HIPAA PRIVACY/SECURITY POLICY
BUSINESS ASSOCIATE AGREEMENTS

I. Policies:

A. HIPAA requires ADH to enter into a Business Associate Agreement (AS- 4001) with persons or entities that:

(1) Provide services that involve the use, creation, or disclosure of PHI, and

(2) The services are provided for, or on behalf of, ADH.

B. Such entities are referred to as business associates. A business associate relationship exists when an individual or entity, acting for and/or on behalf of ADH assists in the performance of a function or activity involving the use or disclosure of protected health information. A Business Associate Agreement (BAA) is used along with a contract, agreement, memorandum of understanding or other legal document that defines the services to be provided by the business associate. The Business Associate Agreement defines the business associate's responsibility to protect PHI.

C. Examples of services performed by business associates that involve the use, creation, or disclosure of individually identifiable health information include, but are not limited to, the following:

(1) claims processing or administration,

(2) data analysis,

(3) processing or administration,

(4) utilization review,

(5) quality assurance,

(6) billing,

(7) practice management,

(8) recycling/shredding services.

D. Exceptions

(1) A Business Associate Agreement is not required if the person or entity providing a service to ADH receives PHI in the following instances:

(a) Treatment - A business associate relationship does not exist when ADH discloses protected health information to another health care provider for purposes of treatment.

(b) Financial Transactions - A business associate relationship does not exist between ADH and a financial institution or health care providers if transactions are for the purpose of health care payment.

(c) Disclosures between a group health plan and plan sponsor - A business associate relationship does not exist between a group health plan and plan sponsor.

(d) Organized health care arrangements - Entities that participate in an organized health care arrangement are not business associates of each other.

(e) Entities Acting as Mere Conduits - A business associate relationship does not exist between ADH and an entity acting as mere conduits in the transmission of protected health information (such as the US Postal Service or a courier service).

(f) Incidental access to individually identifiable health information while performing duties that do not typically involve the use or disclosure of such information generally does not constitute a business associate relationship.

E. ADH may only disclose PHI to a business associate or allow a business associate to collect, receive or use protected health information on the ADH's behalf, consistent with the services the business associate has contracted to provide for ADH, upon execution of a Business Associate Agreement (AS-4001) with the business associate.

F. ADH is required to take reasonable steps to correct any known material breach or violation of any Business Associate Agreement. If such steps are unsuccessful, the agreement must be terminated, if feasible; and if not, the problem must be reported to the ADH Privacy Officer/Program Consultant, who will determine if further actions are warranted, which could include reporting the problem and correction attempts to the United States Department of Health and Human Services.

G. ADH employees must inform the ADH Privacy Officer/Program Consultant whenever they become aware of a material breach of a current Business Associate Agreement to which ADH is a party.

H. All Business Associate Agreements must be reviewed and approved by the ADH Privacy Officer/Program Consultant.

I. A copy of each Business Associate Agreement executed by ADH must be provided to the ADH Privacy Officer/Program Consultant for filing.

II. Procedures:

Responsibility	Action
ADH Staff/Contract Administrator	Determines if the contractor will be required to use or have access to ADH PHI. If contractor will use or have access to PHI, completes Business Associate Agreement (AS-4001). If the service contract and BAA are for a new (non-routine) service, contacts the ADH Privacy Officer/Program Consultant for review.
ADH Privacy Officer/Program Consultant	Reviews proposed BAA and service contract with ADH Legal Services to determine if use of BAA is appropriate. When review is complete, sends BAA back to the contract administrator.
ADH Staff/Contract Administrator	If use of BAA is approved, has contractor execute BAA concurrently with the service contract. Provides one copy of BAA to the contractor, retains one copy, and forwards the original BAA to the ADH Privacy Officer/Program Consultant for filing.
ADH Privacy Officer/Program Consultant	Retains BAA for length of service contract or a minimum of six years.

HIPAA PRIVACY/SECURITY POLICY DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI)

Policies:

A. In most cases, PHI may not be disclosed without prior authorization from the client. The client's authorization is recorded on the Authorization to Disclose or Release Health Information (AS-4000).

B. In other cases, as described in the Disclosure Permitted Without Authorization section of this policy, PHI is permitted to be released without the patient's authorization.

C. ADH must track when a client's PHI is disclosed as described in the Right to Accounting of Disclosure of Protected Health Information policy.

D. The Privacy Notice (AS-30a) describes permitted uses and releases of an individual's PHI.

CLIENT AUTHORIZATION

A. Unless otherwise permitted by the HIPAA Privacy Standards, ADH will not use or disclose any protected health information without first obtaining an Authorization to Disclose or Release Health Information (AS-4000) authorizing the release and signed by the individual or the individual's personal representative. An authorization permits, but does not require, the ADH to disclose individually identifiable health information.

(1) Valid Authorization

(a) An original Authorization to Disclose or Release Health Information (AS-4000) is preferred for disclosure of individually identifiable health information. However, a clear and legible photocopy or facsimile is acceptable.

- Requests for disclosure of protected health information (PHI) must be made using the AS-4000.

- Uses and disclosures must be consistent with what the individual has authorized on a signed AS-4000.

- An authorization must be voluntary. ADH may not require the individual to sign an authorization as a condition of providing treatment services, payment for health care services, enrollment in a health plan, or eligibility for health plan benefits, except as noted under Conditioning of Authorization in this policy.

- Each AS-4000 for use or disclosure of an individual's information must be fully completed jointly by the staff member and the individual, whenever possible, with the staff member taking reasonable steps to ensure that the individual understands why the information is to be used or released.

(b) A valid authorization must contain the following information:

- A description of the information to be used or disclosed that identifies the purpose of the information in a specific and meaningful fashion;

- The name or other specific information about the person(s), classification of persons, or entity (i.e., ADH) authorized to make the specific use or disclosure;

- The name or other specific identification of the person(s), classification of persons, or entity to whom ADH may make the requested use or disclosure;

- A description of each purpose of the requested disclosure (the statement, "at the request of the client," is a sufficient description of the purpose when a client initiates the authorization and does not, or elects not to, provide a statement of the purpose);

- An expiration date or event that relates to the client or the purpose of the use or disclosure. The following statements meet the requirements for an expiration date or an expiration event if the appropriate conditions apply:

  - "End of the research study" or similar language is sufficient if the authorization is for use or disclosure of individually identifying health information for research.

  - "None" or similar language is sufficient if the authorization is for the Agency to use or disclose individually identifying health information for the creation and maintenance of a research database or research repository.

- Signature of the client and the date of the signature. If a client's personal representative signs the Authorization to Disclose or Release Health Information (AS-4000), a description of the personal representative's authority to act on behalf of the client must also be provided, including a copy of the legal court document (if any) appointing the personal representative.

(2) Invalid Authorization

(a) An authorization will be considered invalid if the document has any of the following deficiencies:

- The expiration date has passed, or the expiration event is known to have occurred.

- The authorization form is not completely filled out.

- The authorization form does not contain the core elements of a valid authorization.

- The authorization is known to have been revoked.

- Any information recorded on the authorization form is known to be false.

- An authorization for psychotherapy notes is combined with a request for disclosure of information other than psychotherapy notes.

(3) Compound Authorization

(a) An authorization for disclosure of individually identifiable health information will not be combined with any other written legal permission from the client, e.g., consent for treatment, assignment of benefits. However, research studies that include treatment may combine authorizations for the same research study, including consent to participate in the study.

(b) An authorization that specifies a condition for the provision of treatment, payment, enrollment in a health plan or eligibility for benefits may not be combined with any other authorization.

(c) An authorization that is required for enrollment in a health plan or to determine eligibility for benefits of the health plan cannot be combined with a voluntary authorization. A required authorization and a voluntary authorization must be separate documents, signed separately.

(4) Verification of Individuals Requesting Information

(a) If the ADH staff member fulfilling the request does not know the person requesting information, no information may be disclosed without verification of the identity of the person requesting the information.

(b) If the requestor is a provider, the provider must supply his provider identification number and/or telephone number for call back verification.

(c) For all other requestors, reasonable evidence should be supplied in the form of an identification badge, driver's license, written statement of identity on Agency letterhead or similar proof.

(5) Denial of Requests for Information

(a) Unless an individual has signed an authorization, or the information about the individual can be disclosed pursuant to this policy, ADH will deny any request for individual information.

(6) Conditioning of Authorization

(a) The provision of treatment, payment, enrollment in a health plan or eligibility for benefits should not be conditioned on whether or not a client signs a AS-4000, except as follows:

- The provision of research-related treatment can be conditioned on authorization of the use or disclosure of individually identifiable health information for such research; or

- Provision of health care solely for the purpose of creating individually identifiable health information for disclosure to a third party, e.g., physical exam for life insurance; or

- Prior to enrollment in a health plan if authorization is for eligibility or enrollment determinations and the authorization is not for disclosure of psychotherapy notes; or

- An ADH health care provider may condition the provision of research-related treatment on authorization for the use or disclosure of health information for such research; or

- Before enrolling the individual in an ADH health plan, ADH can require the individual to sign an authorization if needed to help determine the applicant's eligibility for enrollment and the authorization is not for a use or disclosure of psychotherapy notes; or

- ADH and its contracted health care providers can require the individual to sign an authorization before providing health care that is solely for the purpose of creating protected health information for disclosure to a third party.

(7) Revocation of Authorization

(a) An individual can revoke an authorization at any time. An Authorization to Disclose or Release Health Information (AS-4000) allows a client to revoke the authorization at any time, except to the extent that the ADH has already taken action based on the authorization. The AS-4000 is to state how the client may revoke an authorization.

