AMS CORPORATE CONFIDENTIALITY-HIPPA-DUTY TO WARN

Policy:

Confidentiality Guidelines – Introduction
Every patient and former patient must be assured that his or her right to privacy will be protected. Without this assurance, fear of the disclosure of his or her drug abuse or of the records of other behaviors and/or problems will discourage him or her from seeking the treatment. The following will therefore apply:

- The Clinic will protect the confidentiality of all patients. This includes all applicants for services.
- The Clinic will not reveal information about patients, unless authorized by Federal Regulations as stated in (42 CFR Part 2).
- The Clinic may disclose information in certain circumstances, but only after following procedures as stated in Federal Regulations (42 CFR Part 2, Section V).

The Patient must sign a Release of Information form before any information may be released to family members, friends, legal authorities, etc.

Confidentiality Guidelines – Exceptions
It is the policy of AMS to ensure full and complete compliance with local, state and federal regulations maintaining confidentiality of patients at all times and to provide all patients information concerning confidentiality and the exceptions to all confidentiality requirements in an understandable manner.

Employee:

1. All Employees will be provided training in the following areas upon hire and at least once each year:
    a. Confidentiality
    b. Mandated reporting
    C. SUBPOENAS
    d. Search Warrants
    e. Exceptions to Confidentiality.
2. All employees will be required to sign the Confidentiality and Exceptions agreement upon hire. This form will be maintained within the individual employee record.

Patient:

1. Patients will be provided written information concerning confidentiality, exceptions and mandated reporting requirements during the intake process and at least once each year thereafter.
2. Documentation of this orientation will be maintained in the patient record.

Confidentiality Guidelines – Contacting A Patient (Telephone / Mail)

AMS believes that it is a fundamental responsibility to keep patients engaged in recovery. Therefore, it is the policy of the organization to contact any patient that has stopped seeking treatment without prior notification to the treatment team.

1. Confidentiality is a high priority and all procedures to protect the patient's confidentiality are to be followed.
2. Documentation for release of medical information to discuss patient treatment with specific individuals identified by the patient will be maintained in the patient chart.
3. Patient will be contacted by telephone if two (2) consecutive days of "no shows" have occurred and no prior notice had been given to the Clinic.
4. The patient's Counselor will make at least three (3) attempts to make contact with the patient and each attempt will be documented in the patient's chart.
5. If the Counselor is only able to leave a message, he / she is not to identify himself as being from a methadone maintenance clinic or a treatment provider.
6. The Counselor will explain to the patient all available options i.e. returning to treatment, being discharged from the Clinic and the process for future readmission to the Clinic, transferring to another provider, etc.
7. If a patient chooses to discontinue treatment then the Counselor will ask for the patients consent to contact them in 90 days. In 90 days the former patient will be contacted by phone or mail in order to conduct follow-up and to inquire about readmission to the Clinic.
8. The patient has the right to refuse any contact, by phone or mail, from any representative of the Clinic.

FORMAT FOR WRITTEN AUTHORIZATION FOR DISCLOSURE OF INFORMATION

I. The responsible staff person will obtain informed and voluntary written authorization before disclosing information contained in the patient record. The authorization must contain certain elements before it meets state and federal regulations. These regulations are 42 C.F.R. Part 2, Subpart C, §2.31. Authorization must include the following elements:
   - A. The name of the patient;
   - B. The specific name or general designation of the program or person permitted to disclose the information;
   - C. Name of the person and title, or organization to whom disclosure is to be made;
   - D. Specific information (i.e., how much and what kind of information) that may be disclosed within compliance with state and federal laws and regulations (information should be limited to the least amount needed to achieve stated purpose noted in E);
   - E. Specific purpose for the disclosure;

F. A statement that the consent is subject to revocation at any time except to the extent that the person who is to make the disclosure has already acted in reliance on it.
G. Dated signature of patient;
H. Dated signature of a witness (Note: Witness must date and sign at same time as patient for consent to be valid);
I. The date, event or condition upon which the consent will expire, if not revoked earlier; and,
J. A mechanism to verify that the patient was offered a copy of the consent and verification that the patient either accepted or rejected the copy (i.e., checkboxes or initials, etc.).

II. The responsible staff will use the approved AMS consent, which contains all the above elements and will ensure that all items "A" through "J" are completed.
III. A copy of the consent will be given to the patient if accepted, and the original consent will be filed in the patient record.
IV. The appropriate staff will be notified that the consent has been signed (i.e., switchboard operator, counselor, etc.).

In the case of discharged patients, all patients will sign a consent giving AMS will obtain a consent for post discharge follow up.

RELEASE OF INFORMATION WHEN CONSENT IS NOT REQUIRED

I. Under **meshed** State and Federal laws and regulations, the circumstances when information can be released without consent are highly limited and very specific. Information may be disclosed without release under the following circumstances only:

A. In emergency medical conditions where the life of the patient is in immediate jeopardy, records may be released to the proper medical authorities solely for the purpose of providing medical treatment.

B. **In cases of child abuse, reporting is mandated by law**.

C. To official reviewers and evaluators of the program's services and functions for certification, auditing and research purposes.

D. If the event of patient's commission of a crime, or threat to commit a crime on program premises, or against program personnel. In these cases, the only information that may be release to law enforcement officials is:

- the circumstances of the incident;
- status of the individual patient committing or threatening to commit the crime;
- patient's name, address and last known whereabouts.

E. After issuance of a court order meeting the requirements of 42 C.F.R., Part 2, Subpart E, §2.64, Under the Federal regulations, issuance of a court order

requires a special hearing to review the purpose of the disclosure and to determine if good cause exists for the court to issue such an order.

II. Whenever such disclosure is made, the disclosure will be fully documented in the patient's record, the patient will be informed that the information was disclosed (if possible), and the documentation will explain for what purpose the disclosure was made and to whom.

LIMITATIONS ON RELEASE OF INFORMATION

I. Even though a patient signs a written authorization for release of information, there are limitations to what type of information may be released.

A. Information must be limited to the minimum necessary to accomplish the stated purpose under the regulations, rules, and/or laws governing such release.

(1) Whether the patient is or is not in treatment.
(2) Patient's prognosis.
(3) The nature of the Project.
(4) A brief description of the patient's progress.
(5) A short statement as to whether the patient has relapsed into drug or alcohol abuse and the frequency of such relapse.

II. AMS Staff will always use the AMS five (5)-point consent when requesting that a patient sign an authorization for judges, probation or parole officers, insurance companies, health or hospital plans, or government officials.

III. Staff will only checkmark those areas of the five (5) areas on the consent that are necessary to accomplish the stated purpose. Staff will not routinely check all five (5) areas.

REVOCATION OF CONSENT BY A PATIENT FACE TO FACE

The procedure to follow when a patient revokes consent is designed to ensure disclosure is not made without consent of the patient.

a) The assigned counselor will meet with the patient
b) Review the consent the patient would like revoked
c) The counselor will strike a single line diagonally on the consent with a black pen.
d) The counselor will have the patient sign the revocation section of the consent will indicated in writing across the top of the authorization for release of Information form “On this date _____, _____(insert Patient’s name) is revoking this consent.”
e) The above mentioned statement must be dated and signed by both the counselor and the patient
f) The counselor must document on a progress note in the patient record revocation of the release.

REVOCATION OF CONSENT BY A PATIENT VERBALLY

AMS recognizes a verbal revocation of consent; all verbal revocations must be clearly documented on the consent with “Verbal Revocation written clearly and a clinical progress note must be written to reflect the patients request for Verbal Revocation.

RELEASE OF INFORMATION UNDER SUBPOENA OR COURT ORDER

I. The procedure for handling a subpoena or court order is not straightforward or simple. The Executive Director or his/her superior is responsible for executing these steps to protect the facility from a contempt of court charge and to ensure that patient confidentiality is protected as required under meshed state and federal regulations and laws.

Subpoenas

A. Any staff member who receives a subpoena will immediately notify the Executive Director and provide him/her with a copy of the document. The document must be provided without delay since subpoenas are time sensitive and **ALWAYS REQUIRE A RESPONSE.** In the Executive Director's absence, notify the Chief Operating Officer and/or CEO.

B. The problem with a subpoena is that under meshed confidentiality rules, drug and alcohol treatment providers are prohibited from releasing patient records or information unless they have (1) the patient's written authorization to release information, or (2) an accompanying good cause court order that was issued by a court of competent jurisdiction after meeting the provisions found at 42 CFR, Part 2, Subpart E, §2.64.

C. Keep in mind that a subpoena **REQUIRES A RESPONSE**. Even though drug and alcohol confidentiality rules prohibit the release of patient information with a subpoena alone, failure to respond to a subpoena will place the person named in the subpoena, and possibly the facility at risk for a charge of contempt of court, civil charges or other legal consequences. A subpoena is typically requested by a legal party and then issued from criminal, civil, family, or administrative courts A specific type of response is required depending upon the type of subpoena issued:

1. Subpoena Duces Tecum: This type of subpoena generally commands you to appear in court and to bring records with you. In some cases it will have a statement indicating that if you send records by a specific date, you will not have to appear in person.

2. Subpoena: This type of subpoena generally commands a personal appearance in court on a specific date.

D. Since treatment provider release of records/information is prohibited without a court order under meshed State and Federal regulations and laws, the goal is to have the party who requested the issuance of the subpoena dismiss you from having to appear in court so as to avoid a charge of contempt for failure to appear. It is easier to do this ahead of time than to go to the added expense of defending your position in Court on the date of the hearing only to find that the Court itself is often unfamiliar with these rules.

