Alabama Department of Senior Services

HIPAA PRIVACY POLICY
(Effective April 13, 2003)

Overview

"HIPAA" stands for the Health Insurance Portability and Accountability Act (Public Law 104-191), a federal law passed in 1996 to reform health insurance in the United States. Although HIPAA is long and complex, the "Administrative Simplification" portion of the act is of most relevance to states. Administrative Simplification consists of the following seven distinct components: national standards for electronic transactions and code sets; national standard identifiers for employers, health plans, and providers (individual identifiers on hold indefinitely); claims attachments; first report of injury; client privacy; security standards; and enforcement provisions. The privacy rule requires covered health entities to obtain a client's consent or authorization before using or disclosing any personal health information.

The HIPAA Privacy Rule—finalized as federal regulations (45 C.F.R. Parts 160 and 164) on August 14, 2002—ensures that personal medical information shared with doctors, hospitals, and others who provide and pay for healthcare is protected. It is the first ever comprehensive federal protection guideline for the privacy of health information.

Basically, the HIPAA Privacy Rule does the following:

- Imposes new restrictions on the use and disclosure of personal health information,
- Gives clients greater access to their medical records, and
- Gives clients greater protection of the medical records.

I. WHO IS COVERED BY THE HIPAA PRIVACY RULE?

A. Covered entities include:

1. Health plans, which are individual or group plans (or programs) that provide health benefits directly, through insurance, or otherwise.
2. Health care providers, which are providers (or suppliers) of medical or other health services or any other person furnishing health care services or supplies, and who also conduct certain health-related administrative or financial transactions electronically; and
3. Health information clearinghouses, which are any public or private entities that process or facilitate processing of nonstandard health information into standard data elements.

B. The HIPAA Privacy Rule also holds covered entitles liable for the rule violations of their business associates. A "business associate" is a person or entity who:

1. Works on behalf of a covered entity to perform or assist in performing a function or activity that involves "the use or disclosure of individually identifiable health information"; or

2. Performs another regulated function for the covered entity; or

3. Performs a service, such as legal, accounting, or financial services, for a covered entity "where the provision of the service involves the disclosure of individually identifiable health information."

C. The HIPAA Privacy Rule requires "covered entities," such as ADSS/AAA'S, to:

1. Guarantee client privacy rights by:

a. Giving clients clear, written explanations of how the agency may use and disclose their health information;

b. Ensuring clients can see and get copies of their records, and can request amendments;

c. Making a history of non-routine disclosures accessible to clients;

d. Obtaining client consent before sharing their information for treatment, payment, and healthcare operations (TPO);

e. Obtaining client authorization for non-routine disclosures and most non-healthcare purposes; and,

f. Allowing clients to request restrictions on the uses and disclosures of their information.

2. Adopt written privacy procedures, to include:

a. Who has access to protected information,

b. How it will be used within ADSS/AAA'S, and

c. When the information may be disclosed.

3. Ensure that business associates of ADSS/AAA'S protect the privacy of health information.

4. Train ADSS/AAA'S employees in the agency's privacy procedures.

5. Designate a ADSS/AAA'S privacy officer responsible for ensuring that privacy procedures are followed.

II. WHY ADSS/AAA'S ARE COVERED BY HIPAA?

A. As stated above, a covered entity under HIPAA includes health care providers. The term "health care provider" includes not only those entities which provide certain direct health care services (such as doctors and nurses) but also "any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." 45 C.F.R. 160.103.

B. ADSS/AAA'S both bills and is reimbursed for Medicaid services. ADSS/AAA'S receives millions of dollars in Medicaid reimbursement annually. HIPAA would allow hybrid agencies with both covered and non-covered operations, such as ADSS/AAA'S, to place a "firewall" around those covered health-related activities and apply the HIPAA requirements only to those program efforts. However, the creation of a "firewall" would prevent the necessary sharing of health information

with other divisions within ADSS/AAA'S. Since divisions must be able to share necessary client health information, ADSS/AAA'S is required by HIPAA to establish a department-wide privacy practice policy to implement HIPAA.