(b) Any revocation must be in writing and signed by the individual or his/her personal representative. The Authorization to Disclose or Release Health Information (AS-4000) contains a Revocation Section. This Section must be completed when revocation of the authorization to disclose protected health information is requested. Legible faxed copies of this form are permissible.

(c) Upon receipt of the written revocation, ADH will immediately cease release of protected health information.

(d) No such revocation will apply to information already released while the authorization was valid and in effect.

DISCLOSURE PERMITTED WITHOUT AUTHORIZATION

A. ADH may use or disclose protected health information for its own treatment activities, payment activities, or health care operations.

B. ADH may disclose protected health information for treatment activities of a health care provider.

C. ADH may disclose information without authorization to another covered entity or a health care provider for the payment activities of the entity that receives the information.

D. ADH may disclose information without authorization to another entity covered by federal HIPAA law and rules for the health care operations activities of that entity if:

(1) Both that entity and ADH have or have had a relationship with the individual who is the subject of the information;

(2) The information pertains to such relationship; and

(3) The disclosure is for the purpose of:

(a) Conducting quality assessment and improvement activities, including: outcome evaluation and development of clinical guidelines, provided that obtaining generalized knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; OR

(b) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance; conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers; training of non-health care professionals; accreditation, certification, licensing, or credentialing activities; OR

(c) Detecting health care fraud and abuse or for compliance purposes.

E. Internal communication within ADH is permitted without individual authorization in compliance with policies concerning minimum necessary information.

F. ADH may use or disclose PHI to the extent such use or disclosure is required by law when the use or disclosure complies with the relevant requirements of the law, and the use or disclosure is limited to the relevant requirements of the law.

G. ADH may disclose PHI for Public Health Activities and purposes as follows:

(1) To a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(2) To a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(3) To a person authorized by the Food and Drug Administration (FDA) for activities related to the quality, safety or effectiveness of an FDA-regulated product or activity including:

(a) Collecting and reporting adverse events, product defects or problems, or biological product deviations.

(b) Tracking FDA-regulated products.

(c) Enabling product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback).

(d) Conducting post marketing surveillance.

(4) To a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.

H. ADH may use or disclose information without the written authorization of the individual if it has reasonable cause to believe that an adult is a victim of abuse or neglect, i.e., elder abuse, nursing home abuse, or abuse of the mentally ill/developmentally disabled (for child abuse see the section of this policy for disclosure of PHI for Public Health Activities). ADH may disclose protected information to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse or neglect:

(1) If the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law; OR

(2) If the individual agrees to the disclosure, either orally or in writing; OR

(3) When ADH staff members, in the exercise of professional judgment and in consultation with an appropriate supervisor, believe the disclosure is necessary to prevent serious harm to the individual or other potential victims; OR

(4) When the individual is unable to agree because of incapacity, and a law enforcement agency or other public official authorized to receive the report represents that:

(a) The protected information being sought is not intended to be used against the individual, and

(b) An immediate law enforcement activity would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(5) When ADH makes a disclosure permitted above, it must promptly inform the individual that such a report has been or will be made unless:

(a) ADH staff members, in the exercise of professional judgment and in consultation with an appropriate ADH supervisor, believe informing the individual would place the individual or another individual at risk of serious harm; OR

(b) ADH staff members would be informing a personal representative, and the staff reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing such person would not be in the best interests of the individual, as determined by staff members, in the exercise of their professional judgment and in consultation with an appropriate supervisor.

I. ADH may use or disclose information without the individual's written authorization for the purpose of carrying out duties in its role as a health oversight agency. ADH does not need to obtain an individual's authorization to lawfully receive, use or disclose individual information for oversight activities authorized by law.

J. ADH may disclose information to a health oversight agency to the extent the disclosure is not prohibited by state or federal law for its oversight activities of:

(1) The health care system.

(2) Government benefit programs for which the information is relevant to eligibility.

(3) Entities subject to government regulatory programs for which the information is necessary for determining compliance with program standards.

(4) Entities subject to civil rights laws for which the information is necessary for determining compliance.

(5) Exception: A health oversight activity for which information may be disclosed does not include an investigation or other activity of which the individual is the subject unless the investigation or other activity is directly related to:

(a) The receipt of health care;

(b) A claim to recover public benefits related to health; or

(c) Qualifying for or receiving public benefits or services based on the health of the individual.

(6) If a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity is considered a health oversight activity for purposes of this section.

(7) When ADH is acting as a health oversight agency, ADH may use information for health oversight activities as permitted under this section.

K. ADH may use or disclose information without the written authorization of this individual for law enforcement purposes, unless federal or state law prohibits such disclosure.

(1) ADH may disclose information when reporting certain types of wounds or other physical injuries.

(2) ADH may disclose information in compliance with, and limited to the relevant specific requirements of:

(a) A court order or warrant, summons or subpoena issued by a judicial officer;

(b) A grand jury subpoena; OR

(c) An administrative request, including administrative subpoena or summons, a civil or authorized investigative demand, or similar lawful process, provided that the information is relevant, material, and limited to a legitimate law enforcement inquiry.

Note: All subpoenas, discovery requests, court orders, warrants, summons, judicial or administrative proceedings, etc., that request PHI must be forwarded to and handled by ADH Legal Services.

(3) ADH may disclose limited protected information upon request of a law enforcement official without authorization for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that the information disclosed is limited to:

(a) Name and address;

(b) Date and place of birth;

(c) Social Security number;

(d) ABO 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 beard or mustache, scars, and tattoos. In cases of criminal court commitments, a photograph may be provided.

Exception: ADH may not disclose, for purposes of identification or location, protected health information related to the subject's DNA or DNA analysis, dental records, or typing, samples, or analysis of bodily fluids or tissues, unless ordered to do so by a court or a court approved search warrant.

(4) ADH may disclose protected information upon request to a law enforcement official about an individual who is or is suspected to be the victim of a crime if:

(a) ADH is otherwise authorized by law to disclose that information for purposes of an abuse reporting law or for public health or health oversight purposes; OR

(b) The individual agrees to the disclosure, either orally or in writing; OR

(c) ADH is unable to obtain the individual's agreement due to incapacity or emergency circumstance if:

- The law enforcement official represents that such information is needed to determine whether a violation of law by someone other than the victim has occurred and such information is not intended for use against the victim;

- The law enforcement official represents that immediate law enforcement activity would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; AND

- ADH determines that the disclosure is in the best interests of the individual.

(5) ADH may disclose protected information to a law enforcement official about an individual who has died for the purpose of alerting law enforcement of the death, if ADH suspects that death may have resulted from criminal conduct.

(6) ADH may disclose protected information to a law enforcement official if ADH believes in good faith that the information constitutes evidence of criminal conduct on ADH premises.

(7) ADH may disclose protected information to a law enforcement official if it is necessary for law enforcement authorities to identify or apprehend an individual:

(1) Because of a statement by a person admitting participation in a violent crime that ADH reasonably believes may have caused serious harm to the victim; OR

(2) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

L. ADH may disclose limited information without authorization to a correctional institution or a law enforcement official having lawful custody of an inmate for the purpose of providing health care or ensuring the health and safety of individuals or other inmates.

M. ADH may disclose individual information without authorization for specialized government functions, including:

(1) Disclosure of PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities that federal law authorizes.

(2) Disclosure of PHI of individuals who are Armed Forces personnel (or foreign military personnel) for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the Federal Register the appropriate military command authorities and the purposes for which the protected health information may be used or disclosed.

(3) Disclosure of PHI to authorized federal officials for the provision of protective services to the President, or to foreign heads of state or other persons authorized by law, or for the conduct of investigations authorized by law.

N. ADH may disclose PHI as authorized by, and to the extent necessary to comply with, workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illnesses without regard to fault.

O. ADH may disclose PHI for research without the client's authorization if:

(1) An Institutional Review Board (IRB) or Privacy Board approves a waiver to the requirement for an authorization to disclose PHI for the research project in question, or

(2) The PHI is sought solely for preparation to research, is not removed and is necessary, or

(3) The research is solely on PHI of decedents, or

(4) The request is for de-identified data, or

(5) The request is for a limited data set with a data use agreement.

P. ADH may disclose protected information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties authorized by law.

Q. ADH may disclose individual information without authorization to funeral directors, consistent with applicable law, as needed to carry out their duties regarding the decedent. ADH may also disclose information prior to, and in reasonable anticipation of, the death.

R. ADH may disclose individual information without authorization to organ procurement organizations or other entities engaged in procuring, banking, or transplanting cadaver organs, eyes, or tissue for the purpose of facilitating transplantation.

S. To avert a serious threat to health or safety, ADH may disclose individual information without authorization if:

(1) ADH believes in good faith that the information is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; AND

(2) The report is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

T. In case of an emergency, ADH may disclose individual information without authorization to the extent needed to provide emergency treatment.

DISCLOSURES MADE WITHOUT AUTHORIZATION WHEN THE INDIVIDUAL HAS AN OPPORTUNITY TO AGREE OR OBJECT

A. In limited circumstances, ADH may use or disclose an individual's information without authorization if:

(1) ADH informs the individual in advance and the person has been given an opportunity to object.

(2) Unless otherwise protected by law, ADH orally informs the individual and obtains and documents the individual's oral agreement.

B. Disclosures are limited to disclosure of health information to a family member, other relative, or close personal friend of the individual, or any other person named by the individual.

