ARA PRIVACY POLICY

In compliance with the provisions of the Health Insurance Portability and Accountability Act of 1996, the Mental Hygiene Law, Section 33.16, and 42 USC §130d et. Seq., 45 CFR Parts 160 & 164) and the Confidentiality Law (42 USC § 290dd-2, 42 CFR Part 2), ARA has adopted the following procedures to assure the protection of "Protected Health Information" (PHI). The directives of this policy govern the use, disclosure, safeguarding and/or accounting of information that applies to any PHI that ARA creates or receives through normal business conduct.

NOTICE OF PRIVACY PRACTICES

It will be a standard ARA practice to inform a client of the use, release and clients' rights in respect to confidential healthcare information.

ARA has developed a "Notice of Privacy Information Practices" that states the client's rights with respect to the use and release of PHI. ARA will provide each client with a copy of this notice upon admission. ARA will retain a copy and any revisions of the Privacy Notice for six (6) years.

If ARA is in a joint relationship with another healthcare provider, the Privacy Notice is to reflect the joint relationship.

When ARA receives a request for a client's PHI, it is expected to notify the client about the request. Should the client be an inmate of a correctional facility or jail, ARA does not have to inform the client of the request for PHI.

ARA will post a copy of the Privacy Notice in a location where there is clear and easy access to all individuals who are enrolled in any of ARA's treatment programs. The Privacy Notice is also posted on our website (araservices.com).

RELEASE OF INFORMATION (DISCLOSURE) FORM

In compliance with federal regulations 45CFR Part 164 and New York State Law, it is the policy of ARA to receive authorization from a client prior to releasing or utilizing healthcare information. All clients must sign a consent form to the use and disclosure of PHI for the purposes of treatment, payment and conducting day-to-day operations of the agency.

PROCEDURE FOR OBTAINING CONSENT FOR USE OR DISCLOSURE**:**

1. The Receptionist will check the client's record when the client arrives to see if it includes a signed consent form.
2. If a consent form is found in the client's record, no further action is necessary.
3. If no consent form is included in the client's record, the Receptionist will provide the client with a Notice of Privacy Practices form and a consent form. The Receptionist will explain to the client that he or she must sign the consent form before seeing a physician or other caregiver.
4. The Receptionist will respond to the client's questions to the best of his or her ability. If the client has questions that the Receptionist cannot answer, the client should be referred to the Clinical Therapist or Case manager**.**
5. Before escorting the client to an examining or treatment room, the Receptionist must examine the consent form to make sure that the client has signed and dated it.
6. If a client is not able to sign a consent form, the Receptionist or Case Manger should contact the person who is responsible for obtaining consent.

7. If the client signs the consent form, the signed form should be attached to the client's record.
8. If the client refuses to sign a consent form, the Therapist should review the refusal as shown below.

When a Client Refuses to Sign the Consent Form

The reason that consent is needed must be explained to the client. Specifically, the client should be told that federal law prevents the practice from using the client's information for purposes of treatment or payment if consent is not given. The client should be told that he or she may request restrictions on the use and disclosure of his or her information, but that the practice is allowed to accept or reject those requested restrictions.

Procedure:

1. Review the reasons ARA must obtain consent before providing treatment.
2. The reason for the client's refusal to sign the consent should be determined, and the client's concerns should be addressed.
3. It should be explained to the client that he or she may request restrictions on the use or disclosure of PHI, but that the medical practice is not required to accept the restrictions and will not do so if they prevent the practice from meeting the needs of the client or obtaining payment for services.
4. If the client requests restrictions, follow the outline on page 3.

Consent to Emergency Treatment

Consent is not required prior to providing emergency treatment. A medical practice should not delay emergency treatment for the purpose of obtaining the client's consent to the use of PHI for purposes of treatment, payment, or health care operations. As soon as the emergency condition has been treated and the client is stable or recovering, an attempt should be made to obtain the consent.

Definition of Emergency Treatment

An emergency medical condition is generally defined by Medicare as a "condition manifesting itself by acute symptoms of sufficient severity (including severe pain) that immediate medical attention is needed to avoid placing the health of the individual in serious jeopardy, serious impairment of bodily functions, or serious dysfunction of any bodily organ or part."

Procedure:

1. The availability of a personal representative to sign the consent form should be determined. If a representative is available, policy P-3211 should be followed. If the personal representative will not sign the consent, the following steps should be followed.
2. An *unsigned* consent form should be used to document that the client required emergency treatment but was unable to provide consent.
3. When the client has recovered sufficiently to sign the consent form, or when a personal representative becomes available, the consent form should be reviewed with the client or personal representative and his or her signature should be obtained.
4. If the client or personal representative does not sign the consent form, the staff member attempting to obtain the consent should document the reason given on the form. The staff member should sign and date the form.

5. During the intake process, review with the client the Notice of Privacy statement and the Release of Information forms.[1]
    a. Inform the client of his/her rights to have his/her private behavioral and medical information maintained as confidential and private.
    b. Inform the client of who will have access to his/her personal medical information (through the Privacy Notice).
    c. Inform the client (through the Privacy Notice) that they have the right to restrict access to his/her personal medical information.
        i. Should the client request his/her health information be restricted, it is preferred that the client must complete and sign the Restriction Agreement Release of Client Information Consent Form, although verbal restrictions will be documented and complied with if appropriate.
        ii. The completed Restriction Agreement Release of Client Information Consent Form is to be maintained on the client's record for a period of at least six (6) years from either the date created or the date in which it is was last in effect.
6. Ask the client to read, complete, sign and date the authorization form on the designated areas.
7. Place the completed authorization form in the client's medical record.
8. Explain to the client that the authorization form can be revoked at any time. This revocation must be in writing and will go into effect the date it is signed. Revocation does not invalidate any use or disclosure that occurred prior to the date of the revocation.
9. Provide the client or his/her representative with a copy of the signed release.
10. ARA must retain the signed authorization form for a period of six (6) years.