E. The first step in having your appearance dismissed is to send a form letter to the party who requested the issuance of the subpoena. In the letter, explain our position in regard to State and Federal confidentiality regulations.

F. If there is adequate time, the letter must be sent by "Certified Mail with Return Receipt Requested" so that AMS has documentation of a response to the subpoena. If there is not adequate time, send the letter by fax and place a call to document receipt of the fax. Document who verified receipt of the fax and the date.

G. Simply responding by Certified mail or fax still does not relieve you of responsibility to appear in court. The next step is to contact the requesting party once they have received the letter and discuss AMS position. Advise the requesting party that if the individual in question is or ever was a patient at our facility, and if you appear in court, you would not be able to disclose any patient information or records in response to the subpoena for the reasons noted in the letter. Often the requesting party, usually an attorney, will advise that the patient will agree to sign an authorization.

H. If the requesting party persists in requiring an appearance, you will have no choice, but to contact AMS legal counsel to request a "Motion to Quash the Subpoena." Any contact with legal counsel requires pre-approval through the AMS Chief Operating Officer and/or CEO.

I. Legal counsel will advise of any further steps to take from this point forward. Keep in mind that if for any reason you are directed to appear in court with the patient's written consent, release is limited to the five areas identified under law as previously stated, provided that the consent allows for the release of all five areas.

Court Orders

A. Any staff member who receives a court order mandating release of information will immediately notify the Executive Director provide him/her with a copy of the document. The document must be provided without delay since court orders are time sensitive and **ALWAYS REQUIRE A RESPONSE.** In the Executive Director's absence, contact the Chief Operating Officer and/or CEO.

B. In the event that a court order is issued for you to release records or information, the court order should be reviewed by AMS legal counsel to ensure it meets the requirements of 42 CFR, Part 2, Subpart E, §2.64.

C. If the order is valid under those regulations and requires a court appearance, the order will specify what information is to be released. In this case, you are to release whatever information the court order dictates.

D. If the order is not valid because it was not issued properly in compliance with 42 CFR, Part 2, Subpart E, §2.64, then legal counsel will submit a "Motion for a Protective Order" in an attempt to have the order vacated.

E. Legal counsel will advise of any further steps to take from this point forward.

II. Legal counsel for other treatment facilities within the region have repeatedly noted that due to the restrictive nature 42 CFR Part II the courts have, in several cases, ruled that a court order could not be issued to require AMS or one of other providers to release information when an opposing party sought a good cause court order under the Federal regulations. In other cases, it caused the Court to vacate a previously issued order for release of records when challenged. Similarly, both the State and Federal regulations have been used to quash subpoenas on behalf of AMS or other treatment providers in order to protect patient records. Below are several recent cases where another party's request for patient records were challenged by other providers:

Edwards v. Gruman Allied Industries, Inc., 2 D.&C.4th 464 (Lyc. Co. 1988).

Petition of the Commonwealth for Release of Patient Records Pursuant to 42 C.F.R. §2.66 and 71 P.S. §1690.108 (2000).

Motion by White Deer Run, Inc. to Quash Subpoena or for Protective Order No. 1998-2525 Issued March 15, 2002 (2002).

In each of these cases, the courts found in favor of the treatment provider and either vacated their previous orders release records, or quashed an existing subpoena.

RELEASE OF INFORMATION TO ATTORNEYS

I. Attorneys **who represent the patient or former patient** in a civil, criminal, or administrative situation may have whatever information the patient chooses to allow for release with a properly executed authorization under the State and Federal regulations. In this case make certain you do not acknowledge the patient's presence or history of presence prior to a valid authorization signed by the patient or former patient.

II. Attorneys **who represent a party other than the patient or former patient**, according to AMS legal counsel, not permitted to obtain patient information or records even with a valid, written authorization signed by the patient. In the case where an attorney from the opposing party request records, the responsible staff is to respond with the statement written in this policy and procedure under the heading "What To Say To Legal Representatives If The Patient Will Not Sign A Consent". If the attorney presents a consent from the patient, the

same responsible staff is to respond by stating, Legal counsel has advised that AMS is not permitted to release patient information even with a release due to 42 CFR Part II." If the attorney persists in their request by producing a subpoena or court order, follow the instructions for handling a subpoena or court order and advise the Chief Operating Officer and CEO so that legal counsel can be contacted to assist, if it becomes necessary.

RELEASE OF INFORMATION UNDER ARREST WARRANTS / SEARCH WARRANTS

The procedure for handling situations involving arrest or search warrants is rather straightforward compared to that of subpoenas and court orders. The Executive Director is responsible for executing these steps to ensure that patient confidentiality is protected to the best of the facility's ability within the constraints of the strictest state and federal laws and regulations.

State/Local Arrest Warrants

I. Any staff member who receives notification that a law enforcement officer has an arrest warrant and is seeking a patient in treatment is to immediately notify the Executive Director. For Federal Marshal's, refer to section entitled, "Federal Arrest Warrants." The Executive Director or his/her designee will:

A. If the notification of a warrant is by phone:

1. The responsible staff will determine if an authorization for the party that will be serving the warrant exists.

2. If no consent exists, no information may be released, not even an acknowledgment that the person in question was or ever has been a patient in the program (see suggested wording on the next page). The call is then terminated.

3. If a valid release exists for the specific caller or specific agency from which the caller is from, the caller may be informed that the patient is present in treatment.

4. In cases where a valid consent exists, Officials such as sheriffs, magistrates, courts, police, probation/parole officers, etc. may only have information up to the five areas identified under this regulation provided all five areas are authorized for release by the patient and then only on a need to know basis. In this case, all that should be released, if authorized by the patient,
is presence in treatment and nature of the program. Diagnosis, progress and relapse information should not be necessary; therefore, should not be released.

5. The responsible clinical staff, along with the patient, if clinically appropriate, would then speak with the sheriff, or other legal representative(s), to determine if the warrant must be executed immediately. If appropriate, attempts may be made to negotiate with the legal representative(s) to withhold execution of the warrant until after discharge. Often the magistrate or court will agree to such a request. If not, clinical staff shall prepare the patient for discharge.

B. If an arrest warrant is served in person by a law enforcement official, the following procedure is to be followed:

1. The staff person first having contact with the law enforcement official is not to acknowledge the presence of a patient in treatment. This staff person is to immediately notify a Clinical Supervisor and Executive Director that a law enforcement official is on grounds to serve an arrest warrant.

2. The Executive Director or his/her designee will ask the legal representative for identification, where necessary, and will request a copy of the warrant. Next, the Executive Director or a designee will check for a valid release for the individual or agency serving the warrant.

3. If no consent exists, and if the patient is approached and refuses to sign one, no information may be released, not even an acknowledgment that the person in question was or ever has been a patient in the program (see suggested wording on the next page). The law enforcement official is given a copy of the "AMS Statement to Law Enforcement Officials" and the official is advised we are unable to assist them further.

4. If the official persist in attempting to execute the warrant after being told the facility cannot release any information pertaining to past or present patients including confirming a patient is or was a patient in the program, do not assist the official in searching for the patient. Immediately notify the Chief Operating Officer and CEO. At the same time do not interfere. Do not warn the patient of the official's presence or in any way obstruct the official, but continue to protest the official's actions and complete an incident report. Follow the official and take note of all of the official's actions. Document those actions on the incident report.

5. If a valid release exists for the specific law enforcement official or the agency that the official represents, the official may be informed that the patient is present in treatment.

6. The responsible clinical staff, along with the patient if clinically appropriate, would then speak with the sheriff or other legal representative

to determine if the warrant must be executed immediately. If appropriate, attempts may be made to negotiate with the legal representative to withhold execution of the warrant until after discharge. Generally if the legal agent comes to the facility, this negotiation is unsuccessful.

7. Always obtain a copy of the warrant for the patient record and obtain the full names of the official(s) and the name and address of the office they represent. Document the incident in the patient record noting date, time and details of the incident.

What to Say to Legal Representatives If the Patient Will Not Sign a Consent

I. If there is no consent, or if the patient refuses to sign an authorization, the facility must comply with State and Federal regulations and inform the representative of the following:

> "State and Federal confidentiality regulations prohibit the release of any information relating to a present or former patient, including even confirming that a person is or was a patient without a written authorization or a specific type of court order that is obtained from a court of competent jurisdiction in compliance with the provisions of 42 CFR, Part 2."

II. If the legal representative is on site, provide them with a copy of the "AMS Statement to Law Enforcement Officials".

III. In most cases, the guidelines above will solve the majority of the situations facing treatment providers when confronted with arrest warrants. There are, however, some special circumstances. These include Federal Marshal's serving felony arrest warrants and police (state or local) serving search warrants.

Federal Arrest Warrants

I. In the case of a Federal Marshal's serving a felony arrest warrant, they generally will not appear at your facility unless they are certain the patient is there. They will have confirmed the patient's presence at the facility through some other means prior to their arrival. They do not call ahead to advise you they are coming and they typically show up in plain clothes. These are the steps to be followed:

A. Upon arrival, the first staff person having contact is to notify the Executive Director or Chief Operating Officer and/or CEO in the Executive Director's absence.

B The Executive Director or Designee will ask for identification. Federal Marshal's do not have to show you the warrant.

C Do not acknowledge any patient information without proper consent. Typically the officers will ask you to produce the specified patient. Advise them of confidentiality laws and regulations, specifically citing Federal regulations 42 CFR, Part 2, which makes no provisions for the release of information in these circumstances.

