HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

(HIPAA)

PRIVACY POLICIES IMPLEMENTATION MANUAL

June 27, 2003

TABLE OF CONTENTS

Connecticut DMHAS
Department of Mental Health and Addiction Services
A Healthcare Service Agency

HIPAA OVERVIEW

The Health Insurance Portability and Accountability Act of 1996 (HIPAA,) also known as the Kennedy-Kassebaum bill, has brought many changes to behavioral healthcare. These changes include the ability to move one's health insurance coverage when one moves from one job to the next and the right to continue health insurance coverage after employment has ended. HIPAA has also provided the framework for discussions of parity between mental health insurance and general health insurance benefits.

Congress added an Administrative Simplification section to the bill. The goal of this section is to streamline the healthcare system through the adoption of consistent standards for transmitting uniform electronic healthcare claims. However, in order for this to succeed, it also became necessary to adopt standards for securing the storage of that information and for protecting individual privacy. Ultimately, the healthcare industry will have a standardized way of transmitting electronic claims with increased privacy and security protection for the electronic dissemination of healthcare information.

The HIPAA privacy rule was designed to serve as a minimum level of privacy protection. It is intended to:

1. Protect and enhance the rights of service recipients by providing them access to their health information and controlling the inappropriate use of that information.

2. Improve the quality of healthcare in the United States by restoring trust in the healthcare system among consumers, healthcare professionals, and the multitude of individuals committed to the delivery of care.

3. Improve the efficiency and effectiveness of healthcare delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.

By enacting HIPAA, congress recognized the fact that Administrative Simplification cannot succeed if we do not protect the privacy and confidentiality of personal health information. The provision of high quality healthcare requires the exchange of personal, often-time's sensitive information, between an individual and their healthcare provider. Paramount to that interaction is the patient's ability to trust that the information shared will be protected and kept confidential. However, many service users are still concerned that their information is not protected. Among the factors contributing to this concern are: the growth and number of organizations involved in the provision of care and the processing of claims; the increased use of electronic information technology; increased efforts to market healthcare and other products to consumers; and, the growing ability to collect highly sensitive information about a person's current and future health status.

HIPAA Information Privacy Protections are intended to: give service recipient's appropriate control over and access to their health information; set boundaries on the use and release of health records; safeguard that information; establish accountability for inappropriate use and release; and, balance privacy protections with public safety.

Clearly, the impact of HIPAA is far reaching; it affects each and every DMHAS facility, department, program, employee, volunteer, student, and contractor. As such, a DMHAS Privacy Officer will provide central oversight to the DMHAS, its' state-operated facilities and statewide programs (Agency) HIPAA initiative. Each facility will need to identify a Healthcare Information Specialist to oversee the development, implementation and maintenance of the HIPAA policies and procedures within the individual facilities.

The Agency will achieve and maintain compliance with the HIPAA, as well as all state and federal regulations regarding the uses and disclosures of patient Protected Health Information or PHI, by: complying with all applicable requirements of the Privacy Standards no later than April 14, 2003; keeping records of all PHI disclosures and submit compliance reports as required by the United States Department of Health and Human Services (DHHS); permitting the Secretary of the DHHS access to all facilities, books, records, accounts and other sources of information, including PHI that is pertinent to ascertaining compliance; and, developing procedures to assure compliance with the Privacy Standard's policies based on the *Guidelines For Procedural Development* that are attached to most of the policies.

Furthermore, all members of the Agency's workforce will need to be trained prior to April 14, 2003 on HIPAA awareness and privacy, especially as it relates to the individual facility HIPAA policies and procedures. After April 14th, all new employees will be trained as part of the regular orientation training that is provided to all newly hired DMHAS employees. The individual facility HIPAA policies and procedures will be compiled at the facility level, utilizing this manual as a guide, as it is necessary and appropriate for each facility workforce member to carry out their individual functions within the facilities. As pertinent areas of the HIPAA privacy policies and procedures are updated or modified, mechanisms shall be implemented at the facility level to inform and educate all employees that are impacted by the changes.

This Privacy Manual identifies how to implement a Privacy Program within the Agency based on the application of effective policies, procedures and business service agreements to control the access and use of patient/client PHI.

This Manual is divided into two major areas: *Patient Privacy Rights* and *Uses and Disclosures*. It is understood that many of the required Privacy Policies are currently being performed within the Agency. In most cases, all that is required is documenting that a specific activity has occurred. It is not anticipated that the Agency will have to vastly be reorganized based upon the HIPAA requirements. However, it is expected that certain key activities will need to be performed more consistently.

DMHAS believes that the Privacy Standards of the HIPAA will only improve the quality of care provided to all clients. By adhering to all mandated procedures, staff will be part of the finest *Healthcare Service Agency* in the country.

Connecticut DMHAS
Department of Mental Health and Addiction Services
A Healthcare Service Agency

PATIENT PRIVACY RIGHTS

INTRODUCTION

Since privacy has been a major concern within the mental health and substance abuse fields since their inception, many stringent privacy practices were already in place prior to HIPAA. As a result, implementing the HIPAA privacy requirements should not be too difficult within the DMHAS, its' state-operated facilities and statewide programs (Agency.)

Overall, the HIPAA privacy requirements address several major activities, including basic fundamental patient rights, which for the most part, are currently practiced and embraced within the Agency. Included with this is the belief that it is a good business practice to provide all service recipients with fair notice about how their health information will be used, disclosed and protected.

Patient's rights include the right to:

1. Receive a notice of DMHAS Privacy Practices;
2. Access their medical record to inspect and copy their health record;
3. Request an amendment of their health record;
4. Receive an accounting of disclosures of health information; and,
5. Receive confidential communications.

The Agency views it as a good business practice to allow all service users the opportunity to discuss any concerns related to the privacy of their Protected Health Information or PHI, including the right to access, amend and receive an accounting of their PHI. These are important rights of all clients, the ability to: know what information is kept on them; request an amendment of their medical record, to ensure that the most accurate information is placed in their medical record; and, have an accounting of who has accessed their medical record. These important rights of all clients are essential in maintaining the highest level of client confidentiality and trust.

Patient/Client PHI is not simply limited to information found within their medical record. It also includes any records maintained by the Agency that are identifiable by a patient's information. This includes information within B.H.I.S. and eCura as well as any electronic file such as a Word

document, Excel spreadsheet or an Access database. All patient information that is kept within the Agency ***must*** be treated with the highest level of confidentiality.

Another sound business practice to protect the privacy of all service recipients is to support their right to reasonable accommodations for receiving PHI. This can simply mean, at the patient's request, sending their PHI by alternative means or to an address other than their home address.

Privacy is a fundamental right. As such, it must be viewed quite differently and held to much higher standards. The costs and benefits of a regulation must, of course, be considered as a means of identifying and weighing options. At the same time, it is important not to lose sight of the inherent meaning of the word *privacy*: it speaks to our individual and collective freedom.

PROVISION OF *NOTICE OF PRIVACY PRACTICES* FOR PROTECTED HEALTH INFORMATION

POLICY:

Every individual has a right to adequate notice of the uses and disclosures of Protected Health Information (PHI) that may be made by the Agency and of the individual's rights and the Agency's legal duties with respect to PHI. The Agency shall therefore maintain a distinct *Notice of Privacy Practices* for PHI for Mental Health Programs and a distinct *Notice of Privacy Practices* for PHI for Substance Abuse Programs.

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

Facilities/statewide programs will need to implement procedures by April 14, 2003, that specify how they will provide the *Notice of Privacy Practices* document to newly admitted, as well as existing service users. At a minimum, the procedures should cover the following areas:

1. The point at which clients will be provided with a copy of the *Notice of Privacy Practices* and who will be responsible for reviewing its content with the client and obtaining their signature, acknowledging receipt of the *Notice of Privacy Practices*.
2. A system through which clients, who are seen in emergency situations and subsequently served by the agency, are provided with the *Notice of Privacy Practices* document.
3. How existing clients will have the *Notice of Privacy Practices* reviewed with them, and who will be responsible for obtaining their signature acknowledging receipt of the *Notice of Privacy Practices.*
4. Where/how the signed notices will be kept (Note: It is recommended that they be kept in the Medical Record file.)
5. The posting of the *Notice of Privacy Practices* will be in a clear and prominent location and easily accessible to clients throughout the facilities/statewide programs.
6. The maintenance of the *Notice of Privacy Practices* on the local facilities/statewide programs website, as appropriate.

The Office of Healthcare Information will periodically review the *Notice of Privacy Practices* and if any material changes are made, promptly revise and distribute the updated *Notice of Privacy Practices* to all facilities/statewide programs. Facilities/statewide programs will post a notice of the changes and make available the updated *Notice of Privacy Practices* to anyone upon request.