RESTRICTIONS

A client has the right to restrict access to his/her private treatment/medical information.

1. A client can request that his/her private information not be provided to family members.
2. A Client can verbally, or in written format, request that access to his/her private medical information is restricted. Restrictions will be documented in the clinical record.
3. ARA can terminate the agreement to restrict a client's PHI if the information is needed to provide emergency care or treatment. Any information obtained to help provide emergency care will not be used beyond the provision of emergency care. Should ARA decide to terminate a restriction agreement with a client without the client's agreement, any information prior to the termination will need to be maintained as confidential and private. Information obtained after the date and time of the notice of agreement termination would not necessarily be held as confidential and private.
4. ARA will maintain a record of agreed upon restrictions for a minimum of six (6) years from the date it was created or the date it was last in effect, whichever is later, or until legal destruction of the record.

When a client requests that ARA restrict the use of PHI for treatment, payment or healthcare operations:

1. ARA does not have to agree with the client's request.
2. If ARA agrees to the request, PHI may not be released for treatment, payment or healthcare operations unless the information is needed to provide emergency treatment to the client.
3. If the information is released for emergency treatment to the client, ARA must request that the person(s) providing the treatment use the PHI only for the purpose of treatment.

[1] If the PHI contains HIV related information, an additional release of confidential HIV information form that is approved by the Department of Health must be completed. A prohibition on redisclosure notice must accompany disclosures of such information, in accordance with Public Health Law, Article 27F.

ARA may terminate an agreement to restrict the use of PHI if:

1. The client agrees or requests the agreement to be terminated in writing.
2. The client agrees or requests the agreement to be terminated verbally and the termination is documented in the client's medical record.
3. ARA can terminate the agreement to restrict a client's PHI if the information is needed to provide emergency care or treatment. Any information obtained to help provide emergency care will not be used beyond the provision of emergency care. Should ARA decide to terminate a restriction agreement with a client without the client's agreement, any information prior to the termination will need to be maintained as confidential and private. Information obtained after the date and time of the notice of agreement termination would not necessarily be held as confidential and private.
4. ARA informs the client that the agreement to restrict PHI is terminated. Information gathered during the terms of the restriction will continue to be restricted. Information gathered after the termination of the agreement will not be restricted.

Evidence of agreements of restriction and the termination of such agreements must be made in the client's medical record. This information is to be maintained by ARA for a period of six (6) years.

PROCEDURE:

Explain the Privacy Notice to the client by detailing the following:

- Inform the client of his/her rights to have his/her private behavioral and medical information maintained as confidential and private.
- Inform the client of who will have access to his/her personal medical information
- Inform the client that they have the right to restrict access to his/her personal medical information.

Should the client request his/her health information be restricted, it is preferred that the client must complete and sign the Restriction Agreement Release of Client Information Consent Form, although verbal restrictions will be documented and complied with if appropriate.

The completed Restriction Agreement Release of Client Information Consent Form is to be maintained on the client's record for a period of at least six (6) years from either the date created or the date in which it is was last in effect.

ARA can terminate the Restriction Agreement Release of Client Information agreement only after informing the client of the termination of the agreement. Once the client is notified, ARA must maintain the confidentiality of the information in the original agreement prior to the termination of the agreement. Information accumulated after the notification to terminate the agreement would not be covered or restricted by the terms of the previous agreement.

REQUESTING INFORMATION FROM OUTSIDE AGENCIES

When a staff member requires information on a client's health condition from another provider, he or she may request the information without restriction. The client need not authorize this request. The information requested must, however, be used for the purpose of evaluating the client's medical condition or determining a course of treatment. A client may have requested and been granted a restriction on the information that is to be used or disclosed to other providers. In this situation, the restriction must be honored.

DISCLOSURE/USE OF PHI

DISCLOSURES FOR WHICH CONSENT IS NOT REQUIRED:

TREATMENT, PAYMENT AND HEALTHCARE OPERATIONS

ARA may use or disclose PHI without specialized consent if:

1. The information is used to carry out ARA's treatment, payment or healthcare operations.
2. The information is used for healthcare auditing operations in efforts to detect healthcare fraud, detect abuse or compliance.
3. ARA is using the notes for its own training programs in which students, trainees or practitioners in mental health learn under the supervision of ARA personnel.
4. ARA is using the psychotherapy notes is **not** needed to defend a legal action or any other legal proceeding brought forth by the client.
5. ARA uses the psychotherapy notes when used by a medical examiner or coroner.

PUBLIC HEALTH/LAW ENFORCEMENT AGENCIES

ARA may use or disclose PHI without specialized consent to public health authorities or law enforcement agencies without the written authorization of the client or the opportunity for the client to agree or object to the release of confidential healthcare information.

Procedure:

1. Inform the client that PHI may be provided to public health authorities. The content of the information may include:
    a. Prevent or control a disease, injury or disability
    b. Report a communicable disease
    c. Report a birth
    d. Report a death
    e. Report child abuse or neglect
    f. Report or collect information about adverse effects of food or dietary supplements
    g. Report or collect information about defects or problems with a product including any deviations of a biologic product
    h. Report defective products to enable product recalls, repairs, replacements, or look back (in efforts to locate and notify individuals who have received products that are the subject of a look back).
    i. Follow up with the use of products to comply with the requirements of the Food and Drug Administration
    j. Investigate a work-related illness or injury
2. In the event that ARA believes a client is a victim of abuse, neglect or domestic violence, PHI will be provided to a government authority, social service, protective services agency or other agency authorized by law to receive report of such abuse, neglect or domestic violence.
    a. ARA will inform the client if/when this information will be provided to report the abuse, neglect or domestic violence to an authorized agency.
    b. The client can refuse to have the abuse, neglect or domestic violence reported.
    c. ARA can overrule the client's decision to not report the abuse, neglect or domestic violence if it is determined that the reporting is necessary to prevent serious harm to the individual or other potential victims.
    d. If the client is unable to agree to have the information reported about abuse, neglect or domestic violence, a law enforcement or public health official will act upon the

information only if it is determined that waiting until the client agrees to report the information could adversely affect the outcome.

e. ARA will not inform a personal representative of the report of abuse, neglect or domestic violence if ARA believes the personal representative is responsible for the abuse, neglect or other injury.