ROUTINE AND RECURRING DISCLOSURE OF AN INDIVIDUAL'S INFORMATION

A. For the purposes of this policy, "routine and recurring" means the disclosure of records outside ADH, without the authorization of the individual, for a purpose that is compatible with the purpose for which the information was collected. The following identifies several examples of uses and disclosures that ADH has determined to be compatible with the purposes for which information is collected:

1. ADH will not disclose an individual's entire medical record unless the request specifically justifies why the entire medical record is needed.

2. Routine and recurring uses include disclosures required by law. For example, a mandatory child abuse report by an ADH employee would be a routine use.

3. If ADH deems it desirable or necessary, ADH may disclose information as a routine and recurring use to the Department of Justice for the purpose of obtaining its advice and legal services.

4. When federal or state agencies, such as the United States Department of Health and Human Services (DHHS) Office of Civil Rights, the State of Arkansas Medicaid Fraud Unit, or the Arkansas Secretary of State, have the legal authority to require ADH to produce records necessary to carry out audit or oversight of ADH programs or activities, ADH will make such records available as a routine and recurring use.

5. When the appropriate ADH official determines that records are subject to disclosure under the Arkansas Freedom of Information Act, ADH may make the disclosure as a routine and recurring use.

NON-ROUTINE DISCLOSURE OF AN INDIVIDUAL'S INFORMATION

A. For the purpose of this policy, "non-routine disclosure" means the disclosure of records outside ADH that is not for a purpose for which it was collected.

B. ADH will not disclose an individual's entire medical record unless the request specifically justifies why the entire medical record is needed, and applicable laws and policies permit the disclosure of all the information in the medical record to the requestor. Arkansas law and administrative rules prohibit further disclosure of HIV information.

RE-DISCLOSURE OF AN INDIVIDUAL'S INFORMATION

A. Unless prohibited by state and federal laws, information held by ADH and authorized by the individual for disclosure may be subject to re-disclosure and no longer protected by ADH policy. Whether or not the information remains protected depends on whether the recipient is subject to federal or state privacy laws, court protective orders or other lawful process.

HIPAA PRIVACY/SECURITY POLICY GENERAL

Policies:

A. The purpose of this policy is to ensure the privacy/security of medical records, health information, and other types of personal information (herein referenced to as protected health information) in accordance with Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Agency must:

(1) Implement safeguards that ensure the confidentiality, integrity, and availability of the PHI and ePHI (electronic protected health information) collected, maintained, created, or transmitted by ADH.

(2) Protect against reasonably foreseeable threats to the security or integrity of the information (unauthorized access, alteration, deletions, etc.).

(3) Implement and maintain role-based access controls.

This policy applies to any employee (full-time, part-time, contract, extra-help, hourly) in the Arkansas Department of Health (ADH), any volunteers working in the Agency, students, interns, all providers contracted to provide services to the Agency's clients, and Business Associates as defined in the Definitions section of this policy.

B. Pursuant to 45 C.F.R. Sections 164.530(a)(1)(i)and (ii), the ADH Privacy Officer/ Program Consultant is responsible for developing, implementing and maintaining the privacy policies and procedures of the Arkansas Department of Health and is point of contact for an individual to file a complaint and obtain answers to questions concerning ADH's Privacy Notice and privacy policies and procedures.

DEFINITIONS

A. Business Associate: A person/agency that is not a member of the ADH workforce who performs, on behalf of ADH, a function or activity involving the use of PHI.

B. Client: Used interchangeably with patient/individual.

C. Covered Entity: Health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a standard transaction. ADH is a covered entity.

D. Direct Treatment Relationship: Direct treatment relationship is defined as a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

E. Disclosure: The release, transfer, access to or divulging in any other manner of information outside ADH.

F. Health Care: Health care is defined as care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

G. Health Care Provider: A provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care services or supplies in the normal course of business.

H. Health Information: Any information, whether oral or recorded, in any form or medium that:

(1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse,

(2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care; or the past, present, or future payment for the provision of health care to an individual, or

(3) is stored in electronic media and is electronically submitted.

I. Health Plan: An individual plan or group health plan that provides, or pays the cost of, medical care.

J. Indirect Treatment Relationship: Indirect treatment relationship is defined as a treatment relationship where care is provided on the basis of the orders of another health care provider. In such cases, while the services or products (such as a lab test or a diagnostic screening) may involve a relationship with the patient, the diagnostic or other results go to the direct health care provider.

K. Individually Identifiable Health Information: Information that is a subset of health information, including demographic information collected from an individual, and:

(1) is created or received by a health care provider, health plan, employer, or health care clearinghouse, and

(2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, and

(3) identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

L. Operations: Activities that ensure services and benefits provided are appropriate and are high quality, including:

(1) evaluation of treatment and service programs

(2) quality assurance activities

(3) researching health trends

(4) determining what services should be offered

(5) determining new treatments

M. Payment: Coordination of benefits and payments in order to obtain reimbursement for health care services. Payment includes information releases to Medicaid, Medicare, health plans or health insurance carriers, verification of insurance coverage, etc.

N. Personal Representative: A person who has the authority to act on behalf of an individual making decisions related to health care. A parent or guardian is considered the "personal representative" of his/her minor child and has the right to see or authorize release of the child's PHI except when:

(1) The minor controls the use and disclosure of PHI in the following situations:

(a) The minor consented to health care and no other consent is required by law, or

(b) The minor may lawfully obtain such health care without parental consent, or

(c) The parent agreed to a confidential relationship between the child and the health care provider.

(2) ADH believes the child has been or is being abused or neglected and may be harmed by the parent, guardian or personal representative.

(3) An emancipated minor controls the release of his/her own PHI unless he/she is incapacitated and has a personal representative or has appointed a personal representative.

O. Protected Health Information: “Protected health information” (PHI) means individually identifiable information created or received by the Arkansas Department of Health, whether oral or recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; or information that if combined with other data could result in individually identifiable PHI. PHI stored or conveyed in an electronic format is referred to in this document as ePHI.

P. Transaction: The transmission of information between two parties to carry out financial or administrative activities related to health care.

Q. Treatment: Treatment is defined as the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

R. Treatment Provision: Coordination or management of medical services an individual may need, such as:

(1) examinations,

(2) therapy,

(3) nutritional services,

(4) medications,

(5) hospitalization,

(6) determination of appropriate care, or

(7) follow-up care.

S. Use: The term “Use” is used throughout this document in relation to PHI. In this context “Use” is defined as the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

SAFEGUARDS

The Agency must take reasonable steps to safeguard written, oral, or electronic health information (PHI) from any use or disclosure, whether intentional or unintentional, that is not consistent with this policy. Safeguarding PHI includes, but is not limited to, the following steps:

A. General

(1) Ensure that employees' access to PHI is limited to only the information needed to perform their job functions.

(2) Ensure that only the minimum amount of PHI necessary is ever used or disclosed pursuant to this policy.

B. Protecting Printed Information

(1) Route incoming written correspondence through the smallest number of viewers possible.

(2) Keep photocopying of documents containing PHI to a minimum.

(3) Shred or place unneeded copies containing PHI in a security bin.

(4) Place any documents containing PHI with identifying information face down on counters, desks, and other places where patients or visitors might see them. These documents should not be left out on desks or countertops after business hours and should be placed in locked storage bins, locked desk drawers, or other secure areas.

(5) Remove items from fax machines, copiers, and printers promptly.

(6) Process mail in a manner that ensures confidential information is secured.

C. Bulletin Boards

(2) Bulletin boards/white boards should not contain any documents, schedules, lists, lab results, etc., containing PHI.

D. Storage of Paper-Based Data

(1) Store files and documents in locked rooms or storage systems when practical.

(2) After business hours or when not in use by authorized personnel, supervise documents or items containing PHI or keep in a locked desk, locked cabinet or other locked location.

(3) Lock storage of documents containing PHI, whether on-site or off-site, at all times except during use by authorized personnel.

(4) Limit access to filing areas and off-site storage facilities where records or items containing PHI are located to only those employees whose job responsibilities require access to such areas.

(5) Ensure files waiting scanning/destruction are labeled and access is minimal.

E. Outsourcing Shredding

(1) All outsourced shredding contracts must be pursuant to ADH policies.

(2) The outsource shredding company must enter into a Business Associate Agreement (AS-4001) with the ADH before they begin shredding operations for ADH.

F. Physical Security

(1) All persons (patients, visitors, vendors and others) who are not authorized to have access to PHI should be supervised, escorted or observed when visiting or walking through an area where PHI may be easily viewed or accessed.

(2) A system of controlling the distribution of keys should be used. Require all employees to return all keys upon the effective date of termination of their employment with ADH, or when the job responsibilities of the employee no longer require access to the areas or cabinets accessed by the key or keys.

(3) Doors should be locked at night, unless authorized personnel need access to the rooms or areas after hours.

(4) Access to areas containing PHI should be monitored and controlled to the extent possible.

G. Conversations

(1) Do not discuss patient or employee information unless it is needed to perform job duties.

(2) Lower voice if discussing protected health information (PHI) on telephone or in open office area.

(3) Make conversations with a patient, and other conversations in which PHI is being discussed, over the phone or in person, to the extent possible, in a manner or in a location (or both) where persons who are not intended to be a part of the conversation or who are not authorized to receive the PHI cannot easily overhear the conversation.

(4) When having a conversation in a public area with a patient, the patient's family members, or other conversations in which PHI is discussed, conduct the conversation in a lowered voice, to the extent possible, so that unauthorized persons cannot easily overhear the conversation.