ILLUSTRATIONS/EXAMPLES:

Example 1: A new client at your facility/statewide program is presented with the *Notice of Privacy Practices* during the admission process and asked to sign at the bottom, acknowledging receipt. If the client refuses to sign, the staff person who asked for the signature documents on the form that the *Notice of Privacy Practices* was offered, that the client refused to sign, and the reason for the client's refusal to sign.

Example 2: A new client is admitted to your facility/statewide program who is in crisis, or presenting with symptoms of an acute nature which preclude the client from being able to understand the explanation of the *Notice of Privacy Practices* or make it inappropriate to review under the circumstances. A specific staff person should be assigned to follow-up with the client and review the *Notice of Privacy Practices* as soon as it is reasonably possible (for example, in a hospital unit, a Social Worker could be assigned to review the *Notice of Privacy Practices* with all new admissions who come in and are unable to have the notice reviewed with them).

(Facility Name)

NOTICE OF PRIVACY PRACTICES
Mental Health Programs

- THE (FACILITY NAME) *NOTICE OF PRIVACY PRACTICES* ON THE FOLLOWING TWO PAGES DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED, AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. **PLEASE REVIEW IT CAREFULLY**

- (Facility Name) is federally mandated to maintain the privacy of your medical information and wants you to know about our practices for protecting your Protected Health Information (PHI)

- (Facility Name) is required to abide by the terms of the *Notice of Privacy Practices* provided on the attached pages

- Authorized Uses and Disclosures: In general, it is our policy to obtain written authorization for release of information prior to making a disclosure. You may revoke an authorization at any time

- Non-Authorized Uses and Disclosures: Under certain conditions we may make disclosure of your medical information without your authorization. These conditions are listed on the attached pages

WHAT ARE YOUR RIGHTS? YOU HAVE THE RIGHT TO:

- Request restrictions on certain uses and disclosures of your Protected Health Information (PHI)
- Receive reasonable confidential communication of PHI
- Inspect and copy your medical record by written request, with some exceptions. (Facility Name) reserves the right to deny the request, to which you may make a further appeal
- Request an amendment of your medical record. (Facility Name) reserves the right to deny the request, to which you may make a further appeal
- Receive an accounting of (Facility Name) disclosures of your PHI during the six years prior to your request. Accountings of disclosures start as of April 14, 2003 and are unavailable prior to that time
- Receive a paper copy of this notice

HOW YOU CAN ASK A QUESTION, LEARN MORE OR REPORT A PROBLEM?

(Facility Name) urges you to read the complete (Facility Name) *Notice of Privacy Practices* found on the attached pages of this document. The (Facility Name) Privacy Officer (enter contact name and number here), the DMHAS Office of Healthcare Information (OHI) at (860) 418-6901, or the Secretary of the United States Department of Health and Human Services are ready to assist you. There will be no retaliation for filing a complaint.

I hereby acknowledge receipt of the (Facility Name) *Notice of Privacy Practices*:

_____ _____

Patient/Client Signature Date

_____

Patient/Client Name (please print)

_____ _____

Witness Signature Date

___ Patient/Client refuses to sign *Notice of Privacy Practices*:_____

(explanation)

(Facility Name)

NOTICE OF PRIVACY PRACTICES
Mental Health Programs

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED, AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

(Facility Name) is federally mandated to maintain the privacy of your medical information and wants you to know about our practices for protecting your health information.

(Facility Name) is required to abide by the terms of this notice. The medical information we maintain may come from any of the providers from whom you have received services. The medical information we record and maintain is known as Protected Health Information, or PHI. We will not use or disclose your PHI without your permission, except as described in this notice.

We reserve the right to change our practices and to make the new provisions effective for all medical information we maintain. Should our medical information practices change, we will amend this notice and post a notice of the changes, which will be made available to anyone upon request. This notice is effective as of April 14, 2003.

USES AND DISCLOSURES: In general, it is our policy to obtain written authorization for release of information prior to making a disclosure. You may revoke an authorization at any time, except to the extent that we have already acted on it.

We may use your Protected Health Information (PHI) without authorization for:

- Treatment, e.g., share information with other providers involved in your care
- Payment, e.g., to the state Department of Administrative Services to bill for your healthcare services
- Healthcare operations, e.g., to internal staff for evaluation of the quality of services provided
- Reminding you of appointments

Other permitted disclosures of your Protected Health Information (PHI) without authorization might include the following:

- Disclosures required by law, e.g., to the Department of Children and Families when a law requires that we report suspected abuse or neglect
- For research, audit or evaluations
- Public Health, e.g., mandated reporting of disease, injury or vital statistics
- To avert a serious threat to the health or safety of you or others
- As a response to a court order, e.g. a judge orders specific portions of your record as a result of a legal matter
- If deceased, limited information to coroners, medical examiners or funeral directors

WHAT ARE YOUR RIGHTS? YOU HAVE THE RIGHT TO:

- Request restrictions on certain uses and disclosures of your Protected Health Information (PHI)
- Receive reasonable confidential communication of PHI, e.g. contact you at a place of your choosing
- Inspect and copy your medical record by written request, with some exceptions. (Facility Name) reserves the right to deny the request, to which you may make a further appeal
- Request an amendment of your medical record. (Facility Name) reserves the right to deny the request, to which you may make a further appeal
- Receive an accounting of (Facility Name) disclosures of your PHI during the six years prior to your request. Accountings of disclosures start as of April 14, 2003 and are unavailable prior to that time
- Receive a paper copy of this notice

HOW YOU CAN REPORT A PROBLEM?

If you feel your privacy rights have been violated, you may file a complaint with the (Facility Name) Privacy Officer (enter contact name and number here), the State of Connecticut, Department of Mental Health and Addiction Services (DMHAS), Office of HealthCare Information (OHI) at (860) 418-6901, or the Secretary of the United States Department of Health and Human Services (DHHS), Office for Civil Rights (OCR) at: U.S. DHHS, OCR, J.F. Kennedy Federal Building – Room 1875, Boston, Massachusetts 02203. Voice phone: (617) 565-1340. TDD: (617) 565-1343. FAX: (617) 565-3809.

There will be no retaliation for filing a complaint.

WOULD YOU LIKE MORE INFORMATION?

If you have questions and would like more information, you may contact the (Facility Name) Privacy Officer at (phone number), or the DMHAS Office of Healthcare Information (OHI) at (860) 418-6901.

(Facility Name)

NOTICE OF PRIVACY PRACTICES
Substance Abuse Programs

- THE (FACILITY NAME) *NOTICE OF PRIVACY PRACTICES* ON THE FOLLOWING TWO PAGES DESCRIBES HOW MEDICAL AND DRUG AND ALCOHOL RELATED INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED, AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. **PLEASE REVIEW IT CAREFULLY**

- (Facility Name) is federally mandated to maintain the privacy of your medical information and wants you to know about our practices for protecting your Protected Health Information (PHI)

- (Facility Name) is required to abide by the terms of the *Notice of Privacy Practices* provided on the attached pages

- Authorized Uses and Disclosures: In general, it is our policy to obtain written authorization for release of information prior to making a disclosure. You may revoke an authorization at any time

- Non-Authorized Uses and Disclosures: Under certain conditions we may make disclosure of your medical information without your authorization. These conditions are listed on the attached pages

WHAT ARE YOUR RIGHTS? YOU HAVE THE RIGHT TO:

- Request restrictions on certain uses and disclosures of your Protected Health Information (PHI)
- Receive reasonable confidential communication of PHI
- Inspect and copy your medical record by written request, with some exceptions. (Facility Name) reserves the right to deny the request, to which you may make a further appeal
- Request an amendment of your medical record. (Facility Name) reserves the right to deny the request, to which you may make a further appeal
- Receive an accounting of (Facility Name) disclosures of your PHI during the six years prior to your request. Accounting of disclosures start as of April 14, 2003 and are unavailable prior to that time
- Receive a paper copy of this notice

HOW YOU CAN ASK A QUESTION, LEARN MORE OR REPORT A PROBLEM?

(Facility Name) urges you to read the complete (Facility Name) *Notice of Privacy Practices* found on the attached pages of this document. The (Facility Name) Privacy Officer (enter contact name and number here), the DMHAS Office of Healthcare Information (OHI) at (860) 418-6901, or the Secretary of the United States Department of Health and Human Services are ready to assist you. There will be no retaliation for filing a complaint.