C. DIRECT v. INDIRECT TREATMENT PROVIDERS

HIPAA requirements differ depending on whether a person or entity is a direct or indirect treatment provider. "*Indirect treatment relationship*" means that the health care provider, *i.e.*, ADSS/AAA'S, delivers "health care" based upon the orders of another health care provider (such as a doctor) and typically provides services or reports results to that provider who then reports to the client. Anything else is considered a "*direct treatment relationship.*" "*Health care*" is defined as the services related to the health of the individual, including diagnostic, therapeutic, counseling, and assessment services.

1. A direct treatment provider must
   a. Adopt written privacy policies to protect client privacy.
   b. Train staff.
   c. Designate a privacy officer.
   d. Ensure that business associates protect client privacy.
   e. Provide a copy of the privacy notice to each client no later than the date of first service delivery after April 13, 2003.
   f. Make a good faith effort to obtain a written acknowledgement from each client of the receipt of the privacy note described in ¶ 5 above, except in emergency situations.
   g. Have copies of the privacy notice available at offices for clients.
   h. Post the notice in a prominent location in offices.

D. Indirect treatment providers need only perform ¶¶ a through d above.

III. WHAT IS PROTECTED HEALTH INFORMATION?

A. When a client gives personal health information to a covered entity, such as ADSS/AAA'S, that information becomes Protected Health Information—or "PHI." It includes:

1. Any personal health information that contains information that connects the client to the information.

2. Examples of information that might connect personal health information to the client include:
   a. The individual's name or address
   b. Social Security or other identification numbers

c. Physician's personal notes

d. Billing Information

IV. WHAT ARE THE RULES FOR THE USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION?

A. HIPAA's Privacy Rule is all about the use and disclosure of Protected Health Information or PHI. With few exceptions, PHI cannot be used or disclosed by anyone unless it is permitted or required by the Privacy Rule.

B. PHI is used when shared, examined, applied, or analyzed.

C. PHI is disclosed when released, transferred, or in any way accessed by anyone outside the covered entity.

D. Boundaries on medical record use and disclosure: With few exceptions, client health information may only be used for health purposes, such as treatment, payment, and health care operations. Health information generally may not be used for non-health care purposes, such as disclosures to employers to make personnel decisions, or disclosures to financial institutions, *unless* the client gives explicit authorization to do so. Disclosures must be limited to the minimum necessary for the purpose of the disclosure, *except* for treatment purposes, in which case physicians may need full access to such information in order to provide quality care.

E. Consent, authorization, and notice: The Privacy Rule establishes a requirement that most doctors, hospitals, or other desired treatment health care providers obtain a client's written "consent" before using or disclosing the client's personal health information. If a client refuses to consent, the health care provider may refuse to treat the client. A client's written consent need only be obtained by a provider once. The consent document may be brief and may be written in general terms. The consent, however, must:

1. Be in plain language;

2. Inform the person that information may be used and disclosed for treatment, payment, and/or healthcare operations;

3. State the client's rights to review the provider's privacy notice, to request restrictions, and to revoke consent; and,

4. Be dated and signed by the individual or his/her legal representative.

F. Since ADSS/AAA'S is not a direct treatment provider (*i.e.*, provider of physician, nurse, or clinical social work degreed professional services), a written consent form signed by clients may not be required. A covered entity must retain the signed consent form for six years from the date it was obtained.

G. An "authorization" is a more customized document that gives covered entities permission to use specified personal health information for specified purposes or to disclose personal health information to a third party specified by the client. Covered entities may not condition treatment or coverage based on the person's willingness to provide authorization. An authorization form is detailed and

specific to the permitted uses and disclosures, to the permitted recipient, and to the personal health information that may be shared. An authorization also has an expiration date and in some cases may state the specific purpose for health information disclosure. An authorization is not generally required by HIPAA for most ADSS/AAA'S activities. Review the "when is authorization required" section below for more information.