(5) Avoid using patients' names or the names of patients' family members in public hallways and elevators when persons who are not authorized to receive the information are present.

H. Sign-In Sheets

(1) Information on patient sign-in sheets should only include the patient's name and appointment date and time. Do not include unnecessary information such as patient complaint, date of birth, or other information that is not necessary for the sign-in sheet.

I. Voice Mail/Answering Machine Messages

(1) When leaving a voice mail or answering machine message for a patient, always limit the amount of information disclosed to the minimum necessary, such as the provider name and telephone number, or other information necessary to confirm an appointment, or to ask the individual to call back. For example, when confirming an appointment, the information should be limited to appointment date and time, and a contact name and telephone number.

(2) Do not leave messages that include laboratory and test results, or any other information that links a patient's name to a particular medical condition or the type of appointment scheduled. (For example, "I am calling to remind Mrs. Brown of her STD examination appointment tomorrow at 10:00," is not an appropriate message.)

J. E-Mail/Fax

(1) Include on all e-mail messages the confidentiality statement contained in the HIPAA Privacy Requirements for E-Mail and Facsimile Services policy.

(2) Encrypt any e-mails which contain PHI.

(3) Use a coversheet when sending PHI via fax.

(4) Remove items from fax machines, copiers, and printers promptly.

K. Safeguarding PHI and other Confidential Information in Electronic Format

(1) Turn computer screens so that PHI cannot be seen, use a privacy screen, or log off.

(2) Provide access to information systems and electronic media containing PHI at ADH only to authorized ADH employees who have a need for specific access in order to accomplish a legitimate task. ADH employees must not attempt to access, duplicate or transmit electronic media containing PHI for which they do not have appropriate authorization.

(3) Encrypt PHI and other confidential information used or sent outside the ADH network.

L. Transporting and/or Accessing ADH Confidential Information Off Campus for Official Business Use

(1) Transport and store PHI and ePHI in a secure manner.

(2) Use briefcase/portable file/manila envelope or other method to cover/ conceal data if transporting files/documents containing PHI.

(3) ADH employees are responsible for maintaining the privacy and security of all PHI that they may be transporting, storing or accessing off-site. This includes, but is not limited to:

(a) Computers or mobile devices that contain or access confidential information.

(c) Storage media such as diskettes, CD-ROMs, DVDs, digital memory cards, and flash drives containing confidential information.

(a) Printed documents that contain confidential information.

MINIMUM NECESSARY RULE

A. Pursuant to federal HIPAA regulations, when using or disclosing PHI or when requesting PHI from another covered entity, the ADH will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. ADH employees are permitted to access PHI only on a need-to-know basis for carrying out their specific job duties.

B. Minimum Necessary Rule does not apply to:
   (1) Disclosures to or requests by a health care provider for treatment purposes;

   (2) Uses or disclosures made to the individual who is the subject of the PHI;

   (3) Uses or disclosures made pursuant to a valid and HIPAA-compliant authorization signed by the patient or patient's legal representative;

   (4) Disclosures made to the United States Department of Health and Human Services, or any officer or employee of that Department to whom the authority involved has been delegated;

   (5) Uses or disclosures required by law; and

   (6) Uses or disclosures required for compliance with other applicable laws and regulations.

C. ADH will only use, disclose, or request an entire medical record when the entire medical record is specifically justified as being reasonably necessary to accomplish the purpose of the use, disclosure, or request.

D. Although ADH is not required to rely on the following requests to be the minimum necessary, ADH workforce may reasonably rely on requests made by:
   (1) Public health and law enforcement agencies to determine the minimum necessary information for certain disclosures; or

   (2) Other covered entities to determine the minimum necessary information for certain disclosures; or

(3) A professional who is a member of the ADH workforce, or is a business associate of ADH for the purpose of providing professional services to ADH, if the professional or business associate represents that the information requested is the minimum necessary for the stated purpose; or

(4) A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board.

HIPAA PRIVACY/SECURITY POLICY HIPAA COMPLAINT

I. Policies:

A. HIPAA requires the ADH to designate a person/office that is the clear point of contact for an individual to file a complaint and obtain answers to questions concerning ADH's Notice of Privacy Practices and Privacy policies.

B. Additionally, pursuant to HIPAA regulations, the ADH must provide a process for individuals to make complaints concerning ADH's policies and procedures required by HIPAA, its compliance with such policies and procedures, or the requirements of HIPAA in general.

C. Notification of possible HIPAA infractions can originate internally or externally. External notification generally originates from a client and can be an informal complaint or a formal complaint. Formal complaints are made either to the ADH using the HIPAA Complaint Form (AS-4005) or to the U.S. Department of Health and Human Service's Office of Civil Rights. Internal notification of issues or incidents generally originate with ADH staff.

D. All possible privacy violations/complaints are reported to the ADH Privacy Officer/ Program Consultant, who works with the complainant, Agency Legal Services, and Center/LHU designee to investigate and resolve the issue. Violations/complaints should be sent to:

ADH Privacy Officer/Program Consultant 4815 West Markham, Slot 31
Little Rock, AR 72205 501-280-2000

E. Individuals may also file a complaint by contacting the U.S. Department of Health and Human Service's Office of Civil Rights. Individuals who file a complaint with the Secretary must file the complaint within 180 days of when the complainant knew or should have known that the act or omission complained of occurred.

II. Procedures:

Responsibility	Action
Client	Issues informal complaint (verbal) or formal complaint using AS-4005 to work unit/LHU.
Work Unit/LHU	Reports possible privacy violation, both internal and external, to their assigned HIPAA Facilitator.

Responsibility	Action
HIPAA Facilitator	Gathers pertinent information and reports incident to ADH Privacy Officer/ Program Consultant.
Work Unit	Reports issues not involving LHU directly to ADH Privacy Officer/Program Consultant and Branch Chief. Note: Do not complete an Occurrence Report (AS-8) at this time.
ADH Privacy Officer/Program Consultant	Determines if issue is HIPAA related.

If **not** HIPAA related, refers to the Center's designee and/or IS Leader (if security related), who follows occurrence reporting procedures. (See Occurrence and Subsequent Loss Reporting policy in this Volume.)

If a HIPAA issue, determines if it is an official complaint or an internal process issue.

If Official Complaint:

- Informs Agency Legal Services of complaint.
- Contacts complainant and obtains statement.
- Contacts Center designee and/or IHS Coordinator and requests statements from all employees involved.
- Contacts IS Leader (if security related).

Center Designee/IHS	Informs Center Team Leader of complaint. Coordinator/IS Leader. Obtains requested statements and sends to ADH Privacy Officer/Program Consultant within one week. Provides ADH Privacy Officer/Program Consultant with additional information as needed.

Responsibility	Action
ADH Privacy Officer/Program Consultant	Compiles statements/information and reviews with Agency Legal Services representative to determine resolution to the complaint. Informs Center designee and/or IHS Coordinator/IS Leader (if security related) and HIPAA Facilitator of resolution and sends letter to complainant. Provides to Agency legal representative and Center designee a copy of the resolution letter. Works with Center designee and/or IHS Coordinator/IS Leader and HIPAA Facilitator to determine training and corrective action required. If it is an official complaint, responds to complainant, in writing, of the status or resolution of the investigation.
Center Designee and/or IHS Coordinator/IS Leader	Determines if disciplinary action is warranted based on personnel policies.
ADH Privacy Officer/Program Consultant	Retains all complaints/resolutions for at least six years.

If Internal Process Issue:

	- Informs Agency Legal Services. - Contacts Center designee and/or IS Leader and requests plan of correction.
Center Designee and/or IHS Coordinator/IS Leader	Creates plan of correction, including appropriate training. Determines if disciplinary action is warranted based on personnel policies.
ADH Privacy Officer/Program Consultant	Retains all Internal Process Issues for at least six years.

HIPAA PRIVACY/SECURITY POLICY
HIPAA PRIVACY REQUIREMENTS FOR E-MAIL AND FACSIMILE SERVICES

Policies:

GENERAL

A. Electronic mail (e-mail), Internet access, and facsimile (FAX) services are made available to ADH staff for the purpose of facilitating the conduct of ADH business and enabling the efficient communication of information and data. These services must be used by ADH staff in a manner that conforms to all applicable state and federal laws, regulations and policies. Each ADH employee is responsible for ensuring the privacy of protected health information (PHI).

E-MAIL

A. Approved Methods of Conveyance: All e-mail messages containing protected health information (PHI) as defined in this policy and sent by ADH staff to destinations within the state's e-mail system must be sent encrypted. Sending e-mail messages containing PHI to destinations outside the state's e-mail system is not secure and is prohibited, unless the e-mail can be encrypted. If the message cannot be encrypted, it may be sent by FAX, employing the privacy safeguards outlined in this policy. Conveyance of large electronic files requires secure media sharing (password protected files on disk or CD) or conveyance by a secure transfer protocol. Consult with the Chief Information Officer (CIO) for assistance.

B. Content Requirements: Any e-mail message generated by ADH staff that contains PHI must conform to the following requirements:

    1. E-mail Subject Line: For messages containing PHI, the subject line must state, in whole or part, "CONTAINS PROTECTED INFORMATION."

    2. E-mail Addresses: E-mail messages may be sent, copied, or forwarded only to those persons who have a need to know the patient information. Global, group, or broadcast addresses should not be used when sending e-mail messages that contain PHI. The purpose of this requirement is to avoid inadvertent disclosure to addressees who lack a need to know the protected information.