I hereby acknowledge receipt of the (Facility Name) *Notice of Privacy Practices*:

_____ _____
Patient/Client Signature Date

_____
Patient/Client Name (Please Print)

_____ _____
Witness Signature Date

___ Patient/Client refuses to sign *Notice of Privacy Practices*:_____
(explanation)

(Facility Name)

NOTICE OF PRIVACY PRACTICES
Substance Abuse Programs

THIS NOTICE DESCRIBES HOW MEDICAL AND DRUG AND ALCOHOL RELATED INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED, AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

(Facility Name) is required to abide by the terms of this notice. The medical information we maintain may come from any of the providers from whom you have received services. The medical information we record and maintain is known as Protected Health Information, or PHI. We will not use or disclose your PHI without your permission, except as described in this notice.

Information regarding your healthcare, including payment for healthcare, is protected by two federal laws: the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. §1320d *et seq*., 45 C.F.R. Parts 160 & 164, and the Confidentiality Law, 42 U.S.C. § 290dd-2, 42 C.F.R. Part 2. Under these laws, (Facility Name) may not say to a person outside (Facility Name) that you attend the program, nor may (Facility Name) disclose any information identifying you as an alcohol or drug abuser, or disclose any other PHI except as permitted by federal law.

We reserve the right to change our practices and to make the new provisions effective for all medical information we maintain. Should our medical information practices change, we will amend this notice and post a notice of the changes, which will be made available to anyone upon request. This notice is effective as of April 14, 2003.

USES AND DISCLOSURES:

(Facility Name) must obtain your written consent before it can disclose information about you for payment purposes. Generally, you must also sign a written authorization before (Facility Name) can share information for treatment purposes or for healthcare operations. However, federal law permits (Facility Name) to disclose information **without** your written permission for the following:

- Pursuant to an agreement with a person or agency that provides services to (Facility name)
- For research, audit or evaluation
- To report a crime committed on (Facility Name) premises or against (Facility Name) personnel
- To medical personnel in a medical emergency
- To appropriate authorities to report suspected child abuse or neglect
- As allowed by a court order

Before (Facility Name) can use or disclose any information about your health in a manner which is not described above, it must first obtain your specific written authorization allowing it to make the disclosure. You may revoke any such written authorization in writing, except to the extent that we have already acted on it.

WHAT ARE YOUR RIGHTS? YOU HAVE THE RIGHT TO:

- Request restrictions on certain uses and disclosures of your Protected Health Information (PHI)
- Receive reasonable confidential communication of PHI, e.g. contact you at a place of your choosing
- Inspect and copy your medical record by written request, with some exceptions. (Facility name) reserves the right to deny the request, to which you may make a further appeal
- Request an amendment of your medical record. (Facility name) reserves the right to deny the request, to which you may make a further appeal
- Receive an accounting of (Facility name) disclosures of your PHI during the six years prior to your request. Accounting of disclosures start as of April 14, 2003 and are unavailable prior to that time
- Receive a paper copy of this notice

HOW YOU CAN REPORT A PROBLEM?

If you feel your privacy rights have been violated, you may file a complaint with the (Facility name) Privacy Officer (enter contact name and number here), the State of Connecticut, Department of Mental Health and Addiction Services (DMHAS), Office of Healthcare Information (OHI) at (860) 418-6901, or the Secretary of the United States Department of Health and Human Services (DHHS), Office for Civil Rights (OCR) at: U.S. DHHS, OCR, J.F. Kennedy Federal Building – Room 1875, Boston, Massachusetts 02203. Voice phone: (617) 565-1340. TDD: (617) 565-1343. FAX: (617) 565-3809.

There will be no retaliation for filing a complaint.

WOULD YOU LIKE MORE INFORMATION?

If you have questions and would like more information, you may contact the (Facility Name) Privacy Officer at (phone number), or the DMHAS Office of Healthcare Information (OHI) at (860) 418-6901.

ACCESS TO PROTECTED HEALTH INFORMATION

POLICY:

It is the policy of the Agency, in accordance with state and federal laws, that all service recipients have the right to access, inspect or obtain a copy of their Protected Health Information (PHI) for as long as the Agency maintains the PHI.

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

Facilities/statewide programs will need to develop an internal process by which service users can access, inspect or copy their PHI. This process should include the identification of an individual responsible for providing oversight to this process and, implement procedures to be followed when a patient requests access to their PHI.

The facilities/statewide programs will permit a patient to request access to inspect or to obtain a copy of their PHI that is maintained in their medical record. The facilities/statewide programs will require that the patient make their request for access in writing.

The facilities/statewide programs will act on a request for access no later than 30 days after receipt of the request as follows:

a) If the facilities/statewide programs grant the request, in whole or in part, it will inform the patient of the acceptance of the request and provide the access requested; or,
b) If the request for access is for PHI that is not maintained or is not accessible to the facilities/statewide programs, the facilities/statewide programs will take action to notify the patient of the status of access.

<u>Granting of Access</u>

1. If the facilities/statewide programs provide a service user with access to their PHI, in whole or in part, the facilities/statewide programs will:
    a) Provide the access requested by an individual to their PHI, including inspecting and/or obtaining a copy of their Medical Record; and,
    b) If the same PHI, that is the subject of a request for access, is maintained in more than one designated record set or at more than one location, the facilities/statewide programs need only produce the PHI once in response to the request for access.
2. The facilities/statewide programs will provide the patient with access to their PHI in a readable hard copy format.
3. The facilities/statewide programs will provide the patient with a summary of the PHI requested, in lieu of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided, if:

a) The patient agrees in advance to such a summary or explanation; and,
b) The patient agrees in advance to the fees imposed, if any, by the facilities/statewide programs for such summary or explanation.

4. The facilities/statewide programs will provide the access as requested by the patient in a timely manner, including arranging with the individual for a convenient time and place to inspect or obtain a copy of their PHI, or mailing the copy of the PHI at the individual's request.
5. The facilities/statewide programs must document and retain the following in accordance with State of Connecticut record retention guidelines:
    a) The designated record sets that are subject to access by patients; and,
    b) The titles of the persons or offices responsible for receiving and processing requests for access by patients.
6. If the facilities/statewide programs do not maintain the PHI that is the subject of the patient's request for access, and the facilities/statewide programs know where the requested information is maintained, the facilities/statewide programs will inform the patient where to direct the request for access.
7. If the patient receives copies of his/her PHI, or agrees to a summary or explanation of such information, the facilities/statewide programs may impose a reasonable, cost-based fee, not to exceed $ .65/page, that includes:
    b) Copying, including the cost of supplies for and labor of copying the PHI requested by the patient;
    c) Postage, when the patient has requested the copy, or the summary or explanation, be mailed; and,
    d) Preparing an explanation or summary of the PHI, if agreed to by the patient.

<u>Denial of Access</u>

1. PHI that may not be accessed or inspected due to state and federal law are:
    a) Psychotherapy notes;
    b) Information compiled in a reasonable anticipation of, or for use in a civil, criminal, or administrative action or proceeding;
    c) Research;
    d) Correctional Institution records; or,
    e) Information obtained from other healthcare providers.
2. The facilities/statewide programs shall deny a service user access, without providing the patient an opportunity for review, in the following circumstances:
    a) If the patient has agreed to the denial of access when consenting to participate in research that includes treatment, and the covered healthcare provider has informed the patient that the right of access may be reinstated upon completion of the research; or,
    b) If the PHI was obtained from someone other than a healthcare provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
3. The facilities/statewide programs may deny a patient access, provided that the patient is given a right to have such denial reviewed, in the following circumstances:

a) A licensed healthcare 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 patient or another person;
b) The PHI makes reference to another person (unless such other person is a healthcare provider) and a licensed healthcare professional 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 for access is made by the patient's personal representative and a licensed healthcare professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the patient or another person.

4. If access has been denied, a patient has the right to have the denial reviewed by a medical doctor who is designated by the facility/statewide program to act as a reviewing official and who did not participate in the original decision to deny access. The facilities/statewide programs' Healthcare Information Specialist will coordinate this review. The facilities/statewide programs will provide or deny access in accordance with the determination of the reviewing official.
5. If the facilities/statewide programs have denied access to PHI, in whole or in part, the facilities/statewide programs will:
   a) Make other information accessible, by giving the patient access to any other PHI requested, after excluding the PHI which the facilities/statewide programs have a ground to deny access;
   b) Provide a timely, written denial to the patient. The denial must be in plain language and contain:
      i. The basis for the denial;
      ii. A description of how the patient may exercise his/her right to have the denial reviewed by the reviewing official; and,
      iii. A description, including contact information, of how the patient may complain to the facilities/statewide programs or to the DMHAS Office of Healthcare Information.
6. If the individual has requested a review of a denial, the facilities/statewide programs must have the reviewing official review the decision to deny access and determine, within a reasonable period of time, whether or not to deny the access. The facilities/statewide programs must promptly provide a written notice to the individual of the determination of the reviewing official and if access is still denied, their right to a further review by the Office of Healthcare Information.