3. ARA may provide PHI to a health oversight agency for the purpose of conducting audits, civil, administrative or criminal investigations, inspections, licensure, disciplinary actions or other activities necessary for the operations of ARA.
4. ARA may provide PHI if the client is under investigation or to investigate if the client qualifies to receive public benefits when the client's health status is needed to make the decision about receiving the public benefit.
5. ARA may provide PHI in response to a court order. Only the information requested may be provided.
6. ARA may provide PHI in response to a subpoena, discovery request or other lawful process only after informing the client that the PHI has been requested.
7. ARA may provide information to a law enforcement agency seeking PHI if the agency has attempted to reach the client using the client's last known address, if the notice for the information explains the need for the PHI, and the time for the client to raise objections to the law enforcement agency has elapsed.
8. ARA may provide information to a law enforcement agency seeking PHI if ARA has attempted to reach the client but was unsuccessful.
9. ARA may provide information about certain types of disorders, wounds or other physical injuries upon court order, court-ordered warrant, subpoena, summons, grand jury subpoena, civil investigative demand or other similar process when it is determined that the information is relevant and material to the investigation and that de-identified information could not be used.
10. ARA may provide PHI to a law enforcement official for the purpose of identifying, locating a suspect, fugitive, material witness or missing person. This information is limited to:
    a. Name and address
    b. Date and place of birth
    c. Social security number
    d. Blood type and rh factor
    e. Type of injury
    f. Date and time of treatment
    g. Date and time of death, if applicable, and
    h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars and tattoos
11. ARA is not permitted to release information about the client's DNA, DNA analysis, dental records or samples, typing or analysis of body tissues or fluids.
12. ARA prohibits the law enforcement agency from using the PHI for purposes other than the reason it was requested and requires the agency to return the information to ARA or destroy the information at the end of the litigation.
13. ARA may release PHI about a client in response to a law enforcement official's request if the client is suspected of being a victim of a crime and agrees that ARA may provide the information. If the client is incapacitated and cannot agree to the release of the information, ARA will provide the information if the information is not going to be used against the client, that the investigation would be adversely affected by waiting for the client to agree to the release of the information, or providing the information is in the best interested of the client.
14. ARA may release PHI about a client who has died to a law enforcement official if ARA suspects that the death may have resulted from criminal activity.

15. ARA may release PHI to a law enforcement official if there is evidence of criminal conduct on ARA's premises.
16. ARA may release PHI to a coroner or medical examiner to identify a deceased client, determine the cause of death or other duties authorized by law.
17. ARA may release PHI to funeral directors to carry out their duties with respect to the deceased.
18. ARA may release PHI to organ procurement organizations or other entities for the purpose of facilitating organ, eye or tissue donation or transplantation.
19. ARA may release PHI if it believes the information will prevent or lessen a serious/imminent threat to the health or safety of a person or the public. This information may be provided to the person(s) who are the target of the threat or for the identification or apprehension of an individual making the threat.
20. ARA may release PHI to law enforcement officials when it appears that an individual has escaped from a correctional institution or from lawful custody.
21. ARA may release PHI to Armed Forces personnel to assure the proper execution of the military mission if a notice has appeared in the Federal Register stating the military command authorities and the purposes for the PHI.
22. ARA may release PHI to the Department of Veterans Affairs (DVA) of a client who is a member of the Armed Forces upon separation or discharge from the military service for the purpose of determining eligibility of benefits administered by the Secretary of Veterans Affairs.
23. ARA may release PHI of foreign Armed Forces personnel to assure the proper execution of the military mission if a notice has appeared in the Federal Register stating the military command authorities and the purposes for the protected healthcare information.
24. ARA may release confidential healthcare information to authorized federal officials to conduct intelligence, counter-intelligence or other national security activities authorized by the National Security Act or the Department of Homeland Security.
25. ARA may release PHI to authorized federal officials to provide protective services to the President, to foreign heads of state or for the conduct of investigations.
26. ARA may release PHI to the Department of State to make medical suitability determinations for security clearance or for mandatory service abroad.
27. ARA may release PHI to a correctional institution or law enforcement official having custody of an inmate to provide healthcare to the person, to ensure the health and safety of the client or other inmates, to ensure the health and safety of the officers, employees or others at the correctional facility, to ensure the health and safety of those responsible for the transportation of the inmates, to ensure the health and safety of law enforcement on the premises of the facility and to maintain the safety and security of the facility.
28. ARA may release PHI to comply with laws relating to workers' compensation or other similar programs that provide benefits for work-related injuries or illness.

DISCLOSURE/USE – INTERNAL BUSINESS PURPOSES

ARA will determine internally who should access confidential client healthcare information in performing duties relative to client care and billing functions.

PROCEDURE:

ARA's HIPAA Compliance Officer will determine the degree of access for each employee based on his/her function within the agency.

Employees with Unlimited Access:

The following categories of employees are permitted unrestricted access to personal health information:

- Attending physicians
- Consulting physicians
- Nursing personnel
- Therapists, Social Workers, Psychologists, Case Managers
- The Executive Director
- The HIPAA Compliance Officer

Employees with unrestricted access to confidential healthcare information are limited to accessing information for which they are responsible for the provision of healthcare. Individuals are not permitted to access confidential healthcare information for those in which they are not responsible for the provision of healthcare. This means, a member of the physician or nursing staff is not permitted to review a medical record of a client in another care area, of a friend, a relative, upon request of another client, or a client for whom payment is not expected for healthcare services as in the case of physicians.