D. Federal Marshal's have jurisdiction even on private property with a felony arrest warrant (CFBHS legal counsel, 2002). If they choose to search for the patient, do not interfere. By the same token, do not assist.

E. Do not inform the patient they are looking for him and do not assist the patient in hiding from them. Take no further action other than to protect the confidentiality of other patients who are not involved.

F. Always obtain a copy of the warrant for the patient record and obtain the full names of the agents and the name and address of the office they represent.

G. Document the incident in the patient record noting date, time and details.

Search Warrants

If a patient commits or threatens to commit a crime on the premises of the facility or against program personnel, law enforcement can obtain the patient's name from program staff and no search warrant or consent is required.

In cases where a patient commits a crime elsewhere, and law enforcement officials seek the patient's records or identifying information from the facility through a search warrant when the crime did not occur on the premises or against program personnel, the facility is not permitted to release any information, not even an acknowledgement that individual in question is or ever was a patient in the program. Unfortunately, refusing to provide information when presented with a search warrant can be difficult since it is law enforcement that is requiring you to release information, in direct violation of the law.

I. The procedure is as follows:

A. Immediately notify the Clinic Executive Director or Chief Operating Officer and/or CEO in the Executive Director's absence.

B The Executive Director will have other staff immediately notify the Chief Operating Officer and CEO while the Executive Director meets the law enforcement officials who are presenting the search warrant.

C. If necessary, the Executive Director will ask law enforcement officials for identification and request a copy of the search warrant. **DO NOT** acknowledges if the patient had been in treatment.

D. Next, advise that a search warrant does not allow you to ignore State and Federal confidentiality regulations, specifically 42 CFR, Part 2, and 71 P.S. 1690.108, neither of which make provisions for the release of information even with a search warrant.

D. Contact AMS legal counsel to initiate an emergency "Petition to Quash Search Warrant" with the local Court of Common Pleas.

E. The Executive Director will inform the legal representatives that AMS cannot release the requested information, and if they insist on searching for it, cooperate minimally under protest. Do not interfere with, or resist a search since this would likely result in your arrest.

F. The Executive Director or his/her designee will accompany the law enforcement officials if they elect to search the property and will document all actions they take.

G. Always document the events including date, time, names of officers, agency they are from and place a copy of the search warrant in the patient record.

H. Also document contact with legal counsel and the Division of Licensing.

A. An unusual incident report to the Division of Licensing must also be completed and forwarded through the Chief Operating Officer and CEO.

MEGAN'S LAW

Megan's Law has implications for patient confidentiality. Megan's Law was essentially created to register persons convicted of sexual crimes against minors who meet the definition of a "sexual predator." Given the commonalities between chemical addiction and sexual addiction, drug and alcohol treatment providers could be faced with patients who may be required to register themselves under Megan's Law. The confidentiality issue is solved by requiring the patient to conduct his/her own registration as required by law. The facility can provide the resources to assist, but cannot register for the patient.

The following are the basic requirements of Megan's Law. For full details visit Megan's Law on the Internet at: http://www.meganslaw.state.pa.us

- Megan's Law requires the offender to register. The responsibility for registration falls on the offender.
- "An out-of state offender who is required to register as a sexual offender in the offender's home state is automatically required to register in Pennsylvania if the

offender intends to reside, work or attend school in Pennsylvania" (KlaasKids Foundation, 2001).

I. The following procedure will be followed when a patient is required to register under Megan's Law:

A. The patient will be provided phone access to contact his or her legal counsel, probation officer or other legal representatives to assist them in determining their responsibility for the registration process.

B. If the patient and the patient's attorney or probation officer or other legal representative determines that the patient must register with the local police department serving the treatment facility, the facility will provide transportation to and from the police station so that the patient may register. The transportation of the patient will be provided in such a way so as not to identify the patient as a patient of the agency. For example, the vehicle will not be marked, the staff will not accompany the patient into the police station, the staff will not leave the vehicle or wear a nametag identifying where they are from, etc.

C. In the event that the police require verification of the patient's address, the patient will have the option to sign an authorization allowing AMS to verify their presence in treatment.

D. If the patient has any other special needs regarding the registration process the facility will assist the patient in any reasonable way, within applicable laws and regulations.

DUTY TO WARN

Duty to warn is a complicated issue in a drug and alcohol treatment setting due to confidentiality laws and regulations prohibiting or limiting disclosure on patient information. There is a "legal" duty to warn for substance abuse treatment providers in the State of Delaware. Failure to warn exposes a third party to potential harm, exposes the patient to potential additional consequences and may expose the provider to civil liability. Under federal regulations, a drug and alcohol provider cannot warn a third party of a threat without a court order under federal regulations, and then under Maryland State Law, the warning cannot include any information that would identify the patient as a drug and alcohol patient. The warning to a third party can only occur after petitioning the court under a John Doe Court Order.

Confidentiality Guidelines – Reporting Child and Elder Abuse

When the staff member becomes aware that there is some type of abuse, the staff member will follow the **mandated reporter** requirements.

1. The staff member will follow all Confidentiality Regulations.
2. The Executive Director will be notified and become part of the reporting process.
3. The staff member, in coordination with the Executive Director, will inform the appropriate agency, either the child or elderly protections agency within the state wherein the clinic is licensed to operate. All reporting requirements will be met.
4. The staff member, in coordination with the Executive Director, will immediately fill out an Incident Report, detailing known information about the suspected
5. abuse.

Confidentiality Guidelines – Disclosure Notice

*This information has been disclosed to you from records whose confidentiality is protected by Federal Law. Federal Regulations (**42 CFR PART 2**) prohibits you from making any further disclosure of said records without the specific written consent of the person to whom it pertains, or as otherwise permitted by such regulations. A general authorization for the release of medical or other information is **not** sufficient for this purpose.*

Records – Security of Confidential records

In order to protect and ensure the confidentiality of administrative records and records of the patients, AMS will restrict access to all records. The Executive Director and / or Designee shall be responsible for maintaining a secure system that protects and ensures the confidentiality of all records at all times. In the event that a legal process is initiated against the organization, the program director and / or designee shall ensure all records will be maintained, preventing any type of tampering, altering, destruction, etc. If any closed files have been scheduled for destruction an order will be issued to stop the shredding process until those records can be retrieved.

1. Electronic Records

    A. The Backup of all electronic records will be conducted on a nightly basis.

    B. Administrative records received or sent electronically (including facsimiles and electronic mail) will be handled in such a manner as to protect the rights and privacy of all individuals and agencies involved and will be carried out according to all legal requirements.

    C. Patient records received or sent electronically (including facsimiles and electronic mail must follow 42 CFR Part 2 and HIPAA regulations, for disclosure of patient information.

2. Patient Records

   A. All patient records are subject to confidentiality and accountability as defined by 42 CFR Part 2 and HIPAA regulations.

   B. A Quality Service Organization Agreement (QSOA) will be established and maintained with each organization, i.e. janitorial, laboratories, that may have direct or indirect access to confidential patient identifying information.

   C. Records will be stored in designated storage areas (active / inactive) that are maintained in a secure manner at all times that will ensure limited access, and reasonable protection against theft, fire, water damage, and other hazards.
      1. Active Files will be maintained in a Clinic designated securable location.
      2. The designated record location will remain closed and locked when not in use.
         a. Clinic Staff will limit the number of active records, (necessary for daily use) to be removed from the file room.
            1. When removed, records will be maintained in such a manner as to protect and ensure confidentiality, i.e., stored in desk drawer or individual file cabinet when not in use.
            2. A log will be maintained of all records removed, by whom, and include return time and date information.
            3. Records are not removed from the clinic location without Executive Director approval.
      3. Inactive files will be maintained in a Clinic designated storage area.
         a. The designated storage area will remain closed and locked at all times.
         b. Clinic staff with access to the inactive files will ensure confidentiality of such records at all times.
         c. Inactive patient records will be destroyed pursuant to the procedure for Destroying Records.

      4. In the event patient records are destroyed due to a natural disaster or other hazard, the following will be initiated:
         a. A new patient record will be implemented.
         b. Patients will be required to sign intake consent forms.
         c. Agencies maintaining a QSOA will be contacted to obtain copies of necessary records, i.e., laboratory reports.

3. Administrative Records

A. Administrative records stored electronically, i.e., policies, procedures, training materials, and employee data, will be stored on disc and updated on a regular basis (monthly or on addition of new material). Disc(s) will be stored in such a manner as to protect from theft, fire, water or other hazards and ensure confidentiality.

B. All other administrative records will be maintained in Clinic designated secure areas to ensure confidentiality and protect from theft, fire, water or other hazards.

4. Record Destruction

A. Refer to the procedure for Destroying Records for the following:

Patient Medical Record	Biennial Audits
Patient Maintenance Charts	Patient's Ledger / Billing Cards
Detoxification Charts	Production Reports
Discharged Employee Files	Receivables
Day Sheets	Employee Time Cards
Medication Audits	Copies of Patient Receipts
Medication Daily Audits	Other records

B. Miscellaneous documents that have identifying patient information, i.e., communication logs, will be destroyed onsite by designated clinic staff or a professional, certified shredding company which will furnish a certificate stating that all material has been destroyed. Destruction of such records will be performed in such a manner as to eliminate any identifying patient data (electronic paper shredding equipment). Certificates of destruction will be maintained on file by the clinic office manager.

