, or the covered entity informs the individual and the termination is only effective as to PHI created or received after such notice.

- **Requests for Confidential Communications:** The record keeping covered entity must permit individuals to request to receive communications of PHI by alternative means or at alternative locations, and must accommodate all reasonable requests.

Right to Request Amendment of PHI:

- **Requests for Amendment of PHI:** An individual has the right to have the covered entity amend PHI or other information in the designated record set for as long as the covered entity maintains the information. The covered entity must act on the request within sixty (60) days of receipt, or within ninety (90) days if the covered entity notifies the individual within the first 60 days of the reasons for delay and the date by which action will be taken. The Executive Director/designee of NICAO may deny the request if it is determined that the record: was not created by the covered entity (unless the individual provides reasonable basis to believe that the originator of the records is no longer available to act on the request); is not part of the designated record set; would not be available for inspection; or is accurate and complete.

- **Accepting the Amendment:** If the Executive Director/designee of NICAO accepts the amendment, in whole or in part, it must:
  - Make the amendment by, at minimum, identifying the affected records and appending or otherwise providing a link to the location of the amendment;
  - Timely inform the individual that the amendment is accepted, and obtain his/her identification of and agreement to have the covered entity notify relevant persons with a need to know;
  - Make reasonable efforts to inform and timely provide the amendment to those persons and others, including business associates, that the covered entity knows to have the affected PHI and that may have relied, or be foreseen to rely, on that information to the detriment of the individual.

- **Denying the Amendment:** If the covered entity denies the amendment, in whole or part, it must:
  - Provide the individual with a timely denial, written in plain language and including: the basis for denial; notice of the individual's right to submit a written statement of disagreement, and instructions on how to file the statement, or to request that future disclosures of the PHI include copies of the request and the denial; and a description of how the individual may complain about the decision to the covered entity or to the U. S. Secretary of Health and Human Services;
  - Permit the individual to submit a statement of disagreement (but covered entity may reasonably limit its length);

- Provide a copy of any rebuttal prepared to the individual;
- As appropriate, identify the part of the record subject to the disputed amendment and append or otherwise link the request, the denial, and any statement of disagreement or rebuttal to the record;
- For future disclosures of the record, include any statement of disagreement or, in response to the individual's request, the amendment request and the denial (or an accurate summary of either of the foregoing). If standard transaction format does not permit the appending of the additional information, it must be transmitted separately to the recipient of the standard transaction.
- If the covered entity is informed by another covered entity about an amendment to the record, the covered entity must amend the information in its record by, at a minimum, identifying the affected records and appending or otherwise providing a link to the location of the amendment.
- The covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments.

Right to an Accounting of Disclosures:

An individual has a right to receive an accounting of disclosures of his/her PHI in accordance with the policy HIP-00-014, Subject: Accounting for Disclosures of Protected Health Information found on page 36.

HIP-00-009-F1
Request for Communication and/or Disclosure Restrictions

I request these alternatives or limitations relating to communications directed to me by

_____
_____
_____

_____ _____ _____
Print Name (Patient/Client) Signature Date

_____ _____
Print Name (Witness) Signature

▪ ___Accepted ▪ ___ Denied Date _____

Reason: _____ Signature _____

I request these restrictions to the use or disclosure of my personal individually identifiable health information:

_____
_____
_____
_____
_____
_____

_____ _____ _____
Print Name Signature Date

_____ _____
Print Name (Witness) Signature

___Accepted ___ Denied Date: _____

Reason: _____ Signature: _____

HIP-00-010

Subject:

Complaint Process for Alleged Violations of Rights Relating to PHI

Applies To: All covered healthcare components of NICAO

Purpose:

To issue instructions to all NICAO offices, facilities, programs and workforce members regarding procedures for acceptance of, response to, and documentation of individuals' complaints about alleged violations of their rights relating to protected health information (PHI).

Policy:

HIPAA grants individuals specific rights relating to their health information, many of which overlap with patient/client rights mandated by state law. Specifically, in addition to privacy rights related to their PHI, individuals are granted the right to access their designated record set, to request restrictions on uses or disclosures of their PHI, to request that communications related to PHI be confidential, to request amendment of their designated record set, and to receive an accounting of disclosures of their PHI. See details on page 22.