H. All covered entities, such as ADSS/AAA'S, must provide "notice" of an individual's rights and responsibilities with regard to the use and disclosure of his/her personal health information. Since ADSS/AAA'S is not a direct treatment provider, no consent or acknowledgement or receipt of the privacy policy or rights and responsibilities is required. The regulations do not require that the individual correctly read the notice, nor that the covered entity explain each item in the notice before obtaining consent.

I. Permitted disclosures not requiring client consent or authorization: The final federal rule permits—but does not require—covered entities to continue certain existing disclosures without client permission. These disclosures include:

1. Emergency circumstances: ADSS/AAA'S staff may use or disclose PHI in an emergency treatment situation.
2. Communication barriers: ADSS/AAA'S staff may use and disclose PHI if agency staff or a physician attempts to obtain consent from a client but is unable to do so due to substantial communication barriers and it is determined, using professional judgment, that the client intended to consent to use or disclosure under the circumstances.
3. Identification of a body of a deceased person, or the cause of death;
4. Public health needs;
5. Research, generally limited to when a waiver of authorization is independently approved by a privacy board or Institutional Review Board;
6. Oversight of the health care system;
7. Judicial and administrative proceedings;
8. Limited law enforcement activities; and,
9. Activities related to national defense and security.

J. Special protection for psychotherapy notes: Psychotherapy notes (used only by a psychotherapist) are held to a higher standard of protection when they are not part of the medical record.

K. HIPAA's overall impact on states: HIPAA regulations have a direct impact on state social service departments, such as ADSS/AAA'S. There is an impact on computer systems and internal privacy and confidentiality policies that carry with them corresponding costs. These are only the *direct* impacts of HIPAA; other less obvious, secondary impacts on states are discussed below.

1. Preemption of state laws: Federal HIPAA requirements establish national standards for electronic transactions, privacy, and security. As such, federal laws preempt state laws, meaning that state laws which conflict with federal laws are not enforceable, and states must comply with the federal laws. However, a state is free to impose laws that are stricter than federal law. Also, HIPAA does not limit a state's ability to require health plan reporting or auditing.

2. Practical implications: Both the Administrative Simplification and the medical privacy rules affect states because the rules require states to adopt the standard transactions and code sets, as well as establish a formal mechanism for ensuring the privacy of personal health information.

L. ADSS/AAA'S staff are permitted to use or disclose PHI:

1. For treatment, payment, and healthcare operations

2. With authorization or agreement from the individual client

3. For disclosure to the individual client

4. For incidental uses such as physicians talking to clients in a semi-private room

M. ADSS/AAA'S staff are required to release PHI for use and disclosure:

1. When requested or authorized by the individual—although many exceptions apply

2. When required by the Department of Health & Human Services ("HHS") for compliance or investigation

V. WHEN IS AUTHORIZATION REQUIRED?

A. The privacy rule makes consent for routine healthcare optional. A signed authorization from the client is required if his or her Protected Health Information is used or disclosed for purposes other than:

1. Treatment: PHI may be used and disclosed to provide, coordinate, or manage clients' healthcare and any related services, for example, disclosure of PHI, as necessary, to a home health agency that provides care to clients or to a physician to whom the client has been referred to ensure that the physician has the necessary information to diagnose or treat the client.

2. Payment: PHI will be used, as needed, to obtain payment for health care services. For example, obtaining approval for a hospital stay may require that protected health information be disclosed to the health plan to obtain approval for the hospital admission.

3. Healthcare operations: PHI may be used or disclosed, as needed, to support the business activities of the agency. These activities include, but are not limited to, quality assurance activities, employee performance review activities, training of agency staff, and conducting or arranging for

other business activities. PHI may be used or disclosed to third party "business associates" that perform various activities (*e.g.*, billing, transcription services) for the agency. Whenever an arrangement between the agency and a business associate involves the use or disclosure of PHI, a written contract that contains terms that will protect the privacy of the PHI is required.