<u>Records – Destroying Records</u>
It may become necessary to destroy outdated records. All outdated records which have a patient name will be shredded either by designated Clinic staff or a professional, certified shredding company which will furnish a certificate stating that all material has been destroyed. Certificates of destruction will be maintained on file by the clinic office manager.

All patient records will be kept in secure locations for no less than ten (10) calendar year; this includes all patient clinical, medical, financial and other records.

As patient files become inactive, for a period of at least one year, patient records should be placed in an appropriate storage location, and the admit date month and year recorded on the outside of the file. This will assist in locating which outdated files are ready to be destroyed.

On a bi-annual basis, clinic staff should examine outdated files and destroy files that are 10+ years old, in the manner indicated above.

Refer to the Clinic / State Manual for record destruction time frames that may be greater than those indicated within this policy.

In the event that a legal notice is received notifying AMS or any program that a closed record is needed, any order for records destruction will be suspended until that record(s) is/are located and secured.

Records – Order for Purging Patient's Records

All patient records will be purged in a systematic manner ensuring that all documentation will remain in the active folder. Refer to the Clinic / State Manual for the order for patient record purging.

Duty to Warn

HIPAA – Overview of Privacy Rule

Health Insurance Portability and Accountability Act (HIPAA)

The final privacy standards adopted by the U.S. Dept. of Health and Human Services (HHS) take effect for most covered health care entities on April 14, 2003. For providers of alcohol and drug treatment services, 42 CFR, chapter 1, part 2 (Confidentiality of Alcohol and Drug Abuse Records) still prevails).

HIPAA Standards for Privacy of Individually Identifiable Health Information:

In general, the federal Standards for Privacy of Individually Identifiable Health Information, also known as the HIPAA Privacy Rule (45 CFR Part 160-164) requires that:

> *An individual patient has a right to a notice as to the uses and disclosures of protected health information that may be made by the covered health care entity; as well as to the individual's rights, and to the covered entity's legal duties with respect to protected health information.*

In general, the content of the notice must contain:

1. A header "THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."
2. A description, including at least one example of the types of uses and disclosures that the covered entity is permitted to make for treatment, payment, and healthcare operations.

3. A description of each of the other purposes for which the covered entity is permitted or required to use or disclose protected health information without the individual's written consent or authorization.
4. A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization.
5. When applicable, separate statements that the covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other continuing care health-related benefits and services that may be of interest to the individual.
6. A statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights including:
    - The right to request restrictions on certain uses and disclosures as provided by 45 CFR 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction
    - The right to receive confidential communications of protected health information as provided by 164.522(b), as applicable
    - The right to inspect and copy protected health information as provided by 164.524
    - The right to amend protected health information as provided in 164.526
    - The right to receive an accounting of disclosures as provided in 164.528
    - The right to obtain a paper copy of the notice upon request as provided in 164.520
7. A statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with a notice of its legal duties and privacy practices with respect to protected health information.
8. A statement that the covered entity is required to abide by the terms of the notice currently in effect.
9. A statement that the covered entity reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains.
10. A statement describing how it will provide individuals with a revised notice.
11. A statement that individuals may complain to the covered entity and to the Secretary of Health and Human Services if they believe their privacy rights have been violated; a brief description as to how one files a complaint with the covered entity; and a statement that the individual will not be retaliated against for filing a complaint.
12. The name or title, and telephone number of a person or office to contact for further information.
13. An effective date, which may not be earlier than the date on which the notice is printed or otherwise published.

In the preamble to the August 14, 2002, final rule, the government encourages the use of a "layered notice." A layered notice consist of a short notice that briefly summarizes the individual's rights and other information, followed by a longer notice layered beneath that explains all the required notice elements.

A covered healthcare entity that is required to have a notice may not use or disclose protected health information in a manner inconsistent with such notice.

A covered healthcare provider with a direct treatment relationship with an individual must:

- Provide the notice no later than the date of the first service delivery, including service delivered electronically, or in an emergency treatment situation, as soon as reasonably practicable after the emergency situation;
- Have the notice available at the service delivery site for individuals to request and take with them;
- Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered healthcare provider to be able to read the notice.

Except in an emergency situation, the covered entity must make a good faith effort to obtain written acknowledgement of receipt of the notice. If it is not obtained, document the good faith effort and the reason why the acknowledgement was not obtained. If the notice is mailed, along with an acknowledgement form, the covered entity is not required to follow up to ensure the individual returns the acknowledgement form.

A covered healthcare entity that maintains a Web site that provides information about the covered entity's customer services or benefits must prominently post its notice on its Web site.

The covered entity may provide the notice by e-mail if the individual agrees and agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual.

According to the August 14, 2002 final rule preamble, the Department of Health and Human Services believes that providers who provide notices electronically should be capable of capturing the individual's acknowledgement of receipt electronically in response to that transmission. The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

A covered healthcare entity must document compliance with the notice requirements by retaining copies of the notices issued and acknowledgements received.

Confidentiality of Drug and Alcohol Patient Records per 42 CFR, Chapter 1, Part 2: The Confidentiality of Alcohol and Drug Abuse Patient Records rules (42 CFR, Chapter 1, Part 2)

establish the following notice provisions for patients of federally assisted drug or alcohol abuse programs:

At the time of admission or as soon thereafter as the patient is capable of rational communication, each substance abuse program shall communicate to the patient that federal law and regulations protect the confidentiality of alcohol and drug abuse patient records. The program must also provide the patient with a written summary of the federal law and regulations. The written summary of the federal law and regulations must include:

- A general description of the limited circumstances under which a program may acknowledge that an individual is present at a facility or disclose outside the program information identifying a patient as an alcohol or drug abuser.
- A statement that violation of the federal law and regulations by a program is a crime and that suspected violations may be reported to appropriate authorities in accordance with these regulations.
- A statement that information related to a patient's commission of a crime on the premises of the program or against personnel of the program is not protected.
- A statement that reports of suspected child abuse and neglect made under State law to appropriate State or local authorities are not protected.
- A citation to the federal law and regulations.

The program may devise its own notice or use the attached sample notice. In addition, the program may include in the written summary information concerning State law and any program policy not inconsistent with State and federal law on the subject of confidentiality of alcohol and drug abuse patient records.

State Requirements:

Some states have laws or regulations and provide specific requirements for a notice of health information practices.

Privacy Recommendations:

1. Identify applicable notice requirements in both federal and state law.
2. Collect sample notices from associations and other organizations.
3. Identify the way information is used and disclosed in your organization.
4. Decide whether your organization will participate in an organized healthcare arrangement.
5. Assign an individual or department to serve as an initial point of contact for individuals requesting additional information or who would like to file a complaint relative to information privacy practices.
6. Decide how material changes in the notice will be communicated.

7. Although not a required element, consider providing space on the notice to allow an individual to request a restriction to the uses and disclosures of his or her health information.
8. Decide whether your organization will provide space for the acknowledgement on the notice or on a separate form.
9. Draft a notice that complies with federal and state law and regulations and accurately describes your organization's health information practices. (Although models are helpful, they cannot be used without adapting them to reflect actual practices in your organization.)
10. Decide whether to place a copy of the current notice in the individual's record with the individual's acknowledgement or simply to maintain a copy of each version of the notice with the dates it was in effect in a separate file.
11. Ask legal counsel to help develop or review the notice.
12. Generate policies and procedures relative to the notice.
13. Educate and train staff.
14. Post the notice and make copies available for distribution where notice acknowledgements are obtained.
15. Implement and monitor compliance.
16. Prior to making material changes in information practices, generate a new notice and provide that new notice to individuals about whom protected health information is maintained.

HIPAA Security Standards:

Under the final HIPAA security standards published in February, 2003: health insurers, certain health care providers and health care clearinghouses must establish procedures and mechanisms to protect the confidentiality, integrity and availability of electronic protected health information. The rule requires covered entities to implement administrative, physical and technical safeguards to protect electronic protected health information in their care.

The new security standards work in concert with the final privacy standards adopted by HHS. The two sets of standards use many of the same terms and definitions in order to make it easier for covered entities to comply.

Covered healthcare entities must comply with the security standards by April 21, 2005. Small health plans have an additional year to comply.

HIPAA – Accounting of Disclosures of Protected Health Information

AMS in abiding by HIPAA Standards for Privacy of Individually Identifiable Health Information (45 CFR Parts 160 and 164), will keep an accounting of disclosures of protected health information made by this organization **except for disclosures to carry out treatment, payment**

and health care operations. (See accompanying attachment excerpted from HIPAA Privacy Regulation Text, Section 164.528 "Accounting of disclosures of protected health information")

In most cases, a specified authorization, signed by the patient, approving release of Alcohol and Drug Abuse Records (per 42 CFR, Chapter 1, Part 2) is the recommended avenue to be utilized for disclosure of Protected Health Information (PHI).

- A disclosure log will be maintained in each patient record.
- The accompanying example **"Accounting Record of Accesses to Patient Protected Health Information (PHI) for Reasons Unrelated to Treatment, Payment or Healthcare Operations (Non TPO Disclosures)"** may be used for this purpose.
- The log will describe:
  - Date of Access
  - Name of person who accessed the Chart
  - Who (specifically) the PHI was released to
  - Patient Name (top of log is sufficient)
  - Reason for the Disclosure
  - What specific PHI was disclosed
- If a specified Consent is utilized for release of information for TPO, the original is placed in the chart.

Refer to Section 2.1 of the Forms Appendix for the "Accounting Record of Accesses to Patient Protected Health Information (PHI)" form.

HIPAA – Excerpts from Privacy Regulations
§164.528 Accounting of disclosures of protected health information.