3. E-mail Message: At the bottom of the message the following privacy warning must be displayed: “Confidentiality Notice: The information contained in this e-mail message and any attachment is the property of the State of Arkansas and may be protected by state and federal laws governing disclosure of private information. It may contain information that is privileged, confidential, or otherwise protected from disclosure. It is intended solely for the use of the addressee. If you are not the intended recipient, you are hereby notified that reading, copying or distributing this e-mail or the information herein by anyone other than the intended recipient is STRICTLY PROHIBITED. The sender has not waived any applicable privilege by sending the accompanying transmission. If you have received this transmission in error, please notify the sender by reply e-mail immediately, and delete this message and attachments from your system.”

4. Minimum Necessary Content: E-mail messages containing PHI must contain only the minimum necessary information to accomplish the purpose of the communication.

C. Unsecured E-mail Requirements: When originating messages in the state’s unsecured e-mail system (i.e., not Web Access), users are required to review messages and attachments and must expunge all information that may be defined as PHI. Such review is required not only for messages authored by the user, but also for forwarded messages and all the messages in the forwarded strings.

D. User Hard Drives: Hard drives must also be protected from PHI disclosure. Use of Personal Folders (Microsoft Outlook) creates a file on the local hard drive which may be exposed to the Internet through the use of file sharing applications (e.g., Napster, Swapnut, Gnutilla, etc.) and the efforts of malicious hackers. Installation of third party file sharing applications is prohibited. ADH employees must expunge PHI from Personal Folders in their Outlook account.

FAX

A. Approved Methods of Conveyance: All FAX messages containing protected health information (PHI) as defined in this policy and sent by ADH staff to any destination must be safeguarded for confidentiality and privacy in accordance with federal and state law, and must employ privacy safeguards outlined in this policy. FAXes may be sent only to a specific person for whom such release has been determined to be authorized. It should be established, by prior telephone contact, that a specific person is present to receive the transmitted FAX.

B. Content Requirements: FAX messages must use a cover sheet with the word CONFIDENTIAL appearing in bold letters near the top of the form. Further, all such FAXes must include a statement regarding prohibition of disclosure of identifying PHI. The statement should read as follows:

(1) “Prohibition of Redisclosure: This information has been disclosed to you from records that are confidential. You are prohibited from using the information for other than the stated purpose; from disclosing it to any other party without the specific written consent of the person to whom it pertains; and are required to destroy the information after the stated need has been fulfilled, or as otherwise permitted by law. A general authorization for the release of medical or other information is not sufficient for this purpose.”

HIPAA TRAINING REQUIREMENT

Policy:

Since ADH is a covered entity, the entire workforce must complete HIPAA Privacy and Security Training. All employees must review the Privacy/Security Policy in this Volume and sign the Employee Privacy/Security Policy Acknowledgment (AS-38) on their first work day. Note: If a current employee has already signed an Employee Privacy Policy Acknowledgment (No Number) and it is on file, the employee does not have to sign an AS-38.

Each employee's supervisor ensures that the employee signs the AS-38 on his first work day and completes the additional, appropriate training listed below within the first month of employment:

Full-time/Part-time Employees:

HIPAA Web-Based Training
If IHS, also view the Beacon Health Video

Extra-Help Employees:

HIPAA Web-Based Training
Confidentiality Agreement (AS-32)
If IHS, also view the Beacon Health Video

Contract Employees:

Addendum Added to Contract
HIPAA Web-Based Training – Optional – depending on job duties If
IHS, also view the Beacon Health Video

Volunteers/Students:

HIPAA-Web-Based Training – if assignment is > 3 days
Facts ADH Students and Volunteers Should Know about HIPAA (AS-54) – used in place of the HIPAA Web-Based Training when assignment is ≤ 3 days
Confidentiality Agreement (AS-32) **(Must be 18 or older to sign agreement)**
If IHS, also view the Beacon Health Video

HIPAA PRIVACY/SECURITY POLICY INDIVIDUAL RIGHTS

Policies:

A. HIPAA regulations provide specific rights to individuals. These rights are listed on the Privacy Notice (AS-30a) that is provided to all new patients/clients. Specifically, individuals have the right to request to:

(1) Receive a paper copy of the Privacy Notice. The patient may request a paper copy of the Privacy Notice from ADH at any time. (See the Privacy Notice policy in this Volume.)

(2) File complaints regarding violations by ADH of their privacy rights granted to them and created by HIPAA. (See the HIPAA Complaint policy in this Volume.)

(3) Inspect and/or copy their health information. A patient may request to inspect or have a copy of any part of his/her health record. ADH may charge a fee for the costs of copying, mailing, or other supplies associated with this request. (See Right To Inspect and Copy policy in this Volume.)

(4) Amend their health information. If a patient feels that the health information the ADH has created about him/her is incorrect or incomplete, he/she may ask ADH to amend that information. (See the Right to Request Amendment of Protected Health Information policy in this Volume.) The ADH may deny the request if requested to:

(a) amend information that was not created by the ADH;
(b) amend information that is not part of the health information kept by the ADH;
(c) amend information that is not part of the information which the patient would be permitted to inspect or copy; or
(d) amend information that is determined to be accurate and complete.

(5) Request restrictions of their health information. The patient may request ADH to limit the use or disclosure of the patient's health information for treatment, payment, and health care operations or to certain individuals. ADH is not required by law to agree to this request. (See Right to Request Restrictions policy in this Volume.)

(6) Request confidential communication of their health information. The patient may request, in writing, that ADH communicate with him/her in a different way or to a different location, for example, using a different mailing address or calling the patient at a different phone number. (See Right to Request Confidential Communication policy in this volume.)

(7) Obtain an accounting of disclosures of health information. The patient may request an accounting of disclosures of his/her health information. The accounting does not include disclosures for purposes of treatment, payment, health care operations; disclosures required by law for purposes of national security; disclosures to jails or correctional facilities, authorized disclosures, and any disclosures made prior to April 14, 2003. (See Right to Accounting of Disclosure of Protected Health Information policy in this Volume.)

B. All requests must be directed to the Local Health Unit Administrator/IHS Administrator.

C. If there are difficulties in accommodating these requests, the Local Health Unit Administrator/IHS Administrator contacts the ADH Privacy Officer.

D. An individual may revoke an authorization to release his/her information, in writing, and the Agency will no longer release the information.

HIPAA PRIVACY/SECURITY POLICY MARKETING

Policies:

HIPAA MARKETING DEFINITIONS

A. HIPAA defines marketing as:

(1) Communications about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Arrangements between an entity subject to HIPAA regulations ("covered entity") and other entities whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service. Without the client's authorization a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list.

Examples of "marketing" communications requiring prior authorization are:

- A communication from a hospital informing former patients about a cardiac facility, that is not part of the hospital, that can provide a baseline EKG for $39, when the communication is not for the purpose of providing treatment advice.

- A communication from a health insurer promoting a home and casualty insurance product offered by the same company.

It is also considered "marketing" when:

- A health plan sells a list of its members to a company that sells blood glucose monitors, which intends to send the plan's members brochures on the benefits of purchasing and using the monitors.

- A drug manufacturer receives a list of patients from a covered health care provider and provides remuneration, then uses that list to send discount coupons for a new anti-depressant medication directly to the patients.

B. Pursuant to HIPAA, the following types of communications are ***NOT*** considered marketing:

(1) Communications by a covered entity to an individual for the purpose of describing to that individual a health-related product or service that is provided by the covered entity, or included in the covered entity's plan of benefits; or

(2) Communications by a covered entity to an individual as part of the treatment of the individual; or

(3) Communications by a covered entity to an individual in the course of managing or coordinating treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care.

(4) Communications about government and government-sponsored programs do not fall within the definition of "marketing." A covered entity is permitted to use and disclose protected health information to communicate about eligibility for such programs as Medicare, Medicaid, or the State Children's Health Insurance Program (SCHIP).

Examples of communications that are not considered "marketing" are:

- A hospital uses its patient list to announce the arrival of a new specialty group (e.g., orthopedic) or the acquisition of new equipment (e.g., x-ray machine or magnetic resonance image machine) through a general mailing or publication.

- A health plan sends a mailing to subscribers approaching Medicare eligible age with materials describing its Medicare supplemental plan and an application form.

- A pharmacy or other health care provider mails prescription refill reminders to patients, or contracts with a mail house to do so.

- A primary care physician refers an individual to a specialist for a follow-up test or provides free samples of a prescription drug to a patient.

- An endocrinologist shares a patient's medical record with several behavior management programs to determine which program best suits the ongoing needs of the individual patient.

- A hospital social worker shares medical record information with various nursing homes in the course of recommending that the patient be transferred from a hospital bed to a nursing home.

HIPAA MARKETING

A. HIPAA specifically prohibits using or disclosing a client's protected health information (PHI) for marketing purposes, as defined above, unless:

   (1) The client provides written authorization to use his/her PHI for marketing. If there is remuneration for use of the client's PHI, the authorization must state that remuneration is involved;

   (2) The communication occurs in a face-to-face encounter between the covered entity and the individual; or

   (3) The communication involves a promotional gift of nominal value.

B. ADH will not use or disclose a patient's protected health information for marketing purposes except as allowed by federal and state law, including the Federal HIPAA Privacy Regulations.

C. Minimum Necessary: Any and all uses or disclosure of PHI for marketing purposes in compliance with this policy will be limited to the minimum amount of information necessary to achieve the purpose of the use or disclosure.