Employees with Restricted Access:

The following categories of employees are permitted limited access to personal health information, including demographic and insurance information, name, address, telephone number, insurance carrier, social security number, date of birth and clinical chart number:

- Office and Billing Personnel

Employees with restricted access to confidential healthcare information are expected to request permission to view the information that is necessary to achieve the purpose of providing the element of healthcare. Individuals with restricted access to healthcare information who need to see any portion of confidential healthcare information must request permission to view the information. ARA will review the requests on an individual basis.

Employees with no Authorization for Access

The following categories of employees are not permitted access to personal health information:

- Security
- Housekeeping/Maintenance staff

DISCLOSURE/USES – EXTERNAL

ARA may provide limited confidential healthcare information upon request if the request is made by another hospital, health insurance agency or health information clearinghouse or if requested by a business associate of ARA for the purpose of providing professional services to ARA, upon receipt of a signed release of information from the client.

PROCEDURE:

1. Prior to disclosure of PHI, the reasons why the information would be needed should be known or determined. Examples of reasons to provide PHI may include, but are not limited to:
    a. At the request of the client or authorized personal representative;
    b. As needed for treatment, operations or billing;

c. Specific requirements of providers who have an indirect relationship with the client such as a laboratory or pharmacy;
d. If the request is made to provide care to an inmate of a correctional facility or jail;
e. If the request is made by a representative of an accrediting body, governmental or non-governmental oversight agency;
f. If the request is made for the purpose of detecting healthcare fraud or abuse or to insure compliance with care mandates.
g. If the request is made for the purpose of detecting health care compliance.

2. The PHI that may be released is limited to the following:
    a. Complete legal name, address and telephone number
    b. Date of Birth
    c. Social Security Number
    d. Past medical history information
    e. Documentation of completed diagnostic tests, laboratory results.

DISCLOSURE/USES FOR RESEARCH PURPOSES

ARA may provide limited confidential healthcare information if requested for research purposes and according to ARA's policy on research activities.

It is ARA's policy to release PHI for research provided that the client has signed a waiver agreeing to the release of the information.

a. ARA has documentation that PHI is needed to prepare research protocol.
b. No PHI will be removed from ARA.
c. The PHI is needed for research purposes only.
d. The researcher will provide ARA with any PHI on any deceased clients who participated in the research.
e. The researcher will provide ARA with documentation of the death of any clients who participated in the research.

PROCEDURE:

1. Identify if a client is a subject of a research project.
2. Review the terms of the research project.
3. Provide the client with the Waiver of Authorization Form to sign and date.
4. Maintain the Waiver of Authorization Form on the client's medical record.
5. Maintain the Waiver of Authorization Form for a period of six (6) years.

LIMITED DATA SET (Also known as De-identification)

ARA will disclose a limited amount of information about a client, in the form of a limited data set, if the client is aware of the information and if the information is being used for research, public health or healthcare operations.

In response to a request for a limited data set, ARA will create a set of information that causes anonymity by **NOT** including the following information:

a. Name
b. Postal address information other than town/city, state and zip code.
c. Telephone number(s)
d. Fax number(s)
e. Electronic mail address(es)

f. Medical record number(s)
g. Health plan beneficiary number(s)
h. Account number(s)
i. Certificate/license number(s)
j. Vehicle identifiers, serial numbers and license plate number(s)
k. Device identifiers and serial number(s)
l. Web Universal Resource Locators (URLs)
m. Internet Protocol (IP) address number(s)
n. Biometric identifiers including voice and finger prints
o. Full face photographic images and any other comparable images
p. Any other unique identifying numbers, characteristics or codes.

DISCLOSURE/USES – DECEASED INDIVIDUALS

ARA will continue to protect healthcare information about a deceased client for as long as ARA maintains the client's medical record.

PROCEDURE:

1. Upon death, ARA is to complete and close the medical record and store according to the current method of clinical documentation (electronic or hard copy).
2. ARA is to maintain the deceased's record according to applicable federal and state laws.
3. ARA is to release to the funeral director for the deceased any information needed so that the funeral director can carry out duties with respect to the deceased. The release of information can occur when there is a reasonable anticipation of death.
4. ARA is to treat any family members or other legal representatives who have authority to act on behalf of the deceased as the deceased with respect to PHI.
5. If the deceased's healthcare information is being requested for research purposes, ARA must ensure the information is maintained as confidential, private and de-identified prior to releasing the information.

ACCOUNTING OF DISCLOSURES

ARA will adopt a routine procedure for recording disclosures. Whenever a disclosure of information is made from a client's record, a notation shall be made on a log which will become part of the clinical record. This log will record:

a. the Client's name,
b. the date of disclosure,
c. to whom the information was disclosed,
d. the method in which verification of the person requesting the information was substantiated,
e. the name of the person who authorized the disclosure,
f. the details of the disclosure,
g. if and when the client requests the list of disclosures, the date in which the list was given to the client.

A client may request a list of times that their personal health information has been released within a six year time frame. ARA does not have to comply with this policy if the information was:

a. Used to provide client care, payment for services or healthcare operations,
b. Provided to the client,
c. Used for ARA's directory,

d. Provided to employees responsible for the client's care,
e. Provided to national security or intelligence,
f. Used as a part of limited data set,
g. If provided to correctional facilities or law enforcement officials and accessed prior to the date of compliance to this policy.

ARA must suspend a client's right to receive a list of times PHI had been released to a health oversight agency or law enforcement official if the agency or official provides ARA with a written statement that says the client is likely to impede the agency's or official's activities and the time period for the suspension.

If the information to temporarily suspend a client's right to receive a list of times PHI had been released to a health oversight agency or law enforcement official is provided verbally, ARA is to document the statement made, name the individual making the statement and temporarily suspends the client's right to the list of releases. This suspension can be no longer than 30 days unless ARA receives a written request for suspension.