A. Standard: right to an accounting of disclosures of protected health information.
   1. An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six yeAMS prior to the date on which the accounting is requested, except for disclosures:
      a. To carry out treatment, payment and health care operations as provided in §164.506 (see below);
      b. To individuals of protected health information about them as provided in §164.502;
      c. Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;
      d. Pursuant to an authorization as provided in §164.508 (see below);
      e. For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in §164.510;
      f. For national security or intelligence purposes as provided in §164.512(k)(2);

g. To correctional institutions or law enforcement officials as provided in §164.512(k)(5);

h. As part of a limited data set in accordance with §164.514(e); or

i. That occurred prior to the compliance date for the covered entity (April 14, 2003).

2. a. The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

b. If the agency or official statement in paragraph (A)(2)(i) of this section is made orally, the covered entity must:

1. Document the statement, including the identity of the agency or official making the statement;

§164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

A. Standard: Permitted uses and disclosures. Except with respect to uses or disclosures that require an authorization under §164.508(a) (2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

B. Standard: Consent for uses and disclosures permitted.

1. A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment or health care operations.

2. Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under §164.508, is required or when another condition must be met for such use or disclosure to be permissible under this subpart.

C. Implementation specifications:

Treatment, payment or health care operations.

1. A covered entity may use or disclose protected health information for its own treatment, payment or health care operations.

2. A covered entity may disclose protected health information for treatment of a health care provider.

3. A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.

4. A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who

is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is

a. For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or

b. For the purpose of health care fraud and abuse detection or compliance. (5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

§164.508 Uses and disclosures for which an authorization is required.

A. Standard: authorizations for uses and disclosures.

1. Authorization required: general rule. Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.
2. Authorization required: psychotherapy notes. Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:
    a. To carry out the following treatment, payment, or health care operations:
        1. Use by the originator of the psychotherapy notes for treatment;
        2. Use or disclosure by the covered entity for its own training progrAMS in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or
        3. Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and
    b. A use or disclosure that is required by §164.502(a)(2)(ii) or permitted by §164.512(a); §164.512(d) with respect to the oversight of the originator of the psychotherapy notes; §164.512(g)(1); or §164.512(j)(1)(i).
3. Authorization required: Marketing.
    a. Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:
        1. A face-to-face communication made by a covered entity to an individual; or
        2. A promotional gift of nominal value provided by the covered entity.

b. If the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.

B. Implementation specifications: general requirements.

1. Valid authorizations
   a. A valid authorization is a document that meets the requirements in paragraphs (A)(3)(ii), (C)(1), and (C)(2) of this section, as applicable.
   b. A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.
2. Defective authorizations. An authorization is not valid, if the document submitted has any of the following defects:
   a. The expiration date has passed or the expiration event is known by the covered entity to have occurred;
   b. The authorization has not been filled out completely, with respect to an element described by paragraph © of this section, if applicable;
   c. The authorization is known by the covered entity to have been revoked;
   d. The authorization violates paragraph (B)(3) or (4) of this section, if applicable;
   e. Any material information in the authorization is known by the covered entity to be false.
3. Compound authorizations. An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:
   a. An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of protected health information for such research or a consent to participate in such research;
   b. An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;
   c. An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (B)(4) of this section on the provision of one of the authorizations.
4. Prohibition on conditioning of authorizations. A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:
   a. A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;

b. A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

1. The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and
2. The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and

c. A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.

5. Revocation of authorizations. An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:
   a. The covered entity has taken action in reliance thereon; or
   b. If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.
6. Documentation. A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).

C. Implementation specifications: Core elements and requirements.

1 Core elements. A valid authorization under this section must contain at least the following elements:
   a. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
   b. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
   c. The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.
   d. A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
   e. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.
   f. Signature of the individual and date. If a personal representative of the individual signs the authorization, a description of such representative's authority to act for the individual must also be provided.

2. Required statements. In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:
    a. The individual's right to revoke the authorization in writing, and either:
        1. The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or
        2. To the extent that the information in paragraph ©(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.
    b. The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:
        1. The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or
        2. The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (B)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.
    c. The potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer be protected by this subpart.
3. Plain language requirement. The authorization must be written in plain language.
4. Copy to the individual. If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

HIPAA Definitions

Treatment means 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.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination or analysis of such information within an entity that maintains such information.

Payment means:

A. The activities undertaken by:
    1. A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
    2. A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and
B. The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

1. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
2. Risk adjusting amounts due based on enrollee health status and demographic characteristics;
3. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
4. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
5. Utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services; and
6. Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
    a. Name and address;
    b. Date of birth;
    c. Social security number;
    d. Payment history;
    e. Account number; and
    f. Name and address of the health care provider and/or health plan.

Health Care Operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

A. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable 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 of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

B. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan 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;

C. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable;

D. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

E. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

F. Business management and general administrative activities of the entity, including, but not limited to:

1. Management activities relating to implementation of and compliance with the requirements of this subchapter;
2. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
3. Resolution of internal grievances;
4. The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
5. Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Health Oversight Agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

HIPAA – Business Associate Agreement

In complying with HIPAA legislation (45 CFR, parts 160 and 164). AMS requires that all Business Associates appropriately safeguard Protected Health Information (PHI) made available to or obtained by the Business Associate.

Procedure

To determine whether an organization is a "Business Associate" as defined by HIPAA legislation, use the following steps in this "Checklist for Business Associate Agreements":

To find out whether organizations are your business associates by following these steps:

1. Check the boxes below that apply to each of the outside entities with which you do business:

   ☐ It performs services for, or on behalf of, your facility

   ☐ Your Clinic discloses protected health information (PHI) to it

If BOTH boxes are NOT checked, the affiliate is NOT your business associate. If both boxes ARE checked, move to Step 2.

2. Check the boxes below that apply to each of the outside entities and / or your relationship with them, as identified in Step 1 above:

   ☐ It is receiving PHI in order to provide treatment to the patient

   ☐ It is a financial institution processing consumer-related transactions for the purpose of paying for health care services

   ☐ Your contract with the entity involves a relationship in which you both participate in an organized health care arrangement or in which you're both in an affiliated arrangement.

If you've checked ANY of the boxes above, then the organization is NOT your Business Associate. If NONE of the boxes are checked, then the organization IS your Business Associate, and you should enter into a Business Associate agreement on or before April 14, 2003. If this agreement is in addition to another contract or agreement, that should be stated in the cover letter. The cover letter should also state that in addition to the HIPAA requirements of 45 CFR, the requirements of 42 CFR Part 2 (Confidentiality of Alcohol and Drug Abuse Records) must also be maintained.

HIPAA – Posting Notice of Health Information Practices

It is policy of this organization to publicly post a "Notice of Health Information Practices" at all Facilities and Programs and to furnish a copy of this notice to the persons served (patients).

By April 14, 2003, pursuant to 45 CFR, Parts 160 and 164, also known as the Health Insurance Portability and Accountability Act, all Facilities and Programs must:

- Post in a conspicuous public place, the following attached "Notice of Health Information Practices"

- Furnish a copy of this notice to all patients served that explains:
  - The Patient Health Information Rights and
  - Our responsibilities under the HIPAA Standards for Privacy of Individually Identifiable Health Information
  - How to report a problem regarding the privacy of health information

HIPAA – Notice of Health Information Practices
THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY. EFFECTIVE DATE: APRIL 14, 2003

Understanding Your Health Record / Information

Each time you visit a health care facility, physician, or other healthcare provider, a record of your visit is made. Typically, this record contains information about your health history, symptoms, examination and test results, diagnoses, treatment, and a plan for future care or treatment. This information, often referred to as your patient or medical record, serves as a:

- Basis for planning your care and treatment
- Means of communication among the many health professionals who contribute to your care
- Legal document describing the care you received
- Means by which you or a third party payer can verify that services billed were actually provided
- A tool in educating health professionals;
- A source of data for medical research;
- A source of information for public health officials charged with improving the health of the nation;
- A source of data for facility planning and marketing and
- A tool with which we can assess and continually work to improve the care we render and the outcomes we achieve

Understanding what is in your record and how your health information is used helps you to:

- Ensure its accuracy

- Better understand who, what, when, where and why others may access your health information
- Make more informed decisions when authorizing disclosure to others

Your Health Information Rights:

Although your health record is the physical property of the healthcare practitioner or facility that compiled it, the information belongs to you. You have the right to:

- Request a restriction on certain uses and disclosures of your information as provided by 45 CFR 164.522 and 42 CFR, Chapter 1, Part 2
- Obtain a paper copy of the notice of information practices upon request
- Inspect and copy your health record as provided for in 45 CFR 164.524
- Amend your health record as provided in 45 CFR 164.528
- Obtain an accounting of disclosures of your health information as provided in 45 CFR 164.528
- Request communications of your health information by alternative means or at alternative locations
- Revoke your authorization to use or disclose health information except to the extent that action has already been taken

Our Responsibilities: This organization is required to:

- Maintain the privacy of your health information
- Provide you with a notice as to our legal duties and privacy practices with respect to information we collect and maintain about you
- Abide by the terms of this notice
- Notify you if we are unable to agree to a requested restriction
- Accommodate reasonable request you may have to communicate personal health information by alternative means or at alternative locations

We reserve the right to change our practices and to make the new provisions effective for all protected health information we maintain. Should our information practices change, we will mail a revised notice to the address you've supplied us.

We will not use or disclose your health information without your authorization, except as described in this notice.