HIPAA also mandates that a process be in place for individuals to complain about a covered entity's privacy related policies and procedures and/or the covered entity's compliance with those policies and procedures.

The Privacy Officer shall be designated as the person/position title responsible for receiving complaints relating to individuals' privacy rights, and rights to access their designated record set, to request restrictions on the use or disclosure of their PHI, to request confidential communications of health related information, to request amendment of their designated record set, or to request an accounting of disclosures made of their PHI:

For each NICAO program: The Privacy Officer

When a HIPAA related complaint is communicated to any workforce member, that workforce member shall immediately notify the Privacy Officer, and shall inform the individual of the name and contact information for the Privacy Officer. If the Privacy Officer is a subject of the complaint, the individual shall be referred to the NICAO Compliance Officer. If the NICAO Compliance Officer is the subject of the complaint, the individual shall be referred directly to the NICAO Executive Director, who will act as the Privacy Officer for purposes of that complaint. The Privacy Officer shall also give the individual information about his/her right to file a complaint with the U.S. Secretary of Health and Human Services.

If the content of the complaint is an incident, an incident report must be immediately filed.

The Privacy Officer shall investigate the circumstances of the alleged HIPAA rights violation and if appropriate, shall take all reasonable steps to mitigate the effects of any violation. The Privacy Officer shall communicate the results of the investigation and resolution of the complaint to the individual. If the individual is dissatisfied with the result, he/she shall be informed of the right to file the complaint with the U.S. Secretary of Health and Human Services.

The Privacy Officer will assure that **all HIPAA related complaints, their resolution, and any actions resulting there from are documented**. This documentation must be maintained for a minimum period of six (6) years from the date of final resolution.

There shall be no retaliation against any individual or person served, workforce member, or Privacy Officer for having filed or assisted in the filing of a complaint, or for investigating or acting on a complaint. Any workforce member who becomes aware of any such retaliatory action shall immediately complete an incident report

HIP-00-011

Subject:

Use or Disclosure of Protected Health Information for Treatment, Payment or Health Care Operations Purposes

Applies To: All covered healthcare components of NICAO

Purpose:

To issue instructions to all NICAO offices, facilities, programs and workforce members regarding the use and disclosure of protected health information (PHI) and necessary documentation of authority for such use or disclosure, for purposes of Treatment, Payment and health care Operations (TPO).

Policy:

Generally:

In compliance with 45 CFR Part 164, Iowa law, and policies HIP-00-004 through 007, an individual's authorization (or authorization from a personal representative) must be obtained prior to using or disclosing protected health information to do activities besides treatment, payment or health care operations. Exceptions to this rule are defined below:

Exceptions:

- PHI may be shared on a need to know basis with personnel within NICAO and/or business associates of NICAO for activities related to treatment, payment or health care operations.
- Limited PHI (medication history, physical health status and history, summary of course of treatment, summary of treatment needs, and discharge summary) may be used or disclosed for TPO without authorization if disclosure is to another program or facility of NICAO, or to community mental health agencies and/or State agencies with which there is a current agreement for the individual's care or services, and an attempt has been made to obtain the individual's consent to the disclosure.
- Limited PHI (medication information, summary of diagnosis and prognosis, list of services and personnel available for assistance) may be disclosed to family members, other relatives or friends involved in the individual's care, or payment for that care, if the individual is notified and does not object to the disclosure.

In emergency treatment situations, necessary information for treatment may be disclosed if, in the professional judgment of the provider, it is essential to the client's care to do so.

HIP-00-012

Subject:

Public Responsibility Uses and Disclosures of Protected Health Information (PHI)

Applies To: All covered healthcare components of NICAO

Purpose:

To issue instructions to all NICAO offices, facilities, programs and workforce members regarding uses and disclosures of protected health information (PHI) permitted or required in context of NICAO's public responsibilities.

Policy:

State and federal law permit and/or require certain uses and disclosures of PHI for various purposes related to public responsibility. Such uses and disclosures may be made without the agreement or authorization of the individual. The following uses and disclosures fall within this category:

Health Oversight Activities

PHI may be used or disclosed for activities related to oversight of the health care system; government health benefits programs, and entities subject to government regulation, as authorized by law, including activities such as audits, civil and criminal investigations and proceedings, inspections, and licensure and certification actions. Specifically excluded from this category are investigations of an individual that are not related to receipt of health care, or the qualification for, receipt of, or claim for public benefits.