PROCEDURE:

1. When a client indicates to any staff member that he or she would like to receive an accounting of disclosures, the client should be told to contact their therapist.
2. The therapist will inform the client that they must submit a written request for an accounting log to the program director.
3. The program director will determine if the client has had their right to receive an accounting of disclosures suspended by any law enforcement of health-oversight agency.
4. If the client has not been suspended, then the client will be provided with a list of times that Protected Health Information has been released, ARA will provide a written account of the times this information had been released. This written account is to include:
    a. The date of release.
    b. Name of the person or entity and address who received the information.
    c. A brief description of the information released.
    d. A statement of the purpose for the information or, instead of a statement, a copy of the written request for the information.
5. If multiple requests were made by the same individual or entity, ARA is to provide the frequency, periodicity, number of times the information was released and the date of the last release during the period requested by the client.
6. If ARA disclosed the healthcare information for a particular research purpose for 50 or more individuals, ARA is to provide:
    a. The name of the research activity.
    b. A description (in plain language) of the research activity to include the purpose and the reason used to select particular medical records.
    c. A brief description of the type of PHI that was disclosed.
    d. The date or time period when the disclosures occurred including the date of the last disclosure.
    e. The name, address and telephone number of the organization that sponsored the research and of the researcher who received the confidential healthcare information.
    f. A statement that the confidential healthcare information may or may not have been disclosed for a particular research activity.
    g. An assist in contacting the organization that sponsored the research and the researcher upon request by the client.

7. ARA is to act on the client's request no later than 60 days after receiving the request. ARA is to:
    a. Provide the client with the list.
    b. Communicate to the client the reasons why the list will not be prepared within 60 days.
    c. Communicate to the client the date in which the list will be prepared.
    d. Complete the request within an additional 30 days.
8. ARA must provide the client with the first request for a list in any 12-month period with no charge. ARA may charge the client a reasonable, cost-based fee for each future request within the 12-month period provided that ARA informs the client in advance of the fee and offers the client the chance to withdraw or modify the request to avoid or reduce the fee.
9. ARA must document the client's request for a list, a copy of the information provided to the client and the titles of the persons or offices responsible for receiving and processing the request by the client.

BUSINESS ASSOCIATES

A business associate is any person or organization that performs or helps to perform any function or activity that involves the use or disclosure of PHI. In short, any person or organization that receives or uses PHI from ARA Certified Programs is a business associate. A business associate also may be a person or organization that *creates* PHI for the agency. PHI may be disclosed to business associates only if ARA Certified Programs receives satisfactory assurances that the business associate will safeguard the privacy of the PHI that it creates or receives.

PROCEDURE:

ARA will make every reasonable attempt to prevent the indiscriminate disclosure of PHI to outside entities identified as Business Associates unless there is an agreement identifying the role of the business associate and the business associate's uses for the PHI.

1. Define the business associates of ARA.
2. Create a business associate agreement that identifies the following:
    a. Identifies the uses for the client's PHI permitted under the agreement.
    b. Clearly states that the PHI is not be used beyond the limits set forth in the agreement.
    c. Lists who within the business associate organization will have access to the client's PHI including those who are responsible for the management and administration of the business associate organization.
    d. Identifies how the PHI will be protected from indiscriminate use by the business associate and its' employees.
    e. Clearly states how ARA will be contacted if the client's PHI is inappropriately disclosed.
    f. Identifies how any subcontractors of the business associate will safeguard against any indiscriminate use of a clients' PHI.
    g. Lists those types of client's PHI that the business associate will not be able to obtain without additional consent or authorization including psychotherapy notes, any information compiled for use in a civil, criminal or administrative action proceeding, and information that is subject to the Clinical Laboratory Improvements Amendments of 1988.
    h. Identifies how the client's PHI will not jeopardize the health, safety, security, custody or rehabilitation of the clients or any safety of an officer, employee or other person should the information be of inmate of a correctional facility or jail.

i. States the method by which ARA will provide the business associate with any changes or amendments to any of the client's PHI once given to the business associate by the company.
j. Identifies where the business associate's records, books and internal practices are located so that these items can be inspected to determine if the client's PHI is being utilized for the intended purpose.
k. The Business Associate will make available all records that are related to the use and disclosure of PHI available to ARA's Compliance Office for purposes of determining compliance with the privacy standards.
l. Clearly identifies how the PHI will be returned to ARA or destroyed by the business associate at the termination of the contract for services.
m. Provides for PHI that cannot be feasibly returned at the end of the contract, to be protected or destroyed and to have further use limited and how the business associate will inform ARA that the return of the PHI would create a hardship for the business associate.
n. Identifies how a contract for services with the business associate can be terminated if ARA learns that the business associate has breached any terms of the business associate agreement and has not corrected the breach satisfactorily.

3. Establishes a policy that insures that ARA investigates compliance with the business associate agreement if a complaint is made that the business associate has violated the terms of the agreement.
4. ARA has the right to terminate the service contract should it find that the business associate is in breach violation of any of the terms of the business associate agreement contract if steps to correct the breach fail.
5. If after determining a business associate is in breach of their business associate agreement should ARA find it not feasible to terminate the service contract, ARA shall notify the Office of Civil Rights of the breach found, and of ARA's intent to continue the services contract with the business associate, clearly stating the nature of the business and why terminating the contract is not feasible.

In addition to the Business Associate Agreement, if the business relationship entails the sharing of confidential data or access to ARA's computer information systems, the execution of a Confidentiality and Non-Disclosure Agreement, Data Exchange Agreement, and/or Computer/Application Sharing Agreement is required.

Those agencies that are conduits of PHI, such as the United States Postal Services, the United Parcel Services, delivery truck drivers and the like, are not considered to be business associates and are not required to sign business associate agreements. However, **all** visitors to ARA's programs are required to enter the premises through the reception area and sign a sign-in sheet that prominently advises of the need to protect the confidentiality of all PHI that maybe encountered during the visit.

RELEASING INFORMATION

The amount of information that will be made accessible in response to a request for information will be limited to the minimum necessary for the intended purpose. When divulging information, in general, care should be taken to avoid unnecessary disclosures.