ILLUSTRATIONS/EXAMPLES:

Example 1: A client provides an authorization to obtain her records from the facility/statewide program from which she is currently receiving treatment (Program A). Included in this medical record is information received from another treating facility/statewide program (Program B). The client previously signed a release allowing Program B to send intake and discharge information. In response to her request, information included in the data set that had been generated by Program A was provided her, but not the intake and discharge information received

from the other facility/statewide program. Re-disclosure prohibits such release. The client was instructed to make a formal request for that information from Program B.

Example 2: A client signs an authorization to obtain his own record for a particular episode of care, specifically requesting copies of his psychotherapy notes. Upon review of the chart, the primary clinician and the attending psychiatrist believe releasing this information would be medically harmful to the patient. The client is informed that his request has been denied, the reason for that denial, and the process for filing a complaint. The client requests a review of the decision by a reviewing official, who agrees with the original clinician and the denial of access is upheld. The client is informed he may contact the Office of Healthcare Information for additional appeal.

Example 3: A client who was hospitalized in 1988 calls the Medical Records department and requests a copy of their record for that stay. The records clerk sends the patient an authorization form to complete. The client submits the completed authorization form to obtain their record to the Medical Records department. Since the record was stored in the State Records Center Archive in 1992, a request is submitted by the records clerk to the archive to obtain the record. A letter is sent to the client within 30 days of receiving the client's authorization, informing the client of the fact that the record has been archived and that the client will be notified as soon as it is sent back to the hospital. When the record arrives, the records clerk notifies the hospital medical director of the request to view the record. The medical director reviews the client's request and decides to speak personally with the client to ascertain their objectives in reviewing their record. Following a conversation with the client, the Medical Director approves the client reviewing their discharge summary from that hospital stay.

AMENDMENT OF PROTECTED HEALTH INFORMATION

POLICY:

It is the policy of the Agency to allow a service user to request an amendment of their Protected Health Information (PHI) for as long as the Agency maintains the information.

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

Facilities/statewide programs will need to develop an internal process by which service recipients can request an amendment of their PHI. This process should include the identification of an individual responsible for providing oversight to this process and, implement procedures to be followed when a patient requests an amendment of their PHI, including how the amendments are tracked and a process to appeal denials.

Granting Amendment Requests

1. If the facilities/statewide programs grant the requested amendment, in whole or in part, the facilities/statewide programs will:
    a) Make the amendment;
    b) Inform the patient in writing that the amendment has been accepted; and,
    c) Notify all relevant persons with whom the amendment needs to be shared, which must include persons who previously received the specific information that was subsequently amended.
2. If the facilities/statewide programs have accepted the amendment, in whole or in part, the facilities/statewide programs will make a reasonable effort to inform the patient of the decision and provide notification of the amendment within a reasonable time frame. Individuals who may receive this amendment are:
    a) Persons identified by the patient as having received his/her PHI and are in need of the amendment; or,
    b) Persons, including business associates of the facilities/statewide programs, which have previously received the patient's PHI and have relied on the information for the patient's benefit.
3. When an amendment is made, the original record must be marked with regard to where the amendment can be found. The original record should not be altered or destroyed.

Denying Amendment Requests

1. If facilities/statewide programs deny an amendment request, it shall be for the following reasons:
    a) The facilities/statewide programs did not create the entry to which the amendment request is addressed;

b) The portion to which the amendment request is addressed, is not in the medical record;
c) The portion to which the amendment request is addressed, is information to which the patient does not have a right of access; or,
d) The portion to which the amendment request is addressed is accurate and complete.

2. If a request for amendment is denied, the facilities/statewide programs shall provide a written explanation, within a reasonable amount of time, explaining the reason for the denial and the right of the patient to appeal the denial to the facilities/statewide programs Healthcare Information Specialist.
3. If the individual has requested a review of a denial, the facilities/statewide programs must have the Healthcare Information Specialist review the decision to deny the amendment. The Healthcare Information Specialist must then determine, within a reasonable period of time, whether or not to deny the amendment. The facilities/statewide programs must promptly provide a written notice to the individual of the determination of the Healthcare Information Specialist and if the amendment request is still denied, their right to a further review by the Office of Healthcare Information.
4. The original request for amendment and the denial are to be placed in the patient's medical record.
5. If the patient submits a disagreement to the denial, this is to be inserted into the medical record as well.
    a) If the facilities/statewide programs make a rebuttal to the patient's disagreement, this is placed in the medical record as well.

ILLUSTRATIONS/EXAMPLES:

Example 1: A patient's chart reflects a felony history and incarceration. The patient believes the information is both inaccurate and will negatively impact on his ability to obtain employment and wants to amend the record. However, he provides no written documentation to demonstrate the information is inaccurate and his request is denied. The facilities/statewide programs provide a written notification of the denial, within a reasonable amount of time, and honors the request from the patient to enter into the chart his written request for amendment.

Example 2: A client submits a letter on November 15 requesting that all instances in her medical record be removed that refer to a drug screen that indicated a positive for opiates. She provides verification from the laboratory, which had maintained a portion of the sample for retesting as required, that in fact, the results were a false positive. The facilities/statewide programs then inserts a notation at each place in the record where there was a reference to the drug screen results. The notation directs the reader to the laboratory section of the medical record that has the corrected results. This process was completed by January 14th. Those parties that had received copies of the incorrect results were notified within a reasonable period of time.

ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

POLICY:

It is the policy of the Agency to provide an accounting of disclosures of Protected Health Information (PHI) made by the Agency in the six years prior to the date on which the accounting is requested, except for disclosures not required by law or disclosures made prior to April 14, 2003. The accounting will be provided within 60 days of receipt of the request.

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

Facilities/statewide programs will need to develop an internal process by which service recipients can request an accounting of their PHI. This process should include the identification of an individual responsible for providing oversight to this process and, implement procedures to be followed when a service user requests an accounting of their PHI, including how the accounting is tracked.

1. The request for an accounting of disclosures must be in writing.

2. The facilities/statewide programs will provide an accounting of disclosures of PHI made by the facilities/statewide programs in the six years prior to the date on which the accounting is requested (Disclosures made prior to April 14, 2003 are exempt).

3. The written, signed, request must include the individual's:
    a) Name; address; telephone number; social security number; other names used, if applicable (for example: maiden name); date of birth; dates of care; copy of photo identification with signature; subject of the request; and, reason for the request of this information.
    b) If photo identification with signature is not available, a notarized request is acceptable.

4. An accounting of the following disclosures ***will not*** be included:
    a) Disclosures made for carrying out treatment, payment and healthcare operations;
    b) Disclosures made to the individual about their PHI;
    c) Disclosures to national security or intelligence purposes; to correctional institutions or law enforcement officials;
    d) Disclosures that occurred prior to the effective date of April 14, 2003;
    e) Disclosures not created by the facilities/statewide programs, unless the individual provides a reasonable basis to believe that the person who created the PHI is no longer available to act on the individual's request;
    f) If the disclosure is not part of the individual's record;

g) If the disclosure is for psychotherapy notes;
h) If it is information collected and held in reasonable anticipation, or for use in, a civil, criminal, or administrative action or proceeding; or if it is a record that is subject to the Clinical Laboratory Improvements Amendments of 1988;
i) If the disclosure is part of a Limited Data Set; or,
j) Disclosures made as a result of an authorization.

5. Contents of Accounting will include:
   a) The date of the disclosure;
   b) The name of the entity or person who received the PHI and, if known, the address of such entity or person; and,
   c) A brief description of the PHI disclosed (i.e., Public Health Activities, Health Oversight Agency, Research) or a brief statement of the purpose of the disclosure or a copy of their authorization.

   An accounting of disclosures made pursuant to a research project consisting of 50 or more individuals may provide the following:
   a) The name of the protocol or other research activity;
   b) A description of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;
   c) A brief description of the type of PHI that was disclosed;
   d) The date or period of time during which such disclosures occurred or may have occurred, including the date of the last such disclosure during the accounting period;
   e) The name, address and telephone number of the entity that sponsored the research and of the researcher to whom the PHI was disclosed; and,
   f) A statement that the PHI of the patient/client may or may not have been disclosed for a particular protocol or other research activity.

6. The facilities/statewide programs will retain the request and a copy of the documentation provided to the individual in accordance with State of Connecticut record retention guidelines. It will include the title of the person or office responsible for receiving and processing the request.

7. The facilities/statewide programs must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, for the time specified by such agency or official, if such agency or official provides the facilities/statewide programs 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.