For More Information or to Report a Problem

If you have questions and would like additional information, you may contact the Compliance Officer (Paul D. Cassidy) at: 850-723-7703.

If you believe your privacy rights have been violated, you can file a complaint with the Dept. of Health and Human Services / Office for Civil Rights by email at ocrcomplaint@hhs.gov or by calling the national Office at asking for the OCR Health Information Privacy Complaint Form and / or for the appropriate Regional OCR Office. There will be no retaliation for filing a complaint. 1-800-368-1019

Examples of Disclosures for Treatment, Payment and Health Operations

We will use your health information for treatment. For example: Information obtained by a counselor, physician, nurse or other member of your treatment care team will be recorded in your record and used to determine the course of treatment that should work best for you.

With your consent, we also provide your physician or a subsequent healthcare provider with copies of various reports that should assist him / her in treating you once you are discharged from this program.

With your consent, we will use your health information for payment. For example: A bill may be sent to you or a third party payer. The information on or accompanying the bill may include information that identifies you, as well as your diagnosis and descriptions of treatment methods and procedures used.

We will use your health information for regular, internal health operations. For example: members of the treatment staff, the utilization review coordinator, the quality improvement manager, or members of the quality improvement team may use information in your health record to assess the care and outcomes in your case and others like it. This information will then be used in an effort to continually improve the quality and effectiveness of the treatment and service we provide.

Other Uses or Disclosures

Business Associates: There are some services provided in our organization through contacts with business associates. Examples include care by external physicians (in the event urgent or emergency care is needed), pharmacy services (filling prescriptions), and laboratory teAMS. When these services are contracted, we may disclose your health information to our business associate so that they can perform the job we've asked them to do and bill for services rendered. So that your health information is protected, however, we require business associates to appropriately safeguard your information.

Notification: With your prior consent, in the event of an emergency or crisis, we may use or disclose your personal information to notify or assist in notifying a family member, personal representative, or another person that you designate as responsible for your continued care, your location, and general condition.

Communication with Family: With your consent, this program’s treatment personnel, using their best judgment, may disclose to a family member, other relative, close personal friend or other significant person that you identify, your personal health information that is relevant to that person's involvement in your care – or for payment needs related to your care. Un-emancipated Minor: if, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, this

organization's treatment representative may disclose and provide access to protected health information about the un-emancipated minor to the parent or legal guardian, or other person acting in loco parentis.

Research: With your consent, we may disclose information to researchers when their research has been approved by an Institutional Review Board, which has reviewed the research proposal and has established specific protocols to ensure the confidentiality of your health information.

Continuing Care and / or Marketing: With your prior consent, we may contact you to provide appointment reminders or information about continuing care or other related benefits and services that may be of interest to you.

Food and Drug Administration (FDA): We may disclose to the FDA health information relative to adverse events with respect to food, supplements, product and product defects or other information to enable the FDA to notify patients and physicians about emerging dangers.

Disability Insurance and Workers Compensation: With your consent, we may disclose the minimum health information needed to the extent authorized by and to the extent necessary to comply with laws relating to disability and workers compensation or other similar programs established by law.

Public Health: With your consent and if required by law, we may disclose the minimum necessary health information to public health or legal authorities charged with preventing or controlling disease, injury or disability.

Law Enforcement: We may disclose health information for law enforcement per 42 CFR: Chapter 1, Part 2 (see Notice of "Confidentiality of Alcohol and Drug Abuse Patient Records")

Federal law makes provision for your health information to be released to an appropriate health oversight agency, public health authority or attorney, provided that a workforce member or business associate believes in good faith that we have engaged in unlawful conduct or have otherwise violated professional or clinical standards and are potentially endangering you or patients, workers or the public. In this case, a court order is required per 42 CFR, Chapter 1, Part 2.

This organization reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. Revisions of this notice will be posted at this location.

Reference: Health Insurance Portability and Accountability Act (45 CFR Part 160-164) HIPAA Privacy Rule – Standards for Privacy of Individually Identifiable Health Information Adapted from the American Health Information Management Association Practice Brief, "Notice of Information Practices" (Updated November 2002); and 42 CRF, Chapter 1, Part 2: Confidentiality of Alcohol and Drug Abuse Patient Records

<u>HIPAA – Confidentiality of Alcohol and Drug Abuse Patient Records</u>
Per 42 CFR, Chapter 1, Part 2

The confidentiality of alcohol and drug abuse patient records maintained by this program is protected by federal law and regulations. Generally, the program may not say to a person outside the program that a patient attends the program, or disclose any information identifying a patient as an alcohol or drug abuser unless:

1. The patient consents in writing;
2. The disclosure is allowed by a court order; or
3. The disclosure is made to medical personnel in a medical emergency or to designated and qualified staff for research, audit, or program evaluation

Violation of the federal law and regulations by a program is a crime. Suspected violations may be reported to appropriate authorities in accordance with federal regulations.

Federal law and regulations do not protect any information about a crime committed by a patient either at the program or against any person who works for the program or about any threat to commit such a crime.

Federal laws and regulations do not protect any information about suspected child abuse or neglect from being reported under State law to appropriate state or local authorities.

<u>HIPAA – Confidentiality and Security for Protected Health Information (PHI)</u>
Each AMS Clinic / Facility will document that it has established HIPAA compliant policies and procedures per 45 CRF, Parts 160 and 164; as well as maintain the confidentiality of Alcohol and Drug Abuse Patient Records per 42 CFR, Chapter 1 Part 2.

The Clinic / Facility will designate responsibility for the confidentiality and security for PHI by assigning an individual or organizational group to accomplish the following functions (also see attached: AMS HIPAA Facility Privacy Checklist):

- Provide internal leadership for the facility's overall privacy and security of PHI
- Implement controlling policies and procedures for who has information access to PHI
- Have mechanisms in place for information authorization practices, controls and internal audits of access to PHI
- Establish and monitor Business Associate Agreements for all active business associates
- Documenting procedures for processing, storing, retrieving and destroying all records that contain PHI
- Maintaining secure and private workplace and workstation locations to prevent unauthorized leakage or access to PHI
- Providing physical access controls for security of PHI
- Enforce personnel disciplinary procedures for privacy and security breaches and for protection of the integrity of PHI when personnel terminate employment

- Provide ongoing education and training on privacy and security of PHI

HIPAA – Employee Awareness and Training Regarding Protected Health Information (PHI)
It is the policy of AMS that all Clinics and Facilities will operationalize and provide for employee compliance awareness and training under the HIPAA Privacy and Security Standards (45 CRF, Parts 160 and 164) for Protected Health Information (PHI) and the Federal Confidentiality Requirements for Alcohol and Drug Abuse Patient Records (42 CFR, Chapter 1, Part 2).

The Privacy Standards for HIPAA (45 CRF, Parts 160 and 164) take effect April 14, 2003. The Federal Confidentiality Requirements for Alcohol and Drug Abuse Patient Records (42 CFR, Chapter 1, Part 2) have been an ongoing practice.

Each clinic or facility may provide compliance awareness and training that fits the program orientation and the state regulatory environment in which it operates. However, the following points on confidentiality, privacy and security of Protected Health Information should be closely adhered to:

- All new employees will receive the facility-appropriate education and training regarding 45 CRF, Parts 160 and 164; and 42 CFR, Chapter 1, Part 2. AMS supplied documents (attached) may be used for this purpose.
  - The entire text for HIPAA Privacy Rules 45 CRF, Parts 160 and 164 is available at: http://www.hhs.gov/ocr/combinedregtext.pdf
  - The entire text for Federal Confidentiality Laws for Alcohol and Drug Records (42 CFR, Chapter 1, Part 2) is at: http://www.access.gpo.gov/nara/cfr/waisidx_00/42cfr2_00.html

- Upon receiving education and training in confidentiality and privacy of PHI, each employee will sign a "Confidentiality and Security Agreement" as a condition of employment with the Clinic or Facility (see sample form).

- All employees of the Clinic or Facility will receive ongoing educational and training updates when appropriate, but at least on a yearly basis.

Refer to Section 2.1 of the Forms Appendix for the "Employee Security and Confidentiality Agreement for Protected Health Information (PHI)" form.

HIPAA – Privacy Compliance
Implementing the Minimum Necessary Standard

The minimum necessary standard in HIPAA's privacy rule requires that covered health care entities make reasonable efforts to limit protected health information (PHI) to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

The challenge with implementing the minimum necessary standard is defining what is "reasonably necessary" and in determining how “minimum necessary” uses, disclosures, and requests will be managed in both the non-automated and automated worlds.

HIPAA - Regulatory Requirements

For the minimum necessary standard, the privacy rule requires that the covered health care provider identify:

1. Persons or classes of persons in its work force who need access to Personal Health Information (PHI)
2. Categories of PHI to which access is needed,
3. What conditions are appropriate to in order to gain access

This constitutes the requirements for ensuring minimum necessary use. For **routine and recurring disclosures**, the rule requires the covered entity implement standard protocols that limit the disclosures to the amount reasonably necessary to achieve the purpose of the disclosures. For all **other disclosures**, the covered entity must develop criteria designed to limit the PHI disclosed to the minimum necessary. In both cases, where patient alcohol and drug treatment records are concerned, the long-standing 42 CFR, Chapter 1, Part 2, usually prevails. Under HIPAA, all covered health providers and plans (entities) must also limit any **request** they make for PHI to that which is reasonably necessary.