Public Health Activities

PHI may be used or disclosed to:

- A public health authority authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury or disability, reporting vital events, conducting public health surveillance, investigations or interventions;
- A public health or other government authority authorized by law to receive reports of child abuse or neglect;
- A person subject to the jurisdiction of the Food and Drug Administration (FDA) regarding his/her responsibility for quality, safety or effectiveness of an FDA regulated product or activity, to report adverse events, product defects or problems, track products, enable recalls, repairs or replacements, or conduct post-marketing surveillance;
- PHI of potential organ/tissue donors may be disclosed to the designated organ procurement organization and tissue and eye banks.

Required by Law

PHI may be used or disclosed to the extent such use or disclosure complies with and is limited to the requirements of such law.

- Abuse and Neglect: Except for reports of child abuse or neglect, PHI about an individual believed to be a victim of abuse, neglect, or domestic violence may be disclosed to a governmental authority authorized to receive such reports if the individual agrees or the reporting covered entity believes, in the exercise of professional judgment, that the disclosure is necessary to prevent serious physical harm. If the individual lacks the capacity to agree, disclosure may be made if not intended for use against the individual and delaying disclosure would materially hinder law enforcement activity. The individual whose PHI has been released must be promptly informed that the report was made unless doing so would place the individual at risk of serious harm.
- Judicial Proceedings: PHI may be disclosed in response to a court order.
- Law Enforcement: PHI may be disclosed for the following law enforcement purposes and under the specified conditions:
  - Pursuant to court order or as otherwise required by law, i.e. laws requiring the reporting of certain types of wounds or injuries; or commission of a felony (but note reporting exceptions for certain privileged communications).
  - Decedent's PHI may be disclosed to alert law enforcement to the death if the covered entity suspects that death resulted from criminal conduct;
  - Limited PHI (medication history, physical health status and history, summary of course of treatment, summary of treatment needs and discharge summary) of inmates of a correctional facility may be disclosed to the facility as requested in order to provide care for the individual or ensure safety of the individual or others, but only if the individual is told of the request for records and does not object to the disclosure.
  - Compliance/Enforcement of privacy regulations: PHI must be disclosed as requested, to the Secretary of Health and Human Services related to compliance and enforcement efforts.

Serious Threats to Health or Safety

Consistent with applicable law and ethical standards, PHI may be used or disclosed if the covered entity believes in good faith that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public, and disclosure is to someone reasonably able to prevent or lessen the threat, or the disclosure is to law enforcement authorities to identify or apprehend an individual who has admitted to violent criminal activity that likely caused serious harm to the victim or who appears to have escaped from lawful custody.

Disclosures of admitted participation in a violent crime are limited to the individual's statement of participation and the following PHI: name, address, date and place of birth, social security number, blood type, type of injury, date and time of treatment, date and time of death, if applicable, and a description of distinguishing physical characteristics.

Disclosures of admitted participation in a violent crime are not permitted when the information is learned in the course of treatment entered into by the individual to affect his/her propensity to commit the subject crime, or through counseling, or therapy or a request to initiate the same.

Research

NICAO may disclose PHI for research provided that documentation is supplied that a waiver of the need for an individual authorization (or an alteration of the same right) has been approved by an IRB. Such documentation must include:

- Identification of the Institutional Review Board (IRB) and the date the waiver or alteration was approved
- A statement from the IRB that the waiver or alteration satisfies these criteria:
  - The disclosure of PHI represents a minimal risk to the privacy of the individual and a plan exists to protect the PHI from improper use or disclosure. There must also be a plan to destroy the identifiers at the earliest opportunity. Written assurances are also required that state redisclosure of PHI will not be made except where required by law.
  - The research could not be made without the waiver or alteration
  - The research requires the PHI
- A brief description of the PHI needed.
- A statement that the IRB follows the Common Rule and has reviewed the waiver or alteration.
- The documentation must be signed by the IRB's chair or the chair's designated representative.