ILLUSTRATION/EXAMPLE:

Example: On November 15, 2005, an individual believes that a rash of health insurance advertisements mailed to his home are the result of information provided by a facility/statewide program from which he recently received services. He has provided a written document requesting an accounting of all disclosures made in the past six years. The request provided included all the required elements and the information is provided him. The medical records department does not include an accounting of disclosures made that were required to carry out treatment, payment and healthcare operations. The medical records department also did not include disclosures made to the Secret Service who requested information on this client because the client had publicly threatened the Vice President of the United States in the past, and the Vice President was scheduled to make a visit to the city in the near future. It should be noted that the Secret Service representative provided validation of her identity prior to the disclosure being made.

REQUEST FOR CONFIDENTIAL COMMUNICATION OF PROTECTED HEALTH INFORMATION

POLICY:

The Agency shall respect the right of an individual to request reasonable accommodation for receiving Protected Health Information (PHI). Reasonable accommodation may include receiving PHI at alternative locations or by alternative means. The request shall be received in writing and shall specify the alternative address or other method of contact.

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

The facilities/statewide programs will not require an explanation from the service recipient or designee as to the basis for the request as a condition of providing confidential communication or PHI at alternative locations or by alternative means (i.e., fax number, P.O. Box).

If the facilities/statewide programs determine that the request is unreasonable, the facilities/statewide programs will respond to the service user or designee in writing and inform them of their right to file an appeal with the facility/statewide program Healthcare Information Specialist.

If the patient has requested a review of the decision, the facilities/statewide programs must have the Healthcare Information Specialist review the decision. The Healthcare Information Specialist must then determine, within a reasonable period of time, whether or not the request is unreasonable. The facilities/statewide programs must promptly provide a written notice to the individual of the determination of the Healthcare Information Specialist and if the request is still deemed to be unreasonable, their right to a further review by the Office of Healthcare Information.

The facilities/statewide programs will document all requests for alternative confidential communications, and their disposition.

ILLUSTRATION/EXAMPLE:

Example: A patient/client sends a request to have their lab results faxed to their place of business, rather than sent to their home address. If the facility/statewide program determines this to be a reasonable request, the lab results are then faxed to their place of business.

Connecticut DMHAS
Department of Mental Health and Addiction Services
A Healthcare Service Agency

USES AND DISCLOSURES

INTRODUCTION

Service recipients enter treatment with the expectation that the information they share will be used and disclosed exclusively for their clinical care. To protect their privacy and avoid embarrassment, stigma, and discrimination, some service users withhold information from their healthcare providers, provide inaccurate information, doctor-shop, pay out-of-pocket for care that is covered by insurance, and in many cases, avoid care altogether.

Until recently, health information was recorded and maintained on paper and stored in the offices of healthcare providers and within institutions. In some ways, this imperfect system of record keeping created a false sense of privacy among patients, providers, and others. Patients' health information has never remained completely confidential. Until recently, a breach of confidentiality involved a physical exchange of paper records or a verbal exchange of information. Today, however, more and more healthcare providers, plans, and others are utilizing electronic means of storing and transmitting health information. The electronic information revolution is transforming the recording of health information so that the disclosure of information may require only a push of a button. In a matter of seconds, a person's most profoundly private information can be shared with hundreds, thousands, even millions of individuals and organizations at a time. While the majority of medical records still are in paper form, information from those records is often copied and transmitted through electronic means.

Concerns about the lack of attention to information privacy in the healthcare industry are not merely theoretical, they are real. In the absence of a national legal framework of health privacy protections, patients are increasingly vulnerable to the exposure of their Protected Health Information or PHI. Disclosure or misuse of individually identifiable health information can occur deliberately or accidentally and can occur within an organization or be the result of an external breach of security.

The DMHAS, its' state-operated facilities and statewide programs (Agency) have many restrictions placed on how PHI can be used and disclosed. Existing practices regarding the use and disclosure of PHI for treatment, payment and healthcare operations can continue as present. However, the Agency is required to review how information is used and disclosed and make an effort to limit all uses and disclosures to the minimum necessary in order to accomplish the required purpose.

HIPAA establishes national minimum standards to protect the privacy of individually identifiable health information in prescribed settings. The standards address the many varied uses and disclosures of individually identifiable health information including the following mandated requirements:

1. Obtain written authorization from all patients prior to using their PHI, except in limited prescribed situations;

2. Provide all patients with an understanding of how their PHI is being used by the Agency in the *Notice of Privacy Practices*;

3. Default to the more restrictive authorization and/or other written legal permission, when there is a conflict, in order to better protect a patient's PHI;

4. Verify the identity and authorization of all individuals who request a disclosure of PHI;

5. Provide an opportunity for clients to request that restrictions be placed on who can use and access their PHI;

6. Fully comply with all uses and disclosures, without authorization, that are required by law;

7. Limit the disclosure of all requests for PHI to the amount reasonably necessary to accomplish the purpose for which the request was made;

8. Promote the involvement of patients' personal representatives in their care and notification;

9. De-identify, whenever possible, all PHI prior to its release; and,

10. Obtain satisfactory assurance that all Business Associates will appropriately safeguard the PHI they create or receive from the Agency.

PROVISION OF *AUTHORIZATION FOR USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION*

POLICY:

It is the policy of the Agency to obtain a service recipient's written authorization prior to using or disclosing their Protected Health Information (PHI) for specified purposes, other than treatment, payment or healthcare operations. In some cases, state and federal laws provide greater protection to the service user and in those instances, should be adhered to.

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

1. The authorization obtained from the patient will:
   A. Cover only the uses and disclosures and only the PHI stipulated in the authorization;
   B. Have an expiration date not to exceed twelve months or a specified event or condition (i.e., discharge, death);
   C. State the purpose for which the information may be used or disclosed;
   D. Specify the recipient of the information;
   E. Specify the facility/statewide program as the institution releasing the information;
   F. Be signed by the client or his/her legal representative and if it is signed by the legal representative, it must contain a description of the representative's authority to act for the client;
   G. Be dated after the episode record of care;
   H. Include a statement specifying:
      i. That refusal to sign the authorization will not affect their right to obtain present and future treatment, except where disclosure of such communications and records is necessary for treatment;
      ii. How the client may revoke the authorization;
      iii. That the confidentiality of psychiatric, drug and/or alcohol abuse and HIV records are protected under State and Federal Laws and cannot be disclosed without their written authorization unless otherwise provided for by law; and,
      iv. That the information disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer protected by Federal law.
2. The facility/statewide program will provide the client with a copy of the signed authorization.
3. An authorization may be revoked at any time, except to the extent that the facility/statewide program has taken action in reliance thereon.
4. The revocation must be in writing.

ILLUSTRATION/EXAMPLE:

Example: A client stops by the facility/statewide program Medical Records department and drops off an authorization from his new employer requesting a copy of the history and physical his principle physician completed less than a month ago. The authorization does not include all the necessary requirements for a complete and proper authorization. The Medical Records department assists the individual in completing a properly executed authorization to release the information.

STATE OF CONNECTICUT
DEPARTMENT OF MENTAL HEALTH AND ADDICTION SERVICES

Facility Name
Facility Street Address
Facility City/State/Zip
Facility Telephone

AUTHORIZATION TO OBTAIN AND DISCLOSE PROTECTED HEALTH INFORMATION

THIS IS A LEGAL DOCUMENT AND WILL NOT BE HONORED UNLESS IT IS COMPLETED IN FULL

From the medical records of:

_____ ____-____-____ _____ _____
Patient/Client (Last Name, First Name) Date of Birth SS# MPI#

I, the undersigned, authorize the above named agency to: ☐ **DISCLOSE information to** ☐ **OBTAIN information from** the following:

Name of Person:_____ Name of Agency:_____

Street/P.O. Box:_____

City: _____ State: _____ Zip Code: _____

Please check (X) and initial each box below as applicable

Type of Info	Yes	Init
Medical		
Psychiatric		
Substance Abuse		
HIV/AIDS		
Other (specify):		

Info from Documents	Yes	Init.
Psychosocial Hist./Assessmt		
Psychiatric Evaluation		
Psychological Evaluation		
Medical Hist./Physical Exam		
Medication Record		
Discharge/Transfer Summary		
Treatment Plans		
Other (specify):		

Purpose of Release *(Any other use is prohibited)*	Yes	Init.
Assist with Evaluation/Treatment		
Benefit Determination		
Service Determination		
Other (specify):		

Form of Information	Yes	Init.
Written		
Oral		
FAX		
Other (specify):		

Dates of Treatment Covered by this Request:
__ All prior episodes of care, through discharge from present episode of care
__ Limited to the following Date(s)/Program(s):_____
_____

This authorization, if not cancelled, will expire:_____
_____
Date (not to exceed 12 months), event or condition upon which this authorization expires.