The HIPAA “minimum necessary” standard does not apply to disclosures to or requests by a healthcare provider for treatment, uses, or disclosures made:

- To the individual patient
- By direct, specific authorization of the individual
- To the Secretary of the Department of Health and Human Services (HHS) for compliance enforcement

The minimum necessary standard is also distinguished from the confidential communication standard, which permits patients to ask that confidential communications be handled in alternative locations or by alternative means. Confidential communications pertain to discussions and other communications with patients or other members of the work force about treatment and is designed to keep legitimate communications from being overheard or seen by those without authority to have such information.

HIPAA - Achieving and Monitoring Adherence

Once policies and procedures to ensure minimum necessary uses and disclosures have been established, the covered entity must make reasonable efforts to limit the use of PHI in accordance with those policies and procedures. This ongoing monitoring of compliance will require training and regular compliance monitoring.

Staff whose job functions involve the use of PHI should be taught how to adhere to the minimum necessary standard. While the minimum necessary principles can certainly be taught generically to all PHI users, it is probably best to blend this training into the job-specific training that the privacy rule requires. In other words, staff members who use PHI as part of their jobs should be taught what specific information they may access as part of their assigned duties and that they should not be reviewing or using other parts of the patient's medical record or other patients' records if they do not need to.

To ensure compliance with the minimum necessary requirements, internal auditors, corporate compliance officers, or others may establish ongoing monitoring (such as audit trails), periodic checking on particularly vulnerable areas (such as all requests for entire medical record), and triggered reviews when there are special complaints or incidents. This compliance process would result in feedback to members of the work force on areas needing more attention and may necessitate the redesign of work processes or procedures to enhance compliance.

HIPAA - Minimum Necessary Uses

HIPAA - Paper-based Environment

Because most covered entities are still very much in a paper-based environment, special challenges exist in applying the minimum necessary standard to uses in this environment. There is no technology to automatically apply decision rules when accessing a paper chart, billing record, or the many other paper documents containing PHI. Instead, users of paper-based PHI will rely more heavily on the application and interpretation of policies and procedures, and even self-policing. As a result, the development of policies and procedures to appropriately restrict the use of PHI and the need to train staff in those policies and procedures take on special importance for covered entities maintaining PHI on paper. In dealing with alcohol and drug records, 42 CFR (chapter 1, part 2), again takes precedence.

HIPAA - Automated Environment

While not directly referring to information access controls, the minimum necessary use part of HIPAA's minimum necessary standard can be supported in an automated environment by formal information access controls. Many covered entities are planning to adopt Role-Based Access Controls (RBAC) that permit only people in certain roles to access certain types of information. For example, the billing clerk may access a patient's contract and billing information but not medical history; the treating physician, on the other hand, has full access to the patient's medical history and subsequent treatment records.

Information access controls are addressed in HIPAA's Security Rule. Information authorization, establishment, modification, and termination policies and procedures are required. These would require that a supervisor or manager specifically authorize access for a person needing to use PHI, that the person's identity is validated when access privileges are established, that when the person's job changes access privileges are modified accordingly, and that the account is removed when the person terminates.

The proposed security rule affords the covered entity a choice as to the access control model to be used. The three models include User-Based Access Controls (UBAC) in which users must authenticate themselves but there are no constraints on what may be accessed; RBAC in which conditions of access are placed on classes of users (as described below); and Context-Based Access Controls (CBAC), which limit users to accessing information not only in accordance with their identity and role, but to the location and time in which they are accessing the information. Although the security rule provides these options, the Dept. of HHS espouses RBAC as the appropriate security model to safeguard health data.[1]

Further supporting RBAC is the requirement for a procedure for emergency access (sometimes referred to as "break the glass" access). This procedure is typically found in RBAC and CBAC in order to ensure that a person with limited access who has a need to know in an emergency situation can easily access required information. There is generally a special audit function associated with this emergency access that notifies the person's supervisor, the patient's attending physician, or other individual with designated authority to review such accesses for their applicability.

Access controls are linked to the person's unique user identification and password or other form of "entity authentication."

HIPAA - Policies and Procedures Needed

Constructing policies and procedures (and RBAC) to establish minimum necessary uses must identify the persons, or classes of persons, who need access to PHI to carry out their jobs:

- Start by working with each department/unit of the covered entity to examine how members of the work force currently use PHI
- Document the list of people (or job categories) that require access to PHI and the purposes and conditions under which PHI is needed. Some covered entities are documenting this using a grid approach:
  - list all categories of workers on one axis
  - list categories of PHI on the other axis
  - make check boxes and notes regarding special conditions in each cell where those members of the work force need access to specified categories of PHI
- Determine if it would be reasonably possible to achieve the same result with de-identified data. If so, using de-identified data is the preferred strategy. If not, determine the specific PHI needed by each type of member of the work force
- Compare findings of what information is currently made available to the various members of the work force with what they need to know. Do they have access to more health information than they really require? If so, is it reasonably possible to segregate the needed information in a way that gives them only what they need? It may not always be possible or feasible to "strip out" all extraneous health information beyond what is needed. The covered entity's goal, however, should be to restrict access to what is needed, insofar as it is reasonably possible.

Note that once you have performed this exercise, you actually have both the foundation for the minimum necessary policy and procedure as well as the role definitions required for RBAC that can be applied to computerized PHI.

Example: Consider an external recovery home representative/ “business partner” who examines patient records on the inpatient/ residential unit as part of evaluating the patient for possible placement in a long-term sober living facility. Using the minimum necessary principles, the covered healthcare entity/facility would determine what information the recovery home representative needs in order to perform this function.

For this function, the recovery home may need access to information about the patient's current condition, needs for long-term support, basic demographic information, and insurance/financial

resources. The covered clinic / facility determines that de-identified data would not meet the needs of this recovery home representative.

The covered entity then compares these needs to the information to which the recovery home representative currently has access to the patient's the entire medical record. The privacy- trained personnel at the facility then analyze whether it is reasonably possible to limit this outside representative to only a subset of the record. It may be determined that in the paper-based environment, it is not practical to remove certain subsets of information from the record; but it may be feasible to give the minimum necessary info via a private verbal report to the recovery home representative.

The facility could use the results of the analysis to write a policy for all recovery home representatives that defines what information from the patient record they may ordinarily use in performing this placement function. All recovery home representatives would then adhere to these policies and avoid reviewing Personal Health Information that is out of the scope of the function being performed.

Covered entities have the latitude to define and interpret these policies and procedures to meet their particular needs. As the Dept. of HHS notes in its guidance on this subject, these policies and procedures should take professional judgment into account and not sacrifice quality of care in favor of iron-clad policies and procedures.[2]

Covered entities must balance a respect for the privacy rights of their patients with what is reasonably
possible to do, given the organization's resources and limitations.

HIPAA - Minimum Necessary Disclosures and Requests

Disclosure of PHI is different from use of health information. HIPAA defines disclosure as the "release, transfer, provision of access to, or divulging in any other manner PHI outside the entity (facility/organization) holding the information." In comparison, HIPAA distinguishes use as the "sharing, employment, application, utilization, examination, or analysis of PHI within an entity that maintains such information."

Minimum necessary disclosures to or requests from other organizations are also distinguished by their being routine or not routine. Routine disclosures are those made on a recurring basis. For example, a pharmacy may routinely be given a copy of the patient's demographic and insurance information for the medication billing purposes. Non-routine disclosures are those that are made only occasionally, such as to a licensing official investigating a complaint.

HIPAA - Developing Standard Protocols for Routine Disclosures

For consented disclosures made on a routine or recurring basis, a covered entity must implement policies and procedures (that may be standard protocols) that limit the protected information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. These policies and procedures should be designed to balance an individual's privacy against the legitimate need for information requested by the outside entity.

To comply with this requirement, each covered entity should review the requests it routinely receives and determine the appropriate information to be disclosed in response to the request. In

developing policies and procedures or standard protocols for routine disclosures, covered entities should consider discussing this issue with their major requesters to negotiate mutually agreeable disclosures.

If a requester asks for specific information (i.e., the physician's medical exam on the patient performed on a specified date), only the information requested should be disclosed. A standard set of reports should not be disclosed in response to a request for a specified report.

Broadly stated request (i.e., request asking for "any and all records") should be reviewed with the requester to determine the specific information needed. Many requesters who ask for "any and all" records will reduce the amount of information requested when appraised of the HIPAA privacy rules, and the amount of the copy fees for these records.

HIPAA - Criteria for Making Non-Routine Disclosures

For non-routine disclosures, a covered entity must develop criteria to limit the protected information disclosed to what is reasonably needed to accomplish the purpose of the disclosure.

It is impossible to assign scientific methodology to evaluating disclosures. Non-routine request must be reviewed against these criteria on an individual, case-by-case basis. The criteria need to be balanced against each other. For example, if there is knowledge that the individual could be significantly harmed by a disclosure but the provider may not get reimbursed for the care, consider alternatives such as discussing alternative payment arrangements with the patient.

HIPAA - Screening Request from Other Covered Entities

Under the privacy regulations, covered health entities are required to limit their request to the minimum amount of information needed to accomplish the intended purpose. Thus, one covered entity is not required to monitor the request received from another covered entity to ensure compliance. However, the disclosing entity should require supporting documentation for any request made by another covered entity that would involve disclosure of a complete medical record, or for any disclosure that does not appear reasonable under the circumstances.

Covered entities may also rely on a requested disclosure as the minimum necessary for the stated purpose when making disclosures to public officials. The covered entity should verify the identity of such a person.