PHI may be disclosed to a researcher conducting a review in preparation for the creation of a research protocol. NICAO will require representations from the researcher that they are:

- In the process of preparing a research study or protocol and require PHI to review and prepare it
- No PHI will be removed from the custody of NICAO
- All PHI disclosed in this preparation is necessary for research purposes

NICAO may disclose PHI on deceased clients for valid research purposes. NICAO will require that the researcher:

- Provide representations that the research is solely for decedents
- Provide documentation that the client is deceased, if this information is not already known to NICAO
- Provide representations that the PHI is necessary for research purposes

Decedents

PHI may be disclosed to coroners or medical examiners, as necessary for carrying out their duties, and to the designated organ procurement organization, and tissue and eye banks.

Specialized Government Functions

- National Security and Intelligence: PHI may be disclosed to authorized federal officials for the conduct of lawful intelligence, counter intelligence, and other activities authorized by the National Security Act.
- Protective services: PHI may be disclosed to authorized federal officials for the provision of protective services to the President, foreign heads of state, and others designated by law, and for the conduct of criminal investigations of threats against such persons.
- Public Benefits: PHI relevant to administration of a government program providing public benefits may be disclosed to another governmental program providing public benefits serving the same or similar populations as necessary to coordinate program functions or improve administration and management of program functions.

Workers' Compensation

PHI may be disclosed as authorized and to the extent necessary to comply with laws relating to workers' compensation and other similar programs.

Documentation

Documentation of disclosure made hereunder must be retained for a period of at least six years.

HIP-00-013

Subject:

Authorization for Use or Disclosure of Protected Health Information

Applies To: All covered healthcare components of NICAO

Purpose:

To issue instructions to all NICAO offices, facilities, programs and workforce members regarding the use and disclosure of protected health information (PHI), and necessary documentation of authority for such use or disclosure, when use/disclosure is for purposes outside of those permitted by law relating to Treatment, Payment or health care Operations, or public responsibilities (TPO).

Policy:

Generally, in compliance with 45 CFR Part 164 and Iowa law, all uses and disclosures of PHI beyond those otherwise permitted or required by law require a signed authorization according to the provisions of this rule. An authorization is required for each covered entity that is to receive PHI.

The provision of treatment, payment, enrollment in a health plan or eligibility for benefits may not be conditioned on the individual's provision of an authorization for the use or disclosure of PHI except:

- Relating to the provision of research related treatment;
- Relating to health care that is solely for the purpose of creating PHI for disclosure to a third party.

Content Requirements

Each authorization for the use or disclosure of an individual's PHI shall be written in plain language and shall include at least the following information:

- A specific and meaningful description of the information to be used or disclosed;
- The name or identification of the person or class of person(s) authorized to make the use or disclosure;
- The name or identification of the person or class of person(s) to whom the requested use or disclosure may be made;
- Purpose of the disclosure or statement that disclosure is at request of the individual;
- An expiration date, condition or event that relates to the individual or the purpose of the use or disclosure; the authorization shall state that it will expire after ninety days unless the individual has opted for a shorter or longer time. An individual may choose to specify a longer period of time for the duration of the authorization;
- A statement of the individual's right to revoke the authorization in writing, and exceptions to the right to revoke, together with a description of how the individual may revoke the authorization. Upon written notice of revocation, further use or disclosure of PHI shall cease immediately except to the extent that the office, facility, program or employee has acted in reliance upon the authorization or to the extent that use or disclosure is otherwise permitted or required by

law;

- Other statement that treatment, payment, enrollment or eligibility cannot be conditioned on individual signing the authorization or statement setting forth consequences of not signing;
- The dated signature of the individual;
- The individual's date of birth;
- The last 4 digits of the individual's social security number, and;
- If the authorization is signed by a personal representative of the individual, a description of the representative's authority to act on behalf of the individual.

Copy to Be Provided

If the covered entity is seeking the authorization, a copy of the authorization must be provided to the individual

Retention

A written or electronic copy of the authorization must be retained for a period of six (6) years from the latter of the date of execution or the last effective date.

HIP-00-014

Subject: Accounting for Disclosures of Protected Health Information

Applies To: All covered healthcare components of NICAO

Purpose:

To issue instructions to all NICAO offices, facilities, programs and workforce members regarding the provision of an accounting of disclosures of protected health information (PHI).