I understand that refusal to sign this authorization form will in no way affect my right to obtain present and future treatment, except where disclosure of such communications and records is necessary for treatment. I also understand that I may revoke this authorization at any time by signing the "CANCELLATION/REVOCATION" section below, except to the extent that action has been taken in reliance on it. I further understand that the confidentiality of psychiatric, drug and/or alcohol abuse and HIV records are protected under State and Federal Laws and cannot be disclosed without my written authorization unless otherwise provided for by law. The information disclosed by this facility pursuant to this authorization may be subject to re-disclosure by the recipient and no longer protected by Federal law.

_____ _____
Signature of Patient/Client/Authorized (Legal) Representative* Date Translator/Interpreter Signature (if applicable) Date

_____ _____
Relationship to Patient/Client Staff Contact Person (if applicable) - Please Print

CANCELLATION/REVOCATION: _____
Signature of Patient/Client/Authorized (Legal) Representative* Date

* If this form has been signed by the patient's/client's Authorized (Legal) Representative, a copy of the legal appointment must be attached.

RESOLVING CONFLICTING AUTHORIZATIONS

POLICY:

It is the policy of the Agency that conflicting authorizations to disclose Protected Health Information (PHI) be identified and resolved.

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

1. When the facilities/statewide programs are presented with conflicting authorizations to disclose PHI, the facilities/statewide programs shall:
    a) Communicate in writing with the service recipient in order to determine the individual's preference regarding the authorization to disclose PHI; and,
    b) Resolve the conflict by obtaining a new written authorization from the service user or have them cancel the authorization(s) that is/are in conflict with their preference by signing the cancellation section on the authorization(s).

2. Until such time as the conflict is resolved, the facilities/statewide programs will defer to the most restrictive authorization.

ILLUSTRATION/EXAMPLE:

Example: A client signed an authorization in April, which is still in force, to disclose PHI to his spouse. He specifically limited that disclosure to dates he attended sessions at the facility/statewide program. In June, the client's primary clinician receives a signed authorization to disclose dates he attended sessions as well as medical information to his spouse. The medical records department does not release the information, and the primary clinician discusses the conflict with the client during their next scheduled meeting. It is determined that the client believed the most recent authorization overruled the previous authorization. He cancels the April Authorization and the facility/statewide program releases the requested information.

VERIFICATION REQUIREMENTS FOR USE AND DISCLOSURE

POLICY:

It is the policy of the Agency to verify the identity of a person requesting Protected Health Information (PHI) and the authority of any such person to have access to the PHI that is being requested.

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

Facilities/statewide programs will need to implement procedures, which specify how they will verify the identity and authority of persons requesting disclosure of PHI *when it is required as a condition of the disclosure* (See Policy on Disclosure to determine which situations meet the latter condition), at the same time keeping in mind that there may be multiple persons within an organization who will need to be knowledgeable of these procedures. The procedures should cover, at a minimum, the following areas:

1. Verification Methods: Given various situations, which procedure will be followed, as shown in the sample table below:

ENTITY/PERSON MAKING REQUEST	METHOD
Service recipient's authorized representative, i.e., therapist at Outpatient Clinic, conservator, personal representative	Dated and signed authorization on agency letterhead. Dated and signed written statement by the conservator or personal representative.
Client/patient	In person: Identification, i.e., driver's license, passport, birth certificate or state issued identity card. On phone: Caller ID, social security number, birth date, other personal information.
For request made pursuant to legal process	Warrant, subpoena, order, or other legal process issued by a grand jury, judicial or administrative tribunal.

2. Exercise of Professional Judgment: Verification requirements are met if the facilities/statewide programs rely on the exercise of professional judgment or act in good faith in making a disclosure.

3. Recording of Disclosures: The facilities/statewide programs will need to implement a system to document all disclosures that are made including: how the requestor's identity was verified; who the disclosure was made to; what information was

disclosed; when it was disclosed; and, why it was disclosed. This documentation will need to be maintained in a readily retrievable format for individual patients (i.e., within the medical record itself or in a separate log where individual patient PHI disclosures can be easily obtained.)

ILLUSTRATION/EXAMPLE:

Example: A *Release of Information Form* from one Outpatient Clinic is received by the Medical Records Department of another Outpatient Clinic requesting a copy of a Discharge Summary for a former client. The Medical Records staff processing the request reviews the release form to make sure that it is on the letterhead of the requesting agency and that it contains the required signatures. The Medical Records staff then logs the request, noting: the form of verification was *agency letterhead*; who the disclosure was to; what information was disclosed; when it was disclosed; and, why the information was disclosed.

RESTRICTIONS ON THE USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

POLICY:

It is the policy of the Agency to respect the right of a service recipient to request restrictions on the uses and disclosures of Protected Health Information (PHI).

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

1. The facilities/statewide programs shall modify their existing policies and procedures on confidentiality and patient access to records to determine the most appropriate place to insert a section on restrictions, or whether to develop a separate policy/procedure altogether.
2. The procedure shall clearly and simply describe how the service user can go about requesting a restriction of their PHI, who the request is submitted to, and the time frame for a response.
3. The procedure shall indicate how requests for restrictions, and the decisions regarding them, will be documented, by whom, and where the documentation will be stored.
4. If the facilities/statewide programs agree to a service recipient's restriction, the facilities/statewide programs shall not use or disclose PHI in violation of this restriction. Additionally, the facilities/statewide programs shall alert others who receive this information through legitimate processes of the restriction.
5. The facilities/statewide programs may terminate their agreement to a restriction if:
   a) The patient/client agrees to or requests the termination in writing;
   b) The patient/client orally agrees to the termination and the oral agreement is documented; or,
   c) The facilities/statewide programs notify the patient/client it is terminating the agreement and the termination is effective, with respect to PHI, after the individual is informed.
7. If a restriction is denied, the facilities/statewide programs shall notify the patient that the restriction has not been accepted and their right to appeal this denial with the facility/statewide program Healthcare Information Specialist.
8. If the patient has requested a review of a denial, the facilities/statewide programs shall have the Healthcare Information Specialist review the decision to deny the restriction. The Healthcare Information Specialist must then determine, within a reasonable period of time, whether or not to deny the restriction. The facilities/statewide programs must promptly provide a written notice to the individual of the determination of the Healthcare Information Specialist and if the restriction is still denied, their right to a further review by the Office of Healthcare Information.
9. On an annual basis, the facilities/statewide programs shall review their denials on restrictions and verify consistency and adherence with best practice standards.

ILLUSTRATIONS/EXAMPLES:

Example 1: A behavioral health outpatient facilities/statewide programs uses a specific form called "Request for Restriction on Uses and Disclosures of Protected Health Information." A client completes this form, requesting that her parents be restricted from access to her medical record. The form is submitted to the client's clinician who gives it to the Medical Records Department for inclusion in the client's record.

Example 2: A client in a psychiatric hospital completes the "Request for Restriction on Uses and Disclosures of Protected Health Information" form, requesting that the Outpatient Clinic that referred him to the hospital be restricted from access to his medical record. The form is submitted to the client's social worker, who reviews it with the treatment team and denies the restriction because clinicians from the outpatient clinic are involved in planning for the client's discharge. The client is informed of this decision and their right to appeal. The reason for the denial is documented on the request form, which is placed in the client's medical record.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION WITHOUT AUTHORIZATION

POLICY:

It is the policy of the Agency that the Agency may disclose Protected Health Information (PHI) without authorization for the following:

1. Public Health Activities;
2. Victims of abuse or neglect;
3. Health Oversight activities;
4. Judicial or Administrative Proceedings;
5. Deceased individuals;
6. To avert a serious threat to health;
7. Specialized government functions;
8. Shared Government Services; and,
9. Workforce member crime victims.

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

Public Health Activities

The facilities/statewide programs may disclose PHI for the following public health activities and purposes:

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

2. A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

3. A person subject to the jurisdiction of the Food and Drug Administration; or

4. A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the facilities/statewide programs or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.

Victims of Abuse or Neglect

The facilities/statewide programs may disclose PHI about individuals:

1. Whom they reasonably believe to be victims of abuse or neglect to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse or neglect. If facilities/statewide programs make this disclosure, they will promptly inform the individual that such reports have been or will be made, except if:

    a) The facilities/statewide programs, in the exercise of professional judgment, believes informing the patient/client would place him/her at risk of serious harm; or
    b) The facilities/statewide programs would be informing a personal representative, and reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the patient/client.

2. As required by law including laws that require the reporting of certain types of wounds or other physical injuries, or in compliance with a court order.

Health Oversight Activities

The facilities/statewide programs may disclose PHI to a Health Oversight Agency for oversight activities authorized by law, including audits, civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight.