D. Business Associate Agreement Required: If ADH intends to disclose PHI to a third party for the purpose of the third party communicating with clients about the products or services of ADH, such disclosure does not constitute marketing communications and does not require patient authorization. Prior to such disclosure, ADH is required to enter into a written agreement with the third party restricting the third party's use of the PHI to communications on behalf of ADH and ADH's own products and services. The agreement will be a Business Associate Agreement (AS-4001).

Note: The use of a Business Associate Agreement will not take the place of a patient authorization in situations involving the use or disclosure of PHI to facilitate or conduct communications with patients about the products or services of others. This would include, for example, a situation where a company seeks access to a list of ADH patients or any other PHI which the company will use for its own marketing activities to promote its own products or services, regardless of whether the company is to use the PHI on behalf of ADH as well, and seeks to do so under the guise of a business associate relationship or agreement. This situation requires prior patient authorization.

HIPAA PRIVACY/SECURITY POLICY
MITIGATION AND SANCTIONS OF VIOLATIONS OF PRIVACY RIGHTS

Policies:

MITIGATION

A. As required by HIPAA, the ADH will mitigate any known harmful effect(s) of uses or disclosures of protected health information made by ADH or its business associates in violation of HIPAA or ADH policy related to privacy rights granted by HIPAA.

B. Mitigation means taking all appropriate actions listed below if an ADH client's HIPAA privacy rights have been violated:

(1) Notifying any unintended or unauthorized recipient(s) of protected health information (including by e-mail or fax) and requesting that they disregard, keep confidential, not reveal, and discreetly dispose of said information.

(2) Investigating the causes of the disclosure.

(3) Taking corrective action including:

(a) Sanctions for violation of ADH HIPAA Privacy/Security policies.

(b) Training or retraining as necessary.

(c) Correcting faulty processes.

SANCTIONS

A. The HIPAA privacy rule requires that ADH have and apply appropriate sanctions against members of its workforce who fail to comply with ADH HIPAA Privacy/Security policies.

B. Sanctioning personnel for violation of this policy will be pursuant to ADH policies pertaining to policy violation.

C. Sanctions for violation of ADH HIPAA Privacy/Security policies will not apply to employees who disclose PHI if:

(1) The employee, acting as a "whistleblower," believes in good faith that the ADH has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the services provided by ADH potentially endanger patients, workers, or the public; and

(a) The disclosure is to an agency or authority authorized by law to investigate or oversee the conduct of ADH, or

(b) The disclosure is to an attorney retained by the employee in order to determine the legal options of the employee when disclosing information as described in this section.

(2) The employee files a complaint with the Secretary of DHHS pursuant to the HIPAA Regulations, and the PHI disclosed is a necessary part of that complaint.

DOCUMENTATION

A. All mitigation and sanction actions associated with a violation of ADH HIPAA Privacy/ Security policies will be documented and retained on file by the ADH Privacy Officer/ Program Consultant.

HIPAA PRIVACY/SECURITY POLICY PRIVACY NOTICE

Policies:

GENERAL

ADH is required to provide clients with whom it has a "direct treatment relationship" with a Privacy Notice (AS-30a) that describes how ADH uses and discloses protected health information (PHI), describes ADH's legal duties with respect to PHI, and informs the client of his/her rights pertaining to PHI. HIPAA regulations divide treatment relationships into those that involve direct interactions between providers and patients, and those that involve indirect interactions.

PRIVACY NOTICE

The Agency is required to provide the Privacy Notice (AS-30a) to all clients, except for WIC Program Only clients, during their first visit to the clinic.

(1) In emergency situations, the provision of the Privacy Notice and its written Acknowledgment of Receipt (AS-30b) may be given as soon as reasonably practicable after the emergency treatment situation.

(2) A copy of the AS-30a must be given to the client any time it is requested.

(3) If the AS-30a is revised, the revisions must be made available to the patient during his/her next visit if requested.

(4) Reasonable measures, such as translation or reading of the AS-30a, must be provided if requested.

(5) The ADH must make the Privacy Notice available to anyone who asks for a copy. If the person requesting the Privacy Notice is not a patient or client, then an AS-30b is not needed.

(6) In each ADH location that provides service to individuals, the ADH must post the Privacy Notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the ADH to be able to read the Privacy Notice.

PRIVACY NOTICE ACKNOWLEDGMENT

ADH employees providing a copy of the Privacy Notice to clients must request the client to sign an Acknowledgment of Receipt (AS-30b). The AS-30b indicates that the Privacy Notice was given to the client.

(1) If the patient refuses to sign the AS-30b, note such in the "For Official Use Only" section of the AS-30b by signing and dating the form.

(2) If the Privacy Notice is revised and the patient requests a copy of the revised Privacy Notice, then another AS-30b must be obtained from the client.

(3) Exception: For Immunization Only patients, stamp the HIPAA Privacy Notice Acknowledgment statement on the IMM-1, Comments section, and obtain the signature on the IMM-1, instead of the AS-30b.

DOCUMENTATION REQUIREMENTS

A. A copy of the AS-30a and each subsequent revision will be retained for six years by the ADH HIPAA Office.

B. A copy of the AS-30b will be retained by each LHU issuing the AS-30a for six years.

HIPAA PRIVACY/SECURITY POLICY
RIGHT TO ACCOUNTING OF DISCLOSURE OF PROTECTED HEALTH INFORMATION

I. Policies:

1. ACCOUNTING OF DISCLOSURE OF PROTECTED HEALTH INFORMATION

A. ADH clients (and their legal representatives) have a right to request an accounting of PHI disclosures that ADH has made for a period of up to six years previous to the date of request. It is ADH policy that all disclosures of client PHI (subject to accounting and tracking) will be recorded on the Accounting Of Disclosures Of Protected Health Information (AS-31).

B. Upon receipt of a request for an accounting of PHI disclosures, ADH will have a maximum of 60 calendar days to compile the accounting of disclosures and respond to the client request. If ADH is unable to comply with the client's request for an accounting of PHI disclosures within 60 calendar days, ADH may make a one-time extension of the timeframe for response by 30 calendar days.

C. The accounting of PHI disclosures must include:

(1) The date of the disclosure.

(2) The name and address, if known, of the person or entity that received the disclosed PHI.

(3) A brief description of the information disclosed.

(4) A brief statement of the purpose of the disclosure that reasonably informs the client of the basis for the disclosure, or, in lieu of such statement, a copy of the client's written request for the accounting of disclosures.

2. DISCLOSURES SUBJECT TO TRACKING AND ACCOUNTING

A. Disclosures subject to tracking and accounting include, but are not limited to, the following:

(1) Abuse Reports. PHI provided pursuant to mandatory abuse reporting laws to an entity authorized by law to receive abuse reports.

(2) Audit Review. PHI provided from a client record in relation to an audit or review of a provider or contractor or disclosures to insurers for claims investigations.

(3) Health and Safety. PHI provided to avert a serious threat to the health and/or safety of a person or persons.

(4) Licensee/Provider. PHI provided from a client record in relation to licensing, regulation or certification of a provider or licensee involved with the provision of care or services to the client.

(5) Legal Proceedings. PHI ordered to be disclosed pursuant to a court order.

(6) Law Enforcement Official/Court Order. PHI provided to a law enforcement official pursuant to a court order.

(7) Law Enforcement or Other Official/Deceased. PHI concerning a deceased client provided to law enforcement official, medical examiner or other official for the purpose of identifying a deceased person, determining the cause of death, or for other reasons authorized by law.

(8) Law Enforcement Official/W arrant. To the extent permitted by law, PHI provided to a law enforcement official concerning a fleeing felon or client subject to an arrest warrant.

(9) Public Health Authority. PHI provided to public health authorities for the reporting of disease or injury or for the conduct of a public health study or investigation.

(10) Public Record. PHI disclosed pursuant to a Public Record request without the client's authorization.

(11) Research. PHI provided for research purposes using a waiver of authorization provided by an Institutional Review Board (IRB).

(12) Required by Law. Disclosures that result from a requirement from another federal or state law or regulation.

(13) Government Entity. Disclosures to any government entity or health oversight agency, unless otherwise exempted.

3. DISCLOSURES NOT SUBJECT TO TRACKING AND ACCOUNTING

A. Disclosures not subject to tracking and accounting include:

(1) Disclosures for Treatment, Payment and Operations (TPO).

(a) Treatment – 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.

(b) Payment – activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations and utilization review.

(c) Operations – 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.

(2) Disclosures to the client.

(3) Disclosures made pursuant to a valid authorization of the client.

(4) Disclosures or uses made subject to the client's opportunity to object, including:

(a) Use to maintain a facility directory and disclosures from the directory to clergy and persons who ask for the individual by name.

(b) Use and disclosure to persons involved with the client's care, payment for services, or for notification of general condition or death to persons responsible for the care of the client.

(c) Disclosures for disaster relief purposes.

(5) Use and disclosures for national security and intelligence activities.

(6) Use and disclosures to correctional institutions and other law enforcement custodial situations.

(7) Disclosure as part of a limited data set, which excludes direct identifiers for research, public health, or health care operations.

(8) Disclosures which occurred prior to the effective date of HIPAA Privacy requirements.

(9) Incidental disclosures.

(10) Use of PHI within ADH.