Limiting the decision making to individuals well trained in health information management promotes professional judgment and consistency. While qualified personnel should be able to apply institutionally agreed upon criteria to most disclosure request, in some cases it may be best to discuss specifics with the patient's attending physician and/or case manager and to seek further representations of need to know from the person requesting the patient's PHI.

HIPAA - Disclosure of an Entire Medical Record

In compliance with the HIPAA regulations, a covered entity may not use, disclose, or request an entire medical record, except where the entire medical record is specifically justified as the amount reasonably necessary to accomplish the purpose.

HIPAA - Re-disclosure of Health Information

One of the sample criteria is the likelihood of re-disclosure. A healthcare provider's records may contain information about a patient from another healthcare provider's records. Such information may be sent with a patient who is transferred or referred to a facility for definitive treatment or continuing care.

Issues often arise regarding re-disclosure of information from other healthcare providers. Unless otherwise required by state law or regulation, the following is recommended:

- Under 42 CFR, chapter 1, part 2, a provider may not re-disclose health information from another provider, unless a medical emergency exiAMS and the PHI is needed for the patient's continuing treatment. Otherwise, a separate specified release should be signed by the patient and be sent to the previous provider.
- If a patient requests access to health information that was obtained from another medical provider, it may be disclosed to the patient upon written request and following the HIPAA requirements for granting access to PHI. However, highly confidential alcohol and drug abuse records and/or psychotherapy notes obtained from another provider should be excluded, with direction given to the patient to contact that provider directly to view, copy or amend those records originating from outside the facility.
- Unless otherwise required by law, generally no other re-disclosures should be made. In response to a court order or other 42 CFR approved request for confidential alcohol and drug abuse records, the healthcare provider should not disclose information from another provider, with the exception of outside test results that were ordered by the facility (such as from a contracting reference laboratory) that have been made part of the patient's record.

Notes:

1. When responding to questions on access controls, HHS refers visitors to its Web site to the National Institute of Standards and Technology (NIST) publication NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, Chapter 17, "Logical Access Control."

2. According to HHS, "This is not a strict standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers today to limit the unnecessary sharing of medical information." More information is available on the HHS Office for Civil Rights Web site at http://www.hhs.gov/ocr/hipaa/

Adapted from: Journal of AHIMA 73, no.9 (2002): 96A-F. Amatayakul, Margaret; Brandt, Mary D.; and Dennis, Jill Callahan. "Implementing the Minimum Necessary Standard (AHIMA Practice Brief)."

HIPAA – Patient Right To Access, Inspect and Obtain Copies of Their Records

It is the policy of this organization that its patients have a right to access, inspect and obtain a copy of their protected health information as contained in their designated records, for as long as such records are maintained by the facility or program. This right is conditioned by and pursuant to: HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 CFR, Part 164.524: Access of Individuals to Protected Health Information.

If any patient requeAMS to access, see and / or obtain a copy of his / her protected health information. The following general guidelines and procedures are to be followed:

1. The patient will be instructed sign a written release of records to him or her self, which will be placed in the patient's record to serve as documentation of the request.
2. The patient will be informed that--per 45 CFR, Part 2, Section 164.52--that access to the record will be granted within 30 days of the receipt of the written request; unless the record is stored off site. If stored off site, the record will be obtained for inspection within 60 days of the receipt of the written request.
3. Fee for copying: the patient will be informed that a reasonable, cost-based fee may be incurred by the patient to cover the cost of copying labor and supplies, and for postage or delivery charges if patient requeAMS this service.
4. Denial of access: patient will be informed that access to and review or copying records will be denied without opportunity for review / appeal if:
    A. the clinic or facility or its personnel are aware of, or reasonably anticipate, that the protected health information in the patient record may be compiled for a civil, criminal, or administrative action or proceeding;
    B. the protected health information in the record was obtained from someone other than a health care provider under a promise of confidentiality, and access would then be reasonably likely to reveal the source of the information;

C. the record contained information that is construed as being psychotherapy

5. Reviewable / appealable grounds for denial: patient will be informed that access to and review or copying records can be denied, but with opportunity for review appeal if:

   A. the clinic or facility-based health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the requesting individual, or of another individual;

   B. the confidential information in the record makes reference to another person (unless such person is a health care provider) and the facility's staff has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

   C. the request to access the record is made by the patient's personal representative (such as a parent or guardian) and the clinic / facility's staff determine, in their profession judgment, that such personal representative is reasonably likely to cause substantial harm to the patient or another person as a result of seeing the protected information in the record.

6. Review / appeal of a denial to access: if denial is based on the reasons listed in #5. (A)-(C), above, the patient or personal representative has the right to have the denial reviewed by a licensed health care professional who is designated by the facility to act as a reviewing official and who did not participate in the original decision to deny. This designated reviewing official must determine, within a reasonable period of time, whether or not to deny follow up access based on the standards listed in # 5, as previously cited. The reviewing official must promptly provide written notice to the patient of the official determination as to whether continued denial is reasonable or access to the record is to be subsequently granted.

7. The patient has the right to amend protected health information in his / her record if such request is made in writing to the facility / keeper of the record. The procedure for accepting or denying such amendments is delineated in 45 CFR, section 164.526. (See attachment .1)

8. The clinic / facility must identify and document the names / titles of the persons or offices that are responsible for receiving and processing requests for access to patient records.

HIPAA – Attachment 1 – Patient Right to Amend PHI

From: U.S. Department of Health and Human Services Office for Civil Rights Standards for Privacy of Individually Identifiable Health Information (Unofficial Version) (45 CFR Parts 160 and 164) Regulation Text (December 28, 2000) as amended: Part 160 (May 31, 2002) Parts 160, 164 (August 14, 2002)

§164.526 Amendment of protected health information.

A. Standard: right to amend.

1. Right to amend. An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

2. Denial of amendment. A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

    a. Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

    b. Is not part of the designated record set;

    c. Would not be available for inspection under §164.524; or

    d. Is accurate and complete.

B. Implementation specifications: requests for amendment and timely action.

1. Individual's request for amendment. The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

2. Timely action by the covered entity.

    a. The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

        1. If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (C)(1) and (2) of this section.

        2. If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (D)(1) of this section.

    b. If the covered entity is unable to act on the amendment within the time required by paragraph (B)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

        1. The covered entity, within the time limit set by paragraph (B)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

        2. The covered entity may have only one such extension of time for action on a request for an amendment.

C. Implementation specifications: accepting the amendment. If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

1. Making the amendment. The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.
2. Informing the individual. In accordance with paragraph (B) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (C)(3) of this section.
3. Informing others. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:
    a. Persons identified by the individual as having received protected health information about the individual and needing the amendment; and
    b. Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

D. Implementation specifications: denying the amendment. If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.
1. Denial. The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (B)(2) of this section. The denial must use plain language and contain:
    a. The basis for the denial, in accordance with paragraph (A)(2) of this section;
    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 the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and
    d. A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in §164.530(d) or to the Secretary pursuant to the procedures established in §160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).
2. Statement of disagreement. The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

3. Rebuttal statement. The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.
4. Record keeping. The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.
5. Future disclosures.
    a. If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.
    b. If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (D)(1)(iii) of this section.
    c. When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

E. Implementation specification: actions on notices of amendment. A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (C)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (C)(1) of this section.

F. Implementation specification:

Documentation. A covered entity must document the titles of the persons or offices responsible for receiving and processing requeAMS for amendments by individuals and retain the documentation as required by §164.530(j).

HIPAA – Telefacsimile (Faxes)

AMS will comply with all HIPAA and the Federal Confidentiality rules relevant to the use of faxing, by demonstrating adherence to our organization's intent and duty to preserve the confidentiality and integrity of protected health information as required by law, professional ethics, accreditation and licensing requirements.

Background: Often AMS personnel, and the organizations with which we do business, will have a need to transmit or receive documents (that include protected health information) by fax rather than by a slower, more secure method, such as mail or courier. It is possible that personnel could miss-send faxes to unauthorized recipients, faxes could be intercepted or lost in transmission, or the facility may not receive a fax intended for it because of these or other reasons. Thus, the potential for breach of protected health information (PHI) exists every time someone uses such information. Therefore, all personnel must strictly observe the following procedures relating to facsimile communications of PHI:

Personnel must limit information transmitted to the minimum amount necessary to meet the requester's needs. The facility, its officers, agents and employees will send health information by facsimile only when the original record or mail delivered copies will not adequately meet the needs for timely patient care and efficient business operations. Personnel may transmit health records by facsimile only when directly needed for patient care or as required by a third-party payer for ongoing certification of payment for patient treatment.

Except as authorized by law, a properly completed and signed authorization must be obtained before releasing patient information. Personnel may not send by fax especially sensitive medical information, including, but not limited to, AIDS / HIV information, mental health and developmental disability information, alcohol and drug abuse information, and other sexually transmissible disease information without the specific, express authorization of the patient. The cover page accompanying the facsimile transmission must include a confidentiality notice (See sample).

Fax machines must be in secure areas, and the department director is responsible for limiting access to them. Each department is responsible for ensuring that incoming faxes are properly handled, not left sitting on or near the machine, but rather are distributed to the proper recipient expeditiously while protecting confidentiality during distribution, as by sealing the fax in an envelope.

Personnel must report any misdirected faxes to the facility Privacy Officer. The Department Head will periodically and / or randomly check all fax speed-dial numbers pre-programmed in the dept. fax machine to ensure their validity and accuracy, and to verify authorization to receive confidential information. Users must immediately report violations of this policy to their department head and / or the Privacy Officer as appropriate.

All supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination from employment. Civil and criminal charges / penalties may also ensue.