Judicial or Administrative Proceedings

The facilities/statewide programs may disclose PHI in the course of any judicial or administrative proceedings in response to an order of a court or administrative tribunal, provided that the facilities/statewide programs disclose only the PHI expressly authorized by such order.

Deceased Individuals

The facilities/statewide programs may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

The facilities/statewide programs may disclose PHI to funeral directors, as necessary, to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their

duties, the facilities/statewide programs may disclose the PHI prior to, and in reasonable anticipation of, the individual's death.

The facilities/statewide programs may use or disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose facilitating organ, eye or tissue donation and transplantation.

To Avert a Serious Threat to Health

The facilities/statewide programs are permitted to use and disclose PHI, if the facilities/statewide programs believe, in good faith, the use or disclosure:

1. Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and,

2. Is to a person or persons reasonably able to prevent or lessen the threat; including the target of the threat; or,

3. Is necessary for the law enforcement authorities to identify or apprehend an individual:

    a) Because of a statement by an individual admitting participation in a violent crime that the Agency reasonably believes may have caused serious physical harm to the victim; or,
    b) Where it appears from all the circumstances that the individual has escaped from a correction institution or from lawful custody.

The facilities/statewide programs are not permitted to use or disclose the PHI, if the information is learned by the facilities/statewide programs:

1. In the course of treatment, counseling, or therapy, to affect the propensity to commit the criminal conduct that is the basis for the disclosure; or

2. Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy.

Specialized Government Functions

The facilities/statewide programs disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (e.g., Executive Order 12333).

The facilities/statewide programs disclose PHI to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C 2709(a)(3), or to the conduct of investigations authorized by 18 U.S.C. 871 and 879.

Shared Government Services

DMHAS' State Administered General Assistance program may disclose PHI relating to eligibility for or enrollment in the program, to another Agency administering a government program providing public benefits, if the sharing of eligibility or enrollment information between the agencies, or the maintenance of such information in a single or combined data system accessible to the agencies, is required or expressly authorized by statute or regulation.

Workforce Member Crime Victims

The facilities/statewide programs are not considered to have violated the right of a service recipient if a member of its workforce, who is the victim of a criminal act, discloses PHI to a law enforcement official, provided that:

1. The PHI disclosed is about the suspected perpetrator of the criminal act; and
2. The PHI disclosed is limited to the following:
   (a) Name and address;
   (b) Date and place of birth;
   (c) Social security number;
   (d) ABO blood type and Rh factor;
   (e) Type of injury;
   (f) Date and time of treatment;
   (g) Date and time of death, if applicable; and
   (h) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars and tattoos.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION, MINIMUM NECESSARY

POLICY:

It is the policy of the Agency to make efforts that shall limit the use, disclosure, and all requests for service user Protected Health Information (PHI), to the minimum necessary that is needed in order to accomplish the intended purpose.

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

The facilities/statewide programs shall apply the "Minimum Necessary" standard to both external disclosures and internal communications of patient/client PHI.

External Disclosures

The facilities/statewide programs shall develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the intended purpose. Criteria includes the purpose for which the disclosure or use is requested, what should be disclosed, who is requesting disclosure, and how long a time period is granted for use of PHI.

The facilities/statewide programs shall designate a person to oversee or review all requests on an individual basis in accordance with such criteria.

The facilities/statewide programs shall limit requests for PHI from other facilities or covered entities to that which is reasonably necessary to accomplish the purpose for which the request is made.

Internal Communications

The facilities/statewide programs shall not permit individually identifiable health information to be displayed in common settings or public areas, such as on white boards or rosters in hallway where the public or other patients would have ready access.

The facilities/statewide programs shall permit oral communications in public areas that are necessary to carry out treatment, but encourages that this communication be kept to a minimum. Providers in a facilities/statewide programs shall make reasonable efforts to avoid others from intercepting the information, in whatever medium.

The facilities/statewide programs shall identify and make reasonable efforts to limit access of those persons, or classes of persons in its workforce, who need access to PHI to carry out their

duties and to identify the categories of PHI to which access is needed and any conditions appropriate to such access.

In the facilities/statewide programs, there are various functions performed by multiple workforce members, with different job titles. In the performance of these functions, staff shall be provided with access to only the minimum necessary of PHI that is needed in order to fulfill their duties. This may include that in the performance of one function, a workforce member is provided access to the entire medical record of an individual. In the performance of a second function, this same workforce member will only have access to a portion of the medical record. Please refer to the sample table below.

Function	**Access**
Audit: – H.C.F.A. Compliance Activities - Peer Review - Q.I. - U.M./U.R.	Entire record under audit
Secretarial /Data Entry	Administrative information for filing and administrative care
Clinical Functions: – M.D., Ph.D., R.N., Clinical Case Manager, L.C.S.W., M.H.W.	Entire record of service recipients on their unit or for whom they have responsibility in their program
Disposition/Transfer/Referral Meetings	Entire record of disposition
Discharge	Entire record of discharged service user
Information Technology Staff	Databases and IT resources for systems management
Medical Record Staff	Entire record
Support Staff: - Facilities Management - Business Office - Housekeeping - Dieticians	Minimal access to administrative components of the medical record
Billing	Administrative and payment information of the record.

ILLUSTRATIONS/EXAMPLES:

*Example 1***:** The Hospital maintains a database on the provision of twenty-hours of active treatment for each patient per regulatory requirements. Staff on each unit have read only access to the data pertinent only to their assigned patients. In addition, certain designated staff on each

unit, have been granted access for data entry purposes, based on their assigned responsibilities therefore meeting the minimum necessary standard.

*Example 2***:** In a hospital setting, a nursing station is used as a central communication area. Oral communications are made with discretion to avoid public disclosure of protected health information. The medical records and computer screens are set up to avoid inadvertent disclosure or public display. Whiteboards or other display material with patient identifying information are not located in a public area or are moved away from public view**.**

Example 3: A DMHAS agency conducts a particular audit to ensure that for each service submitted for data entry, there is an accompanying progress note in the medical record. A social worker is not directly involved in the care of the client whose chart is being reviewed, but is a member of the audit team. That staff should only be reviewing the client's service code record and progress note section, but has no need to be looking at other sections of the medical record, i.e., correspondence, intake information, etc.

DISCLOSURES TO PERSONAL REPRESENTATIVES

POLICY:

It is the policy of the Agency that if a person has the legal authority to act on behalf of a service recipient in making decisions related to healthcare, the Agency shall treat such person as a personal representative with respect to Protected Health Information (PHI.)

If an executor, administrator, or other person has the legal authority to act on behalf of a deceased service user or of the service user's estate, the Agency shall treat such person as a personal representative with respect to the patient/client's PHI.

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

1. The facilities/statewide programs shall review their existing policies and procedures on releases of PHI to determine if they include a section on disclosures of PHI to legally authorized personal representatives of clients. If there is not an existing policy, one should be inserted within an appropriate existing policy, or a separate policy developed which reflects the areas covered in the statements above.

2. The facilities/statewide programs may decline to treat a person as a personal representative of a service recipient if:
    a) The facilities/statewide programs have a reasonable belief that:
        i. The patient/client has been or may be subjected to abuse, or neglect by such person; or
        ii. Treating such person as the personal representative could endanger the patient/client; and
    b) The facilities/statewide programs, in the exercise or professional judgment, decides that it is not in the best interest of the patient/client to treat the person as the patient/client's personal representative.

Refer to the Verification Policy for criteria to identify that a person has legal authority to act on behalf of a patient/client.

ILLUSTRATION/EXAMPLE:

Example: In a psychiatric hospital a legally appointed Conservator of Person of a patient requests disclosure of an evaluation from the patient's medical record. The Conservator presents a copy of the legal document verifying their authority as a personal representative to the Medical Records Department, along with a release form. The Medical Records Department releases the record.

USES AND DISCLOSURES REQUIRED BY LAW FOR RESEARCH

POLICY:

It is the policy of the Agency to use or disclose Protected Health Information (PHI) for research purposes in full compliance with all applicable state and federal laws and regulations. The confidentiality rights of the service recipient are held in the highest regard by the Agency at all times.

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

The facilities/statewide programs may use or disclose PHI for research if at least one of the following criteria is met:

1. The facilities/statewide programs obtain documentation that an alteration to or waiver, in whole or in part, of the individual authorization has been approved by the facilities/statewide program's Institutional Review Board (IRB.)

2. The facilities/statewide programs obtain from the researcher representations that:
    a) Use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;
    b) No PHI is to be removed from the facility/statewide program by the researcher in the course of the review; and,
    c) The PHI for which use or access is sought is necessary for the research purposes.