4. REQUESTS FOR ACCOUNTING OF PHI DISCLOSURES

A. Clients (or their legal representatives) may make their requests by completing a Request for an Accounting of Disclosures of Protected Health Information (AS-33). A request for an accounting of PHI disclosures must identify the record holder and the period of time covered by the request. When a request for an accounting is received:

(1) The ADH staff member receiving the request for an accounting must document the identity of the requestor by identification badge, driver's license, written statement of identity on Agency letterhead, or similar proof. When an oral request is received in person or by phone, ADH will confirm the request with a written statement describing the request and obtain a client signature for authentication.

(2) When the request for accounting is documented and accepted, the client will be provided an acknowledgement statement indicating when he/she can expect to receive an accounting. An Acknowledgement of Request for Accounting of Disclosure or Amendment to PHI (AS-4009) will be used.

(3) The client's health record will be reviewed to determine if PHI disclosures have occurred during the time period covered by the client's request. This will be accomplished through manual review of the Accounting of Disclosures of Protected Health Information (AS-31). If accounting of disclosures cannot be completed within 60 days of the request, the client will be notified using an Accounting of Disclosures Response Letter (AS-34).

(4) When a list of disclosures has been compiled, the AS-34 will be completed and a copy of the client's AS-31 will be forwarded to the client.

(5) Client requests for accountings of PHI disclosures will be filed in the client's health record and maintained for a period of six years from the date the request is completed.

(6) The accounting must be documented on the Accounting of Disclosures of Protected Health Information (AS-31). Individuals may request an accounting for up to six years prior to the date on which the accounting is requested. The earliest possible beginning date is April 14, 2003.

(7) The Agency provides the first accounting in any 12 month period without charge. ADH may charge for additional copies.

(8) If the client has any questions concerning the content of the accounting, he/she will be referred to the ADH Privacy Officer/Program Consultant at:

Arkansas Department of Health
ADH Privacy Officer/Program Consultant 4815 W. Markham Street, Slot 31
Little Rock, Arkansas 72205-3867 Phone - 501-661-2000

5. SUSPENSION OF ACCOUNTING OF PHI DISCLOSURES

The Agency must temporarily suspend an individual's right to receive an accounting provided to a health oversight agency or law enforcement official if provided a written statement indicating the accounting would likely impede the Agency's activities. The statement must specify the timeframe the suspension is required. If the agency or official requests a suspension orally, ADH must document the statement, including the identity of the agency or official making the statement, temporarily suspend the client's right to an accounting of disclosures subject to the statement and limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

II. Procedures:

Responsibility	Action
Client	Completes a Request for an Accounting of Disclosures of Protected Health Information (AS-33). Retains AS-33 in client's file.
LHU Administrator/IHS Administrator/Designee	Documents the identity of the requestor by identification badge, driver's license, written statement of identity on Agency letterhead, or similar proof. Notifies the client of receipt of the request using the Acknowledgement of Request for Disclosure or Amendment to PHI (AS-4009). Retains a copy of the AS-4009 in the client's file. Notifies the ADH Privacy Officer/Program Consultant immediately after the request for accounting has been verified.

Responsibility	Action
LHU Administrator/IHS Administrator/Designee	Determines if access is granted based on timeframe and/or disclosure exceptions.

Note: Individuals may request an accounting for up to six years. (The earliest possible beginning date is April 14, 2003.)

If request is granted:

Within 60 days of receipt of the request, sends client an Accounting of Disclosures Response Letter (AS-34) and attaches a copy of the Accounting of Disclosures of Protected Health Information (AS-31) and any blanket disclosure statements. Provides a copy of both to the ADH Privacy Officer/Program Consultant.

If request cannot be granted within 60 days from date of client's request, notifies client prior to 60 day limit
using AS-34. Provides a copy to the ADH Privacy Officer/Program Consultant.

If request is denied:

Determines access is denied, completes Accounting of Disclosures Response Letter (AS-34), sends a copy to individual
making request within 60 days of the request, and sends a copy to the ADH Privacy Officer/Program Consultant.

If request is suspended:

Notifies client that his/her request has been suspended by sending the client an Accounting of Disclosures Response Letter (AS-34) and sends a copy to the ADH Privacy Officer/Program Consultant.

Note: In all cases, a copy of the AS-34 is retained in the client's file.

HIPAA PRIVACY/SECURITY POLICY RIGHT TO INSPECT AND COPY

I. Policies:

A. Individuals have the right to inspect and obtain a copy of their health information. This request may include medical, billing, or health care payment information, but does not include information that is needed for civil, criminal, or administrative actions or proceedings or psychotherapy notes. The Agency may charge a fee for the costs associated with an individual's request.

B. All requests for clients to inspect or obtain a copy of their health information must be in writing, preferably using the Authorization to Disclose or Release Health Information (AS-4000).

C. ADH must provide access or deny the request no later than 30 days following the receipt of a request when the PHI is maintained or accessible on-site. Within 30 days of a request, individuals must have appointments scheduled to access their PHI, copies of PHI given or mailed to them, or be sent a denial notice disallowing access.

D. If the PHI is not accessible on-site, the covered entity must provide access or deny access no later than 60 days from receipt of such a request.

E. ADH may delay the response to the request for access only once by 30 days as long as a written statement of the reasons for the delay and the date the covered entity will take action on the request is provided to the individual within the above deadlines. This makes the maximum time to respond to be 60 days to provide access or deny a request for on-site PHI and 90 days for off-site PHI.

F. ADH may deny an individual's request to inspect and obtain a copy of his/her protected health information (PHI) for the following reason(s):

(1) ADH does not possess the information requested. If ADH knows where the information resides, it must inform the client.

(2) Requested information was/is being compiled in anticipation of, or for use in, a civil, criminal or administrative action or proceeding

(3) Requested information is subject to or exempted by the Clinical Laboratory Improvements Amendments (CLIA) of 1988.

(4) Requested information was obtained from someone other than a healthcare provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(5) Requested information was/is being created or obtained in the course of ongoing research that includes treatment and the client agreed to the denial of access when he/she consented to participate in the research. (The client's right of access will be reinstated upon completion of the research.)

(6) ADH may choose not to release Psychotherapy notes (as defined by HIPAA).

(7) The requested information is contained in records subject to the federal Privacy Act, 5 U.S.C. §552a, and this denial meets the requirements of that law. (The Privacy Act of 1974 protects personal information about individuals held by the federal government.)

(8) A licensed healthcare professional has determined in his/her professional judgment that access to the requested information is reasonably likely to endanger the individual's or another's life or physical safety.

(9) The requested information makes reference to another person and a licensed healthcare professional has determined, in the exercise of reasonable judgment, that the requested access is reasonably likely to cause substantial harm to such other person.

(10) If the requestor is the personal representative of the subject of the requested information, and a licensed healthcare professional has determined, in the exercise of professional judgment, that the requested information should not be provided to the personal representative.

G. If access to requested information has been denied under items F.8, F.9, or F.10 listed in this policy, the client has the right to a review of the denial by ADH's Patient Care Team members who did not participate in this denial by submitting a written request to the ADH Privacy Officer/Program Consultant.

II. Procedures:

Responsibility	Action
Client	Submits written request or completes an Authorization to Disclose or Release Health Information (AS-4000) to inspect/ obtain a copy of his/her protected health information and provides to the LHU.
Local Health Unit Administrator/ In-Home Services Administrator/ Designee	Consults with PHN/HHN (Home Health Nurse) (if LHU Administrator is not a PHN/HHN) to determine if access is granted or denied. (See Copy/Inspect Denial Letter (AS-35) to make determination.)

Responsibility	Action
Local Health Unit Administrator/ In-Home Services Administrator/ Designee	**If request is granted:** Provides a copy to the individual PHN/HHN to determine if access is within 30 days of receipt of the request in the requested format, if possible; if not, in a readable hard copy form.

Note: The time limit may be extended an additional 30 days if the date by which the copies will be sent and a written statement of the reason for the delay is sent to the individual within the first 30 days.

Arranges a convenient time and place for individual to inspect or obtain copy, or mails the copy at the individual's request. Charges for copying according to the Record
Maintenance Fee, Record Duplication, in the Funds Control Section of the Financial Management Volume. Note: If individual inspects record, it must be
in the presence of the Local Health Unit Administrator/IHS Administrator/ designee.

If request is denied:
Completes Copy/Inspect Denial Letter (AS-35) and sends a copy to individual within 30 days of request. Note: If denial is for certain reasons (see
AS-35 for explanation), individual can request in writing for decision to be reviewed by Patient Care Managers/IHS Coordinators who did not participate
in the original decision to deny access. ADH must provide or deny access based on this determination.

If review is requested:
Contacts ADH Privacy Officer/Program Consultant, who contacts Patient Care Manager/IHS Coordinators for review of "reviewable" PHI to determine if PHI can be released.

Responsibility	Action
ADH Patient Care Manager/IHS Coordinators/ADH Privacy Officer/ Program Consultant	Members who did not participate in the original decision review request and determine if PHI can be released.

Notifies Local Health Unit Administrator/ IHS Administrator of decision. If denied, sends letter to requesting individual and a copy to the Local Health Unit Administrator/ IHS Administrator. Note: Other information is made accessible to the individual after excluding the PHI that was denied access.

HIPAA PRIVACY/SECURITY POLICY
RIGHT TO REQUEST AMENDMENT OF PROTECTED HEALTH INFORMATION

I. Policies:

A. An individual has the right to request an amendment to his/her health information if he/she feels the information is incorrect or incomplete. ADH will review the request and grant or refuse the request. Requests for amendment of protected health information must be made in writing to the LHU Administrator of the Local Health Unit where the client's medical records reside and must clearly identify the information to be amended and the reasons for the amendment.