B. Generally, signed authorization is required to use PHI:

1. For use or disclosure of psychotherapy notes (except for treatment, payment, or healthcare operations)

2. For use and disclosure to third parties for marketing activities such as selling lists of clients and enrollees.

C. However, covered entities can communicate freely with clients about treatment options and health-related information.

VI. WHAT IS INCLUDED IN AN AUTHORIZATION FORM?

A. Each authorization form covers only the use/disclosure outlined in that form. The form must contain:

1. A description of the PHI to be used/disclosed, in clear language

2. Who will use/disclose PHI, and for what purpose

3. Whether or not it will result in financial gain for the covered entity

4. The client's right to revoke the authorization

5. A signature of the client whose records are used/disclosed, and a date of signing

6. An expiration date

VII. WHEN IS AUTHORIZATION NOT REQUIRED?

A. PHI can be used/disclosed without authorization, but with client agreement, for the following reasons:

1. To maintain ADSS/AAA'S'S client list or directory

2. To inform family members or other identified persons involved in the client's care, or notify them on client location, condition, or death

3. To inform appropriate agencies during disaster relief.

B. Other permitted uses/disclosures that do not require client agreement include:

1. Required by law: ADSS/AAA'S staff may use or disclose PHI to the extent that the use or disclosure is required by law. The use or disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law.

2. Public health: ADSS/AAA'S staff may disclose PHI for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information. The disclosure may be made for the

purpose of controlling disease, injury, or disability. ADSS/AAA'S staff may also disclose PHI, if directed by the public health authority, to a foreign government agency that is collaborating with the public health authority.

3. Communicable diseases: ADSS/AAA'S staff may disclose PHI, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.

4. Health oversight: ADSS/AAA'S staff may disclose protected health information to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs, and civil rights laws.

5. Abuse or Neglect: ADSS/AAA'S staff may disclose PHI to a public health authority that is authorized by law to receive reports of abuse, neglect, or exploitation. In addition, ADSS/AAA'S staff may disclose PHI if it is believed that a child or adult has been a victim of abuse, neglect, exploitation, or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

6. Legal Proceedings: ADSS/AAA'S staff may disclose PHI in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized), in certain conditions in response to a subpoena, discovery request or other lawful process.

7. Law Enforcement: ADSS/AAA'S staff may also disclose PHI so long as applicable legal requirements are met, for law enforcement purposes. These law enforcement purposes include (1) legal processes and otherwise required by law, (2) limited information requests for identification and location purposes, (3) pertaining to victims of a crime, (4) suspicion that death has occurred as a result of criminal conduct, (5) in the event that a crime occurs on the premises of the agency, and (6) medical emergency and it is likely that a crime has occurred.

8. Coroners, Funeral Directors, and Organ Donation: ADSS/AAA'S staff may disclose PHI to a coroner or medical examiner for identification purposes, determining cause of death or for the coroner or medical examiner to perform other duties authorized by law. ADSS/AAA'S staff may also disclose PHI to a funeral director, as authorized by law, in order to permit the funeral director to carry out their duties. ADSS/AAA'S staff may disclose such information in reasonable anticipation of death. PHI may be used and disclosed for organ, eye, or tissue donation purposes.

9. Research: ADSS/AAA'S staff may disclose PHI to researchers when their research has been approved by the agency after review of the research proposal and established protocols to ensure the privacy of PHI.

10. Criminal Activity: Consistent with applicable federal and state laws, ADSS/AAA'S staff may disclose PHI if the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. ADSS/AAA'S staff may also disclose protected health information if it is necessary for law enforcement authorities to identify or apprehend an individual.

11. Military Activity and National Security: When the appropriate conditions apply, ADSS/AAA'S staff may use or disclose PHI of individuals who are Armed Forces personnel (1) for activities deemed necessary by appropriate military command authorities; (2) for the purpose of a determination by the Department of Veterans Affairs of the client's eligibility for benefits, or (3) to foreign military authority if the client is a member of that foreign military services. ADSS/AAA'S staff may also disclose PHI to authorized federal officials for conducting national security and intelligence activities, including for the provision of protective services to the President or others legally authorized.