PROCEDURE FOR RELEASING INFORMATION:

Questions about disclosures should be directed to the Privacy Officer before the documents are released.

Requests Made In Person

The steps outlined below for written requests should be followed when a request for information is made in person.

Written Requests

The steps outlined below should assist in determining what information should be released based on the type of request:

1. Obtain the properly authorized release of information signed by the client or his/her representative.
2. Verify the identity of the person requesting the PHI. Before disclosing information to another provider for treatment purposes, a staff member must verify the identity of the person making the request. In other words, the staff member must determine that the person making the request is, in fact, a health care professional who is requesting the information for the purpose of treatment. If the professional is known to the practice, is a member of a group that is known to a staff member, or is affiliated with a facility that is known to the practice, a staff member may presume that the provider is who he or she claims to be. Otherwise, a staff member should obtain additional assurances sufficient to satisfy his or her professional judgment that the person requesting the information is a health care provider who will use the information for purposes of treatment.
    a. Employees of ARA are to request identification from any person requesting PHI if the identity or the authority of the person is not known to the employee.
    b. ARA may rely on the following as verification of identity when the release of PHI is being requested by a public official:
        i. If the request is made in person, the person provides an ID badge, official credentials or other proof of status.
        ii. If the request is in writing, the letter is written on the appropriate government letterhead.
        iii. If another person on behalf of a public official makes the request, a written statement on appropriate letterhead or other evidence or documentation such as a contract for services, memo or purchase order that establishes that the person is acting on behalf of the public official.
        iv. An oral statement of legal authority if a written statement would be impractical.
    c. If the request is made in the form of a warrant, subpoena, order or other legal process issued by a grand jury or other judicial body.
    d. Employees of ARA are to obtain any documentation, statements or representations from the person requesting PHI. The documentation, statements or representations can be either verbal or written. The decision to release PHI can be made based upon written documentation if it is signed and dated by the individual making the request. The PHI should be sent to the verified business address of the provider requesting the information.
3. Define the reason for the needed PHI. Examples of reasons PHI may be needed include, but are not limited to:
    a. For the provision of client care

b. For billing of client care
c. For case management or coordination
d. For utilization review

4. Define the amount of PHI to be provided for each request. Information provided without definition shall be limited to:
    a. Complete legal name, address and telephone number, and guarantor
    b. Date of birth
    c. Social security number and/or insurance information
    d. Past behavioral history information
    e. Documentation of completed diagnostic tests, laboratory values, results of sessions or consultations.
5. Each written request for PHI by parties not directly involved in the provision of client care are to be maintained by ARA and retained for a period of no less than six (6) years, or until the time of record destruction.
6. Document the release in the client's clinical record by noting:
    a. The date of release;
    b. The name of the person or entity and address who received the information;
    c. A brief description of the information released; and
    d. Filing a copy of the written request for the information.

Telephone Requests

As a general rule, information regarding PHI may not be disclosed over the telephone, due to the difficulty in verifying the identity of the caller and ensuring the security of the transmission. Therefore, telephone requests must be handled as follows:

1. Callers must be advised that it is against ARA policy to provide information about clients over the telephone, including confirming the caller whether the client is even enrolled in any of ARA's treatment programs.
2. Explain that all requests must be in writing on letterhead, with original signatures. An alternative is the caller can provide his/her name, phone number, relationship to the client and the reason for the call. The caller should be advised that if the individual is, in fact, enrolled in the program, the call will be returned after the appropriate follow-up is completer. If the caller selects the latter option, the information provided by the caller should be promptly relayed to the client's therapist for further handling.

The call recipient should always rely on the exercise of professional judgement, as an exception to the above is in cases where the information requested is for the purpose of emergency treatment of the client.

Facsimile Transmissions

If there are no other timely or reasonable alternatives, and provided that appropriate safeguards are followed, it is acceptable to transmit PHI via facsimile (fax) upon receipt of a fully executed release.

Reasonable efforts must be made to ensure that facsimile transmission is sent to the correct destination. Reasonable efforts should include:

1. Obtaining the name and phone number of the party receiving the information

2. Verifying the fax phone number with the intended recipient prior to the transmission of data. When feasible, the sender and recipient shall agree on a time for transmission or take other appropriate steps, in order toe reduce the lag time between transmission and pickup;
3. Verify the receipt of the information to the appropriate party.
4. To the extent possible, destination numbers must be programmed into the machine to eliminate errors in transmission from misdialing

When sending a fax, the cover page should always be on ARA letterhead and must contain a confidentiality notice that indicates that the information is confidential and prohibits its redisclosure. It should also include the sender's name, business address and phone number, the fax recipient's name, fax number, business address and regular telephone number. The transmission date, time and what machine the fax was sent from should also be noted on the form, if the fax machine does not automatically send this information on the fax. In addition, standard confidentiality transmission footer should always appear on the bottom of the cover page, the wording of which should read as follows: *"Confidentiality Notice: Warning! Unauthorized interception if this communication is a violation of federal and state law. The documents accompanying this fax transmission may contain information which is legally privileged. The information is intended only for the use of the recipient. You are hereby notified that any disclosures, copying, distribution or the taking of any action in reliance on the contents of this faxed information is strictly prohibited. If you have received this fax in error, please immediately notify the sender by telephone to arrange for return of the original documents to sender."*

Whenever possible, all pages of a fax, including the cover page, must be marked confidential.

Facsimile machines should be located in secure areas with limited access to appropriate personnel. Incoming data should be delivered in an expeditious, confidential manner and never left sitting on or near the machine.

Documentation of these types of disclosures must include the fax cover sheet sent with the transmission.

<u>E-Mail</u>

The HITECH Act adds further protections for Electronic PHI, or EPHI. These include requirements that EPHI access be limited to the minimum amount required for healthcare operations. HITECH also adds substantial notification requirements and potential penalties for breaches of EPHI.