Policy:

Generally, an individual has a right to receive an accounting of disclosures of PHI by the covered entity during a time period specified up to six (6) years prior to the date of the request for an accounting except for disclosures:

- To carry out Treatment, Payment and Healthcare Operations (TPO) as permitted under law;
- To the individual about his or her own information;
- To persons involved in the individual's care, or other notification purposes permitted under law;
- Pursuant to the individual's authorization;
- For national security or intelligence purposes;
- To correctional institutions or law enforcement officials as permitted under law;
- That occurred prior to April 14, 2003.

The individual's right to receive an accounting of disclosures of PHI to a health oversight agency or law enforcement official must be suspended for the time period specified by such agency or official if the agency or official provides a written statement asserting that the provision of an accounting would be reasonably likely to impede the activities of the agency or official and specifying a time period for the suspension. Such a suspension may be requested and implemented based on an oral notification for a period of up to thirty (30) days. Such oral request must be documented, including the identity of the agency or official making the request. The suspension may not extend beyond thirty (30) days unless the written statement described herein is submitted during that time period.

Content Requirements: The written accounting must meet the following requirements:

- Other than as excepted above, the accounting must include disclosures of PHI that occurred during the six (6) years (or such shorter time period as is specified in the request) prior to the date of the request, including disclosures by or to business associates;
- The accounting for each disclosure must include:
  - Date of disclosure;
  - Name of entity or person who received the PHI, and, if known, the address of such entity or person;
  - A brief description of the PHI disclosed;
  - A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or in lieu thereof, a copy of the individual's authorization or the request for a disclosure;

- If, during the time period for the accounting, multiple disclosures have been made to the same entity or person for a single purpose, or pursuant to a single authorization, the accounting may provide the information as set forth above for the first disclosure, and then summarize the frequency, periodicity, or number of disclosures made during the accounting period and the date of the last such disclosure during the accounting period;
- If, during the time period for the accounting, the covered entity has made disclosures of PHI for research purposes, for 50 or more individuals, the accounting may provide:
  - The name of the research protocol or activity
  - A description, in plain language, of the activity including the purpose and the selection criteria.
  - A brief description of the type of PHI used.
  - The date or period, during which disclosures occurred, including the date of the last disclosure during the accounting period.
  - Contact information for the entity responsible for sponsoring the research.
  - A statement that the PHI of the individual may or may not have been disclosed for a particular research activity.

Provision of the Accounting

The individual's request for an accounting must be acted upon no later than sixty (60) days after receipt, as follows:

- Provide the accounting as requested, or;
- If unable to provide the accounting within sixty (60) days, the time for response may be extended by no more than thirty (30) additional days, provided that:
- Within the first sixty (60) days, the individual is given a written statement of the reasons for the delay and the date by which the accounting will be provided, and;
  - There are no additional extensions of time for response.
- The first accounting in any twelve-month period must be provided to the individual without charge. A reasonable, cost-based fee may be charged for additional accountings within the twelve month period, provided the individual is informed in advance of the fee, and is permitted an opportunity to withdraw or amend the request.

Documentation Requirements

The covered entity must document and retain documentation, in written or electronic format, for a period of six years:

- All information required to be included in an accounting of disclosures of PHI;
- All written accountings provided to individuals, and;
- Titles of persons or offices responsible for receiving and processing requests for an accounting from individuals.

HIP-00-020

Subject: Designating the Covered Entity Components of NICAO

Applies To: All covered healthcare components of NICAO

Purpose:
To designate and document the health care components of NICAO.

Policy:
NICAO is a hybrid entity that performs functions covered by HIPAA as well as non-covered functions. HIPAA penalties only impact the health care component of NICAO.

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
- Mail Services
- Associate Director of Planning and Development

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
- Mail Services

HIP-00-025

Subject: Use of PHI for Fundraising

Applies To: All covered healthcare components of NICAO

Purpose:
To explain the use of PHI in fundraising activities of NICAO.

Policy:
NICAO may ask clients if they would like to make a charitable contribution to NICAO. This request would be made during a face-to-face encounter. NICAO will not use PHI to solicit funds.