12. Social Security/Workers' Compensation: PHI may be disclosed by ADSS/AAA'S staff to comply with Social Security dependent or disability benefits, workers' compensation laws, and other similar legally established programs.

13. Inmates: ADSS/AAA'S staff may use or disclose PHI if the client is an inmate of a correctional facility and PHI is needed in the course of providing care to the client.

14. Required Uses and Disclosures: Under the law, ADSS/AAA'S staff are required to make disclosures when required by the Secretary of the Department of Health and Human Services to investigate or determine ADSS/AAA'S compliance with HIPAA requirements.

15. Statistics: De-identified health information may be used or disclosed to private and public sources and individuals as allowed or required by law.

VIII. WHAT IS MINIMUM NECESSARY?

A. In general, use/disclosure of PHI is limited to the minimum amount of health information necessary to get the job done. That means:

1. Covered entities must develop policies and practices to make sure the least amount of health information is shared

2. Employees who regularly access PHI must be identified

3. The types of PHI needed and the conditions for access

B. The Minimum Necessary Rule does not apply to use/disclosure of medical records for treatment, since healthcare providers need the entire record to provide quality care.

IX. WHAT IS THE PRIVACY NOTICE?

A. Clients have the right to adequate notice concerning the use/disclosure of their PHI on the first date of service delivery, or as soon as possible after an emergency. New Notices must be issued when the facility's privacy practices change.

B. The Privacy Notice must:

1. Contain client's rights and the covered entities' legal duties

2. Be made available to clients in print

3. Be displayed at the site of service, or posted on a web site if possible

C. Once a client has received notice of his or her rights, direct healthcare treatment providers must make an effort to get written acknowledgement of receipt of notice from the client, or document reasons why it was not obtained. Copies of all notices and acknowledgements must be kept. Since ADSS/AAA'S is not a direct treatment provider, the agency is not required to obtain a written acknowledgement of receipt of notice from the client.

X. WHAT ARE THE PRIVACY RIGHTS OF CLIENTS?

A. The Privacy Rule grants clients new rights over their PHI. These rights include the following:

1. Right to inspect and copy health information: The client has the right to inspect and copy his/her PHI. This means the client may inspect and obtain a copy of PHI contained in the record, including medical and billing records. Under federal law, however, the client may not inspect or copy the following records: psychotherapy notes; information complied in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding; such as a child or adult abuse investigation, and PHI subject to law that prohibits access to PHI. ADSS/AAA'S may deny a client access to PHI without providing an opportunity for review if the PHI relates to any of the above or if the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably expected to reveal the source of the information. Depending on the circumstances, a decision to deny access may be reviewed on the request of the client. There are state laws that make certain ADSS/AAA'S records confidential and not subject to public disclosure.

2. Right to request restrictions: Clients have the right to request a restriction of their PHI. This means the client may ask ADSS/AAA'S staff not to use or disclose any PHI for the purposes of treatment, payment, or healthcare operations. The client may also request that any part of his/her PHI not be disclosed to family members or friends who may be involved in his/her

care or for notification purposes as described in the Notice of Privacy Practices. ADSS/AAA'S staff are not required to agree to a restriction that the client may request. If ADSS/AAA'S staff believe it is in the client's best interest to permit use and disclosure of the client's PHI, the PHI shall not be restricted. If ADSS/AAA'S staff do agree to the requested restriction, PHI may not be used or disclosed in violation of that restriction unless it is needed to provide emergency treatment. **Review program policy with supervisor on all requests.**

3. Right to receive confidential communications: The client has the right to request that confidential communications from the agency be sent by alternative means or to an alternative location. ADSS/AAA'S staff shall accommodate reasonable requests. ADSS/AAA'S staff may also condition this accommodation by asking the client for information as to how payment will be handled or specification of an alternative address or other method of contact. ADSS/AAA'S staff will not request an explanation from the client as to the basis for the request. Such requests must be made in writing to the Civil Rights and Equal Employment Partnership. **Review program policy with supervisor on all requests.**