All outgoing e-mail correspondence originated by an ARA employee must contain a disclaimer that reads as follows: *"Disclaimer: This message (including any attachments) contains confidential information intended for a specific individual and purpose, and is protected by law. If you are not the intended recipient, please notify the sender by e-mail, delete and destroy this message and any attachments. Any disclosure, copying, or distribution of this message or the taking of any action based on it, is strictly prohibited."*

<u>RECOGNIZING A CLIENT'S PERSONAL REPRESENTATIVE</u>

It is the policy of ARA to recognize a client's personal representative as the client with respect to the client's protected health information.

PROCEDURE:

1. Verify that the client has another individual identified as a personal representative. This situation might exist in the case of an un-emancipated minor.
2. Recognize that a parent, guardian or other person acting in-loco-parentis has the authority to act on behalf of the client who is an un-emancipated minor. Document this relationship in the client's medical record and attach any documentation to support this relationship.
3. Realize that the un-emancipated minor can over-ride any decisions made by a parent, guardian or other person acting in-loco-parentis if he/she consents to the healthcare service. The minor's consent to healthcare will be acknowledged even if the parent, guardian or in-loco-parentis have not consented to the health service or if the decision for health service is in contradiction to the minor's decision. Document the decisions regarding consent to healthcare services provided to the un-emancipated minor and the individual(s) responsible for the decisions.
4. ARA may refuse to accept an individual as a personal representative of a client if ARA believes the client has been or may be subjected to domestic violence, abuse or neglect, or the client's life could be endangered by the individual identified as the client's personal representative.
5. ARA may exercise professional judgment and decide that it is not in the best interest of the client to accept the individual identified as the client's personal representative should there be a threat of violence, abuse, neglect or endangerment of life.

CLIENT'S RIGHT TO ACCESS PHI

It is the policy of ARA to provide clients with their personal healthcare or treatment information. This information can be provided through alternative means upon client request. (ARA does not need an explanation from the client as to why the requested healthcare information is to be provided via an alternative means.)

Please refer to the section of this policy manual entitled, "Access to Clinical Records" for more information.

AMENDMENT OF PHI

ARA may agree to make changes to a client's medical record upon client request. Please refer to the section of this policy manual entitled, "Access to Clinical Records" for more information.

COMPLAINTS

ARA will review and address any complaints in regard to protecting PHI.

PROCEDURE:

1. Any complaint regarding the privacy of confidential healthcare information is to be made in writing to ARA's Administrative offices, to:

   Compliance Officer
   ARA
   4222 Bolivar Road
   Wellsville, NY 14895
   585-808-7660 Confidential Hotline
   585-593-5700 X553 Compliance Officer Desk

2. Upon receiving the complaint, the Compliance Officer is to:
    a. Document the complaint in the Complaint Log.
    b. Document the date, time and name of person making the complaint in the Complaint Log.
    c. Investigate the compliant.
    d. Document the resolution of the complaint in the Complaint Log.
    e. Communicate the outcome of the complaint with the individual filing the complaint, within a thirty day period of the receipt of the complaint.
3. The Compliance Officer is to communicate the number of complaints and resolutions during routine ARA Board of Director meetings.
4. The client may appeal the Compliance Officer's findings by contacting the Bureau of Quality Management of the NYS Office of Mental Health.

ADMINISTRATIVE REQUIREMENTS

STAFF REQUIREMENTS:

It is the policy of ARA to employ one individual to serve as the Compliance Officer for the organization either solely or in addition to their standard duties.

1. The Compliance Officer is responsible for ensuring the confidentiality of all client PHI.
2. The Compliance Officer is responsible for developing and implementing all policies and procedures affecting client PHI.
3. The Compliance Officer is responsible for developing and conducting training programs on privacy policies and procedures.
4. The Compliance Officer is responsible for limiting the incidental use of PHI.
5. The name, location and telephone number of the Compliance Officer is to be posted throughout ARA in the event that a client elects to file a complaint. This same information is to be provided with all correspondence pertaining to PHI.
6. The Compliance Officer is responsible for documenting, investigating and responding to all client complaints regarding PHI.
7. The Compliance Officer is responsible for auditing the program sites for compliance with privacy policies.

The ARA HIPAA Compliance Officer may assign any of these responsibilities to other staff members or contractors, but continues to be responsible for making sure these responsibilities are carried out. ARA's HIPAA Compliance Officer is appointed by the Executive Director.

TRAINING

ARA will conduct formal training to all employees on the policies and procedures about PHI. The training must be appropriate for each level of employee to carry out their healthcare function within ARA.

1. In-service education programs are planned to address the degrees of access to confidential healthcare information.
2. All existing staff are trained on the policies and procedures regarding confidential healthcare information. All existing staff shall be trained no later that the implementation date for ARA.
3. All future staff shall be trained during orientation on the policies and procedures about confidential healthcare information.
4. The type, amount, date and employees who received training on the policies and procedures about confidential healthcare information is documented.

STAFF RESPONSIBILITIES

All staff are responsible for preserving the integrity and confidentiality of client health information. Specific staff responsibilities under these privacy policies and procedures will be listed in the staff member's job description.

All staff members must:

- Complete Privacy training
- Use their best efforts to ensure the accuracy, timeliness and completeness of PHI data and ensure that appropriately authorized persons can access the data when needed;
- Implement reasonable safeguards to protect the security and integrity of all PHI, regardless of the medium, in which it exists or through which it is transmitted in accordance with applicable professional ethics;
- Recognize that all clients have a right of privacy and respect such right, consistent with the provision of high quality mental health care and with the efficient administration of the agency.
- Use and disclose PHI only as authorized in their job description or as authorized by a supervisor conduct oral discussions of personal health information with other staff or with clients and family members in a manner that limits the possibility of inadvertent disclosures report suspected violations of a business associate's contractual obligations to safeguard PHI.
- Report suspected violations of a business associate's contractual obligations to safeguard PHI
- Report suspected violations of the policies and procedures established in this manual by staff members.