(1) Request is Granted. If the individual responsible for the entry to be amended grants the request after review and approval, ADH must:

(a) Insert the amendment or provide a link to the amendment at the site of the information that is the subject of the request for amendment.

(b) Inform the individual that the amendment is accepted.

(c) Obtain the individual's identification of and agreement to have ADH notify the relevant persons with whom the amendment needs to be shared.

(d) Within a reasonable timeframe, make reasonable efforts to provide the amendment to persons identified by the individual, and persons, including business associates, that ADH knows have the protected health information that is the subject of the amendment and that may have relied on or could foreseeably rely on the information to the detriment of the individual.

(2) Request is Denied. Requests may be denied if the material requested to be amended:

(a) Was not made by ADH, unless the originator is no longer available to act on the request.

(b) Is not part of the individual's health record.

(c) Is not accessible to the individual because federal and state laws do not permit it (see reasons for denial of request to inspect or copy listed on AS-35).

(d) Is accurate and complete.

B. ADH must act on the individual's request for amendment no later than 60 days after receipt of the amendment. ADH may have a one-time extension of 30 days for processing the amendment if the individual is given a written statement of the reason for the delay and the date by which the amendment request will be processed.

C. If the request is denied, ADH must provide the individual with a timely written denial by issuing a Denial of Amendment Request (AS-36). The AS-36 must be written in plain language and must contain the following:

(a) The basis for the denial.

(b) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement.

(c) A statement that if the individual does not submit a statement of disagreement, the individual may request that ADH provide the individual's request for amendment and the denial with any future disclosures of the protected health information that was the subject of the request.

(d) A description of how the individual may complain to ADH or the Secretary of Health and Human Services.

(e) The name or title and the telephone number of the designated contact person who handles complaints for ADH.

D. ADH must permit the individual to submit to ADH a written statement disagreeing with the denial of all or part of the requested amendment and the basis of such agreement. ADH may reasonably limit the length of a statement of disagreement.

E. ADH may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, ADH must provide a copy to the individual who submitted the statement of disagreement.

F. ADH must, as appropriate, identify the record of protected health information that is the subject of the disputed amendment and append or otherwise link the individual's request for amendment, ADH denial of the request, the individual's state of disagreement, if any, and ADH's rebuttal, if any.

G. If the individual has submitted the statement of disagreement, ADH must include the material appended or an accurate summary of such information with any subsequent disclosure of the protected health information to which the disagreement relates.

H. If the individual has not submitted a written statement of disagreement, ADH must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of protected health information only if the individual has requested such action.

I. When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included, ADH must separately transmit the material required.

J. A covered entity that is informed by ADH of an amendment to an individual's protected health information must amend the protected health information in written or electronic form.

K. ADH must document the titles for the persons or offices responsible for receiving and processing requests for amendments.

L. Amendments received from other covered entities:

(1) When a provider receives notification from another health care provider or health plan that a patient's protected health information has been amended, the receiving provider must:

(a) Ensure that the amendment is appended to the patient's health record.

(b) Inform its business associates that may use or rely on the patient's protected health information of the amendment (as agreed to in the business associate contract), so that they may make the necessary revisions based on the amendment.

II. Procedures:

Responsibility	Action
Individual	Provides a written request to amend his/her protected health information to the Local Health Unit. Notes: 1. The request must provide a reason to support the amendment. 2. The Agency must act on the request no later than 60 days after receipt of the request.

LHU Administrator/IHS Administrator/Designee Program Consultant.	Reviews record and sends request and copy of information to ADH Privacy Officer/
ADH Privacy Officer/Program Consultant	Informs the ADH Privacy/Security Officer and contacts Patient Care Horizontal Team/IHS Coordinators for determination of amendment.
ADH Patient Care Horizontal Team/ IHS Coordinators	Determines if amendment is accepted or denied.

If request for amendment is accepted:

Notifies the LHU Administrator/IHS Administrator, ADH Privacy Officer/Program Consultant, and ADH Privacy/Security Officer of determination.

LHU Administrator/IHS Administrator/Designee	In consultation with PHN/HHN, ensures individual's medical record is appropriately amended. Informs the individual that his/her record has been amended. Informs relevant persons that the individual's record has been amended if requested by the individual.

Notes:

1. Relevant persons include:

   - Persons identified by the individual as having received incorrect health information.
   - Business associates that have incorrect health information and may have relied on the information to the detriment of the individual.

2. If informed by another covered entity of an amendment to health information, amend the medical record following these procedures.

Responsibility	Action
LHU Administrator/IHS Administrator/Designee	**If request for amendment is denied:** Completes and provides to the individual the Denial of Amendment Request (AS-36). Permits the individual to submit a statement of disagreement with the AS-36. Notifies ADH Privacy Officer/Program Consultant of statement of disagreement.
ADH Privacy Officer/Program Consultant	Works with ADH Privacy/Security Officer and LHU Administrator/IHS Administrator to prepare rebuttal statement with advice from Legal Services to the individual's statement of disagreement.
LHU Administrator/IHS Administrator	Places a copy of the rebuttal statement in the client's medical file and provides a copy to the client.

HIPAA PRIVACY/SECURITY POLICY
RIGHT TO REQUEST CONFIDENTIAL COMMUNICATION

Policies:

A. Individuals have the right to request that the Agency communicate with them about health care matters in a certain way or at a certain location, but must specify how or where they want to be contacted.

B. ADH must permit clients to request and must accommodate reasonable requests by clients to receive communications of protected health information (PHI) from ADH by alternate means or at alternate locations. Examples of such requests may include, but are not limited to, mailing PHI to an alternate address specified by the individual, transmission of such information to a specific phone number by facsimile, transmission of such information via e-mail or a request that the Agency only contact the individual at work.

C. The Department is not required to accommodate unreasonable requests for alternate delivery of PHI. Examples of such requests may include asking for delivery of PHI by registered or certified mail or requesting that PHI be hand carried to the client to an off-site location.

D. The client must request in writing to receive PHI from ADH by alternate means or to an alternate location and must specify the preferred alternate means or location.

E. Documented client requests for alternate means of delivery or alternate locations for delivery of PHI will be filed in the client's record and appropriate updates will be made to the client's record.

F. Prior to sending any PHI to a client, ADH staff will review the client's record to confirm whether the client has requested that PHI be sent by alternate means or to an alternate location.

G. ADH will forward PHI to the client in accord with the client's preferred means or location when requested or to his/her current mailing address, as appropriate.

H. ADH may terminate its agreement to deliver PHI via alternate means or to an alternate location if:

(1) The client agrees to or requests termination of the alternate delivery location or method of communication in writing. ADH staff must document the request in the client's record.

(2) Use of the alternate delivery location or method of communication is not effective (i.e., ADH is unable to contact the client at the location or in the manner requested by the client). In this instance, ADH must inform the client that it is terminating its agreement to alternate means or location of delivery of PHI and provide the reason(s) for termination of the agreement.

I. ADH must retain all documentation related to requests for alternative means of delivery of PHI or alternate delivery location for PHI for a minimum period of six years.

J. When the client terminates the request for alternate delivery of PHI or it is determined that the alternate method of delivery is unreliable (i.e., mail has been returned, FAX machine number has been disconnected or has no FAX to receive messages, etc.), the ADH will notify:

(1) The client of the termination of alternate delivery of PHI

(2) The ADH Privacy Officer/Program Consultant

HIPAA PRIVACY/SECURITY POLICY RIGHT TO REQUEST RESTRICTIONS

I. Policies**:**

A. HIPAA requires ADH to permit an individual to request that ADH restrict health care information the Agency uses or releases for treatment, payment, operations, or disclosures permitted to family members, other relatives or close personal friends of the individual for involvement in the individual's care and notification purposes.

For example, a patient could request that his or her records not be shared with a particular physician because the physician is a family friend, or an individual could be seeking a second opinion and might not want his or her treating physician to be consulted.

B. HIPAA does not require ADH to agree or comply with the requested restriction or limitation. However, if ADH does agree to a restriction, it may not use or disclose PHI in violation of such restriction.

II. Procedures:

Responsibility	Action
Individual	Provides a written request for a restriction to the Local Health Unit.
Local Health Unit	Consults with PHN/HHN (if Local Health Administrator/IHS Unit Administrator is not a PHN/HHN) to Administrator/ designee to determine if restriction is granted/denied.

Note: ADH must permit an individual to request restrictions on use/disclosure for treatment, payment, health care operations, involvement in individual's care, and notification purposes. ***ADH is not required to agree to a restriction.***

If restriction is denied:

LHU Administrator/IHS Administrator/Designee	Documents request and denial in individual's chart.

Responsibility	Action
If restriction is granted:	
LHU Administrator/IHS Administrator/Designee	Documents restriction in individual's chart. Note: ADH may not use or disclose protected health information in violation of the restriction unless for emergency treatment. Then, ADH must request that emergency providers do not use or disclose further. Restrictions are not effective to prevent uses or disclosures when: - required by law, - for public health activities, - about victims of abuse, neglect, or domestic violence, - for health oversight activities, - for judicial and administrative proceedings, - for law enforcement purposes, - about decedents, - for cadaveric organ, eye or tissue donation purposes, - for research purposes, - to avert a serious threat to health or safety, - for specialized government functions, and - for workers' compensation.
Termination of a restriction:	
Individual	Agrees to or requests termination of restriction in writing.
LHU Administrator/IHS Administrator/Designee	Informs individual that the restriction will not apply to future protected health information created or received.