If NICAO chooses to solicit funds, an external list acquired from third parties may be used to solicit funds by mail, e-mail, or telephone contact.

HIP-00-030

Subject: Verification of Identity and authority prior to release of PHI

Applies To: All covered healthcare components of NICAO

Purpose:
To explain the ways NICAO will verify the identity and authority of any party requesting PHI.

Policy:
NICAO will verify the identity of the parties who are requesting PHI. NICAO will also verify that the identified requestor has the authority to ask for PHI.

Procedure:
This policy must be coordinated with activities described in HIP-00-005, Subject: Minimum Necessary Standard found on page 14.

For Public Officials
The staff may reasonably rely on any of the following to verify the **identity** of a request made by a public official or person acting for the official:

- Subpoenas or similar legal requests
- Public officials making a request:
  - in person, provided they show identification such as badges or licenses or are otherwise known to the NICAO staff person
  - through a written request on appropriate government letterhead
  - to a third party acting on behalf of the official, provided that proof of a legitimate relationship is shown to NICAO such as
    - a contract or memorandum of understanding
    - a purchase order that establishes the authority to request PHI for the official

The staff may reasonably rely on any of the following to verify the **authority** of a request made by a public official or person acting for the official after the requestor's identity is verified:

- a written or oral statement that the official has legal authority
- a request is made using a subpoena, warrant or other legal process issued by a grand jury or administrative tribunal

NICAO staff will exercise professional judgment at all times.

In Emergencies
In emergencies, where serious harm may come by not disclosing PHI, NICAO staff will use their best judgment. In such cases the request will be documented, whether or not PHI is disclosed.

For Other Situations

Upon receiving a request for PHI the NICAO staff person shall verify the identity of the requestor. The staff person shall also verify that the requestor has the authority to access PHI. Phone numbers used to fax PHI will be verified before transmission. If a fax number is believed to be used for the first time NICAO staff will fax a page requesting the receiver to fax back verification that they are the intended party.

HIP-00-035

Subject:

Preference to use de-identified data and limited data sets in place of PHI

Applies To: All covered healthcare components of NICAO

Purpose:

To explain alternatives to PHI to satisfy requests for health information.

Policy:

NICAO will attempt to use de-identified data or limited data sets whenever possible. Disclosures made using these methods do not need to be tracked in the accounting of disclosures. Both of these methods seek to remove the connection between the data disclosed and the individual described by the data.

Procedure:

De-identified Data

The Privacy Rule only protects individually identifiable information. By removing sufficient identifying fields a data file can be considered "de-identified". Two tests are used to determine when de-identification occurs:

1. A person with appropriate knowledge and experience determines that the individual cannot be identified using the information that remains.
2. Specific fields have been removed (called the "safe harbor" method) and the covered entity has no knowledge that the remaining information can be used to identify the individual it describes. These fields are:

- Names
- All geographic subdivisions smaller than a state, including
    - Street address
    - City
    - County
    - Precinct
    - Zip code
    - Geocodes equivalent to the above except for the initial three digits of a zip code as long as the Bureau of Census has said:
        - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, AND
        - The initial three digits of a zip code where less than 20,000 are contained are changed to 000.
- All elements of dates except year are removed for dates that relate to the individual. This includes birth date, admission date, discharge date, date of death, and all ages over 89 and

all elements of such dates (including year) indicative of age. An exception is allowed to create a grouping of all those who are age 90 or older.

- Telephone numbers
- Fax numbers
- E-mail addresses
- Social security numbers (SSNs)
- Medical record numbers (NICAO Client Number)
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- URLs
- Internet IP addresses
- Biometric identifiers, including finger and voiceprints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic or code

The covered entity must not have knowledge that the information so de-identified could reasonably be used to identify a person when combined with other available information.

De-identified data could be used freely for marketing or any other purpose.

See also related policy HIP-00-036, Subject: Proper use of the NICAO Client Number, found on page 45.

Limited Data Sets:

A second option is to use a limited data set. This file has some geographic information but does not allow for re-identification. A data use agreement limiting the receiver to only the specific stated purpose and nothing else.