4. Right to amend health care information: The client has the right to request that ADSS/AAA'S amend PHI. The client may request an amendment of PHI in the ADSS/AAA'S case record. In certain cases, ADSS/AAA'S staff may deny a client's request for an amendment. If ADSS/AAA'S staff deny the request for amendment, the client has the right to file a statement of disagreement with the agency. The agency may then prepare a rebuttal to the client's statement and provide the client with a copy of any such rebuttal. **Review program policy with supervisor on all requests.**

5. Program staff are to consult with ADSS/AAA's Privacy Officer, as needed, on all requests to inspect, copy, copy of privacy policy, amend health care information, accounting, receive confidential information and restrict health information. ADSS/AAA's must act upon a request for PHI within **thirty (30) days** after receipt of the request (60) days if the PHI is not on site; (90) days if written reasons for delay are given by granting or denying the request, in whole or in part, in writing. ADSS/AAA's may charge the client for the cost of copying, postage, and preparation of any explanation or summary of PHI released at the rate of 25 cents per page plus the salary rate of the staff labor spent on the production. A denial shall contain (1) the basis for the denial; (2) statements that the person may request a review and may file a complaint with ADSS/AAA'S or the federal DHHS/OCR.

6. The client has the right to receive an accounting of certain disclosures, if any, ADSS/AAA's staff has made of the client's PHI. This right applies to disclosures for purposes other than treatment, payment, or healthcare operations as described in ADSS/AAA's Notice of Privacy Practices. It

excludes disclosures ADSS/AAA's staff may have made to the client, for a client list, to family members or friends involved in the client's care, or for notification purposes. The client has the right to receive specific information regarding any such disclosures that occur after April 14, 2003. The client may request a shorter timeframe. The right to receive this information is subject to the exceptions, restrictions, and limitations allowed by law. ADSS/AAA's staff may not release such information if it would violate the law, interfere with an agency investigation, or be detrimental to case planning or program objectives.

7. Right to a copy of privacy policy. The client has the right to obtain paper copies of the ADSS/AAA's Privacy Notice and privacy policy upon request. The Privacy Notice and privacy policy will be available on ADSS/AAA's web site, www.ageline.net **Review program policy with supervisor on all requests.**

XI. WHAT ABOUT THE PRIVACY RIGHTS OF MINORS?

A. In general, parents have the right to access and control the PHI of their minor children—except when state law overrides parental control. Examples of cases in which parents do not control the PHI of minors include:

1. HIV testing of minors without parental permission
2. Cases of abuse or neglect
3. Cases in which the release of PHI would be detrimental to case planning
4. When parents have agreed to give up control over their minor child voluntarily or by court order.

XII. WHAT ABOUT THE RIGHT OF PERSONAL REPRESENTATIVES (Parents, Guardians, etc.) TO PHI ON THE INDIVIDUALS THEY REPRESENT?

A. In general, a personal representative stands in the shoes of the individual and is, therefore, treated as the individual with respect to notices, use and disclosure, and rights under HIPAA. Where HIPAA gives an individual certain rights, such as the right to receive notice or the right to inspect PHI, the personal representative also has those rights

B. The authority of the personal representative is set by state law and is limited under HIPAA to PHI that is relevant to the representation. For example, a personal representative with a limited health care power of attorney to make only life support treatment decisions is restricted to PHI related to those decisions and does not have the right or authority to sign an authorization for disclosure of PHI for other purposes.

C. The following persons are recognized as personal representatives for a category of individuals:

1. If the individual is an adult or emancipated minor (by court order after age 18 but under age 19 or by marriage after age 18), the personal representative is a person with legal authority to make health care

decisions on behalf of the individual; *e.g.*, health care power of attorney, court-appointed guardian, general/durable power of attorney.