The policies in this section of the privacy manual establish disciplinary procedures for employees whose actions are not in compliance with ARA's privacy policies and procedures.

Reporting of Suspected Violations of Privacy Policies

All staff members should report possible violations of privacy policies and procedures to their supervisor. If the supervisor determines that a violation occurred, or that the situation warrants further investigation, the possible violation should be reported to ARA HIPAA Compliance Officer. Under the following circumstances, potential violations should not be reported by a staff member to his or her supervisor:

- When the violation involves ARA HIPAA Compliance Officer it should be reported to the ARA Board of Directors.
- When the violation involves a member of the ARA Board of Directors it should be reported to the Secretary of Health and Human Services (HHS).

Reportable offenses include use and disclosure of PHI that may violate:

- the practices described in the Notice of Privacy Practices form
- a client's consent
- a client's authorization

Sanctions and Penalties

There are two types of violations of privacy policies and procedures:

- technical violations that do not result in the use or disclosure of PHI
- violations that do involve the use or disclosure of protected health information

There also are two types of violations that involve use and disclosure:

- unintentional or accidental uses or disclosures
- intentional and deliberate uses and disclosures

The severity of penalties varies based on the type of violation. The most severe penalties apply to the intentional disclosure of PHI in violation of policies and procedures. The least severe penalties apply to unintentional technical violations of policies that do not result in the disclosure of PHI. Examples of violations include:

- *Technical violations*. When obtaining a consent, a staff member fails to notice that the client signed but did not date the consent form.
- *Accidental disclosure*. Information on two clients is accidentally mixed up, and the wrong information is sent to third-party payers.
- *Intentional disclosure*. A staff member provides a drug company representative a list of clients with an identified medical condition without obtaining the client's authorization for this disclosure.

Discipline

It is the policy of ARA to apply discipline to employees failing to comply with the policies and procedures regarding PHI.

Procedure:

1. If an employee is found to violate any policy or procedure in regards to confidential healthcare information, disciplinary action will be implemented.
2. The severity of discipline will be determined according to:
    a. The severity of the violation.
    b. If the violation was intentional or unintentional.
    c. If the violation indicates a pattern or practice of improper use or release of PHI.
3. The degree of discipline may range from a verbal warning to termination.
4. Each episode of employee discipline regarding PHI is to be documented and reported to the Compliance Officer.
5. Documentation is to include:
    a. Name of employee
    b. Degree of violation
    c. Location of violation
    d. Date and time of violation
    e. Disciplinary action provided
6. Refer to ARA's Disciplinary Policy as outlined the Personnel policy for further information.

DISCLOSURE BY WHISTLEBLOWERS (Good Faith Disclosure)

It is ARA's policy to investigate allegations of misconduct by an employee or business associate when PHI is released as evidence of ARA's misconduct.

For the purposes of this policy, it shall not be considered to be a breach of confidentiality if an employee believes in good faith that ARA has engaged in conduct that is unlawful (or which otherwise violates professional or clinical standards), or the care, services, or conditions provided by the agency will potentially end\anger one or more clients, employees or the public and the employee therefore discloses PHI to:

1. A public health authority, health oversight agency or other agency authorized to investigate, or oversee the conduct of the agency;
2. An attorney retained by the employee for the purpose of determining legal options of the employee in regard to the alleged misconduct.

PROCEDURE:

1. The employee or business associate must, in good faith, believe that ARA has engaged in unlawful conduct, has violated professional or clinical standards, or the care, services or conditions provided by ARA potentially endangers one or more clients, employees or the public.
2. The employee releases information to a health oversight agency, a public health authority, an accreditation organization or an attorney retained by the employee or business associate for the purpose of determining the legal options of the employee/business associate with regards to the conduct of ARA.
3. In the event that an employee is a victim of a crime, ARA is not held responsible for the release of confidential healthcare information if the employee notifies a law enforcement official. The information provided by the employee must be:
    a. About the suspected perpetrator of the criminal act.
    b. The information is limited to:
        i. Name and address
        ii. Date and place of birth
        iii. Social Security number
        iv. Blood type and rh factor
        v. Type of decease, injury or condition
        vi. Date and time of treatment
        vii. Date and time of death, if applicable, and
        viii. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars and tattoos

MITIGATION

ARA will mitigate any harmful effects from the misuse of PHI by ARA or any of its' business associates.

PROCEDURE:

1. ARA is notified that confidential healthcare information has been misused by an employee or business associate.
2. ARA shall communicate this information to the Compliance Officer.
3. If the information has been misused by an employee, the policy on employee sanctions is to be implemented.
4. If the information has been misused by a business associate, ARA is to:
    a. Investigate the misuse of the information.
    b. Determine if the misuse was serious.
    c. Determine if the misuse is repeated.
    d. Counsel the business associate on the misuse of confidential healthcare information.
    e. Monitor the business associate's performance to ensure that the wrongful behavior has been remedied.

ARA reserves the right to terminate a business associate agreement in the event the misuse of confidential healthcare information continues despite counseling.

SECURITY SAFEGUARDS

ARA will assure the safe, confidential storage of client data. The following steps are to be used to protect PHI:

1. Clinical records of current clients on any client care area are stored in the office in cabinets which will be located in an area with restricted access.
2. Work stations will be configured so that electronic/computerized records of any current or previous client can only be accessed by those with permission to do so. Permission is granted via the login procedure and utilizing the designated password.
3. Any non-medical record documents containing identifiable client healthcare information are to be shredded prior to disposal. Examples of these documents include notes taken by nurses during change of shift report, notes made during the course of providing client care, and notes made from communication among and between other healthcare providers regarding client care.

TRANSPORTING FILES

Occasionally, a client's file will need to be transported to another site. When this occurs, the file must be placed in a locked briefcase. The employee transporting the file should be careful not to leave the briefcase unattended, unless the briefcase is left in a secure area or locked vehicle.