A limited data set excludes the following fields:

- Names
- Postal address information other than city, state and zip code
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social Security Numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- URLs

- Internet IP addresses
- Biometric identifiers, including finger and voiceprints
- Full face photographic images and any comparable images

Limited Data Sets may only be used for research, public health or health care operations. NICAO is allowed to use a business associate to aggregate detailed PHI into a Limited Data Set.
The Data Use Agreement must limit the recipient of the data set as follows:

- The recipient cannot use or further disclose the data other than as permitted by the agreement
- The agreement will specify who is to use or receive the data set
- The recipient will apply appropriate safeguards to prevent further use or disclosure
- The recipient will report any non-covered use or disclosure to the covered entity.
- The recipient will bind any agents or sub-contractors who encounter the data set to the same terms.
- The recipient will not attempt to use any means to re-identify the data

HIP-00-036

Subject: Proper use of the NICAO Client Number

Applies To: All covered healthcare components of NICAO

Purpose:
To explain how to ensure the utility of the NICAO Client number as a key field to re-identify de-identified data. To explain how NICAO staff can protect client PHI by using client number appropriately.

Policy:
NICAO will take all necessary steps to ensure the future use of the NICAO Client Number as a key to re-identify de-identified data. NICAO will use client number wherever possible to de-identify forms and other information.

The NICAO Client Number is a "random" number that is assigned, as it is needed to clients of NICAO. It is never to be used as an explicit identifier or surrogate of an identifier like SSN. Doing so would destroy its value to NICAO. It will only be used to allow a linkage between de-identified data and client identifying information.

Client data is scanned to create a permanent record when required and the written data is destroyed after the required period of retention has passed, currently 5 to 7 years depending on the program. The Client Number is then purged from the system.

Procedure: See above.

Steps to ensure the future utility of NICAO Client Number:
- The client number is never used as a surrogate for SSN or other identifiers
- The printed client number-to-patient-name list is kept in a location that is only available to staff members.

HIP-00-040

Subject:

Use of authorizations signed and received prior to April 14, 2003

Applies To: All covered healthcare components of NICAO

Purpose:
To explain how to handle authorizations in use prior to HIPAA.

Policy:
The covered component of NICAO will use HIPAA compliant authorizations for all new clients who are assigned client numbers after NICAO is compliant with HIPAA.

Procedure:
All existing authorizations will continue to be honored. As they expire, if new authorizations are needed, HIPAA compliant authorizations will be used.

HIP-00-042

Subject:

Transition to the use of HIPAA compliant business associate contracts

Applies To: All covered healthcare components of NICAO

Purpose:

To explain how and when to replace old contracts with contracts compliant with the business associate provisions of HIPAA.

Policy:

Non-compliant contracts will be replaced according to the transition provisions of HIPAA.

Procedure:

Note: for the purposes of this standard a "renewal" is not a self-renewing contract (sometimes called an evergreen renewal).

- For contracts in existence prior to April 14, 2003, NICAO will replace them with language compliant with the business associate standard prior to April 14, 2004.
- All affected contracts will be replaced with compliant versions no later than April 14, 2004.

Following the compliance of all contracts this policy will automatically expire and will be removed from the Policies and Procedures manual.

HIP-00-050

Subject: Remote worker/work-at-home policy

Applies To: All covered healthcare components of NICAO

Purpose:
To explain how to safeguard PHI when working from home.

Policy:
The general rule is that PHI is never removed from the office for any purpose. However, there are situations where working with PHI outside of the office is sanctioned. In these cases extreme care will be maintained at all times.

A guiding concern for remote work is that NICAO must be able to account for the location of files containing PHI at all times. Remote work is only allowed where this concern is satisfactorily addressed.

Procedure:

Formal Check-in and Check-out Process
A formal written or electronic process that links the worker to the files they possess will be implemented. Any remote worker who does not follow this process will immediately lose the authority to remove PHI from the office and will be subject to other sanctions.

Remote Storage of PHI
Any PHI that is not checked-in on the same day it is checked-out must be stored in a secure location. One or both of the following is required:
- Storage in a locked room
- Storage in a locked drawer or cabinet

Use of Employee's Personal Computer
No permanent record of PHI will be left on an employee's home computer. All CD's, floppy disks or other electronic devices used to record data will be turned in to NICAO, erased, reformatted, or destroyed so as to render the PHI unreadable.