2. If the individual is an unemancipated minor (under age 19), the personal representative is a parent, guardian, or other person acting *in loco parentis* (such as a foster parent or residential care provider or relative with written parental delegation of authority). The parent/guardian/person *in loco parentis* is allowed to make health care decisions for a minor child only to the extent expressly permitted or required by state or federal law (including case law). HIPAA prohibits disclosure or access to a minor child's PHI when, and to the extent, it is expressly prohibited under state or federal law (including case law). Under HIPAA, state and other applicable law governs when such law explicitly requires, permits, or prohibits the disclosure of or access to health information about a minor child. Alabama law on confidentiality, relevant federal confidentiality law, and court cases, such as the *R.C.* child welfare case, constitute governing law under this provision. Additionally, there are three situations in which a parent/guardian/person acting *in loco parentis* is not the child's personal representative:

   a. when the minor is the one who consents to care and consent of the parent is not required under state or federal law (such as in some abortion or STD treatment cases);

   b. when the minor obtains care at the direction of a court or a person appointed by the court (such as juvenile court or adult protective service court orders); and

   c. when, and to the extent, the parent/guardian/person acting *in loco parentis* agrees that the minor and ADSS/AAA'S staff may have a confidential relationship.

   Access by a parent/guardian/person acting *in loco parentis* is denied when state law prohibits such access. If state law is silent, ADSS/AAA'S staff may exercise professional judgment to the extent allowed by law to grant or deny access to the minor's PHI. HIPAA does not change state statutes with regard to treatment or consent to treatment of minors or adults in need of protection. HIPAA addresses access and disclosure of PHI not underlying treatment decisions.

D. In cases involving allegations or determinations of abuse, neglect, exploitation, endangerment, or domestic violence by a personal representative, ADSS/AAA'S staff may decide not to treat the personal representative as the individual's personal representative for PHI purposes if, in the professional judgment of the worker, doing so would not be in the individual's best interest.

XIII. WHAT MUST ADSS/AAA'S DO TO COMPLY WITH HIPAA?

A. Designate a full- or part-time privacy official responsible for implementing the programs.

B. Designate a contact person or office responsible for receiving complaints.

C. Develop a Notice of Privacy Practices document

D. Develop policies and safeguards to protect PHI and limit incidental use or disclosure

E. Institute employee training programs, so everyone knows about the privacy policies and procedures for safeguarding PHI

F. Institute a complaints process, and file and resolve formal complaints

G. Make sure contracts with business associates comply with the Privacy Rule

XIV. WHAT HAPPENS TO THOSE WHO DO NOT COMPLY?

A. Penalties: Individuals have the right to sue covered entities, such as doctors and nurses, in court to enforce HIPAA. Due to sovereign immunity, clients do not have the right to sue ADSS/AAA's or ADSS/AAA's staff in court for civil damages. Clients do have the right to file a formal complaint with the United States Department of Health & Human Services ("HHS") Office of Civil Rights ("OCR") if they believe a covered entity has violated HIPAA requirements. HHS/OCR has the authority to investigate and penalize covered entities. There are civil and criminal penalties associated with HIPAA noncompliance. If a covered entity is found in violation of HIPAA, these are the potential consequences:

1. Civil penalties: $100 per violation, up to $25,000 per person, per year for each requirement or prohibition violated.

2. Criminal penalties: For knowingly violating client privacy, the following federal criminal penalties apply:

   a. Up to $50,000 and 1 year in prison for obtaining or disclosing protected information.

   b. Up to $100,000 and up to five years in prison for obtaining or disclosing protected information under false pretenses.

   c. Up to $250,000 and up to 10 years in prison for obtaining or disclosing protected information with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.

XV. WHAT CAN ADSS/AAA'S STAFF DO TO PROTECT ADSS/AAA'S CLIENTS' PRIVACY AND CONFIDENTIALITY?

A. HIPAA further defines and protects the fundamental right of clients to privacy and confidentiality of PHI. To do your part:

1. Make sure you fully understand ADSS/AAA's privacy practices

2. Protect clients' PHI

3. Encourage others to do the same.