3. The facilities/statewide programs obtain from the researcher:
    a) Representation that the use or disclosure is sought solely for research on the PHI of decedents;
    b) Documentation, at the request of the facility/statewide program, of the death of such individuals; and,
    c) Representation that the PHI for which use or disclosure is sought is necessary for the research purposes.

For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, the documentation must include all of the following:

1. A statement identifying the IRB and the date on which the alteration or waiver of authorization was approved; and,
2. A statement that the IRB has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:
    a) The use or disclosure of PHI involves no more than minimal risk to the individuals;

b) The alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals;
c) The research could not practicably be conducted without the alteration or waiver;
d) The research could not practicably be conducted without access to and use of the PHI;
e) The privacy risks to individuals whose PHI is to be used or disclosed are reasonable in relation to the anticipated benefits if any to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research;
f) There is an adequate plan to protect the identifiers from improper use and disclosure;
g) There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; and,
h) There are adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted.

A brief description of the PHI needed will be required describing which use or access has been determined to be necessary by the IRB.

A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows: An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)); or, The expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110); and, The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB.

ILLUSTRATIONS/EXAMPLES:

Example: A researcher requests identified data on individuals who have received services in the past but who are not currently available to sign a release form. Access may be granted if the IRB finds that such release of information is acceptable under the HIPAA privacy regulation and 45 CFR 46.

DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION

POLICY:

It is the policy of the Agency to de-identify Protected Health Information (PHI) as warranted by the request for disclosure.

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

The facilities/statewide programs shall determine that health information is not individually identifiable only if:

1. A person with appropriate knowledge of, and experience with generally accepted statistical and scientific principles, determines that the risk is very small that the information could be identifiable and documents the methods and results of the analysis that justify such determinations; or,
2. The information identifiers of the service user or of relatives, employers or household members of the service user, are removed. These identifiers include:
   a) Names;
   b) All geographic subdivisions including address and zip code;
   c) All dates, except year, including birth date, admission date, discharge date, date of death;
   d) Telephone numbers;
   e) Fax numbers;
   f) Electronic mail addresses;
   g) Social security numbers;
   h) Medical record numbers;
   i) Health plan beneficiary numbers;
   j) Account numbers;
   k) Certificate/license numbers;
   l) Vehicle identifiers and serial numbers, including license plate numbers;
   m) Device identifiers and serial numbers;
   n) Web Universal Resource Locators (URL's);
   o) Internet Protocol (IP) address numbers;
   p) Biometric identifiers, including finger and voice prints;
   q) Full face photographic images and comparable images;
   r) Any other unique identifying number, characteristic, or code; and,
3. The facilities/statewide programs do not have actual knowledge that the information could be used alone or in combination with other information to identify a patient/client who is a subject of the information.

The facilities/statewide programs may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the facilities/statewide programs, provided that:

1. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and,
2. The facilities/statewide programs do not use or disclose the code or other means of record identification for any other purpose, and do not disclose the mechanism for re-identification.

The facilities/statewide programs shall assign an individual responsible for determining that the information that is finally released, complies with all aspects of this policy.

ILLUSTRATIONS/EXAMPLES:

Example 1: The facility/statewide program receives a request for information on medication errors from the Office of the Commissioner (OOC) for performance improvement purposes. The Pharmacy and Therapeutics Committee, with assistance from MIS, de-identifies the data requested prior to its' submission and clears the data prior to its release with the individual responsible for compliance with this policy.

Example 2: The facility/statewide program receives a request from Yale University who are conducting a study on the number of admissions, by month, for severe depression. The facility/statewide program in turn requests this information from the OOC where the data is compiled and all patient identifiable information is removed. A report is then submitted back to the facility/statewide program with the aggregate data that was requested. This data is then forwarded to Yale University.

LIMITED DATA SET

POLICY:

It is the policy of the Agency to utilize a Limited Data Set (LDS), whenever possible, while performing research and healthcare operation activities. The LDS will not contain any of the following Protected Health Information (PHI):

1. Names;
2. Postal address information, other than town or city, state, and zip code;
3. Telephone number;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate and/or license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints; or
16. Full-face photographic images and comparable images.

GUIDELINES FOR PROCEDURAL DEVELOPMENT:

1. When utilizing patient records (electronic or physical) for review of healthcare operations (such as quality assurance reviews) or research, the facility/statewide program should attempt to use de-identified information where possible. If this is not practical, then the agency may use a LDS.

2. If a LDS cannot be used and the project is a research project, the project should be performed under an Institutional Review Board. If a LDS cannot be used and the project is a review of healthcare operations, then the full patient record (electronic or physical) can be used, but solely for the purpose of the review.

ILLUSTRATION/EXAMPLE:

Example: The facility/statewide program is in the process of carrying out a peer review of several of its' providers. In doing so, it wishes to review the relative frequency of a diagnosis by

zip code. The facility/statewide program has a large database of electronic billing records that it can use to make this determination. As the only PHI required in this scenario is a zip code, the facility/statewide program could extract the diagnosis code by zip code excluding any of the PHI named in the above list. However, if it is felt that it *may* be possible to identify a patient from a given zip code, this patient's data *shall* be excluded from the LDS.

PROVISION OF BUSINESS ASSOCIATE CONTRACT LANGUAGE FOR PROTECTED HEALTH INFORMATION

POLICY:

It is the policy of the Agency, in order to ensure the continued privacy protections for all service user Protected Health Information (PHI) during the contracting process, that the Agency will enter appropriate Business Associate (BA) language into all contracts, where PHI is created or received, to appropriately safeguard the service recipient's PHI.

PROCEDURES:

The Agency will work with the State of Connecticut Office of the Attorney General and the Office of Policy and Management to obtain Business Associate Agreement language for use in all Human Service Contracts, Human Service Agreements, Personal Service Agreements and Memoranda of Understanding where the BA performs, or assists in the performance of a function or activity involving the use or disclosure of PHI.

The Agency will review all Human Service Contracts, Human Service Agreements, Personal Service Agreements and Memoranda of Understanding to determine which documents shall contain the authorized Business Associate Agreement language.

The agency will identify for state-operated facilities, statewide programs and for the agency all Human Service Contracts, Human Service Agreements, Personal Service Agreements and Memoranda of Understanding that need to be updated with the Business Associate Agreement language. Where appropriate, facilities and statewide programs will be asked to update contracts originated at the facility and/or program level.

All updated Human Service Contracts, Human Service Agreements, Personal Service Agreements and Memoranda of Understanding will be processed through the Purchased Service Unit at the Office of the Commissioner and signed by the Commissioner.

When complaints or other information containing substantial and credible evidence of a violation(s) by a BA are known, facilities and statewide programs should report the complaint or other information to the department's Privacy Officer. The Privacy Officer will assist the statewide program or facility to take reasonable steps to correct the breach or end the violation though the mechanisms defined in the contract and if unsuccessful, after reviewing the situation with the Agency's Chief Operations Officer, to terminate the contract with the BA in conjunction with appropriate personnel and contract mechanisms. If termination is not feasible (e.g., where there are no other viable business alternatives for the BA), the Privacy Officer will report the problem to the Department of Health and Human Services Office for Civil Rights. See 45 CFR 164.504(e)(1).

HUMAN SERVICE CONTRACT

BUSINESS ASSOCIATE LANGUAGE

(*insert § # here for Part I)* **HIPAA Provisions**

(a.) If the Contactor is a Business Associate under HIPAA, the Contractor must comply with all terms and conditions of this Section of the Contract. If the Contractor is not a Business Associate under HIPAA, this Section of the Contract does not apply to the Contractor for this Contract.

(b.) The Contractor is required to safeguard the use, publication and disclosure of information on all applicants for, and all clients who receive, services under the contract in accordance "with all applicable federal and state law regarding confidentiality, which includes but is not limited to the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), more specifically with the Privacy Rule at 45 C.F.R. Part 160 and Part 164, subparts A and E; *and*

(c.) The State of Connecticut Department named on page 1 of this Contract (hereinafter "**Department"**) is a "covered entity" as that term is defined in 45 C.F.R. § 160.103; *and*

(d.) The Contractor, on behalf of the Department, performs functions that involve the use or disclosure of "individually identifiable health information," as that term is defined in 45 C.F.R. § 160.103 ; *and*

(e.) The Contractor is a "business associate" of the Department, as that term is defined in 45 C.F.R. § 160.103; *and*

(f.) The Contractor and the Department agree to the following in order to secure compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), more specifically with the Privacy Rule at 45 C.F.R. Part 160 and Part 164, subparts A and E:

I. Definitions

A. Business Associate. "Business Associate" shall mean the Contractor.

B. Covered Entity. "Covered Entity" shall mean the Department of the State of Connecticut named on page 1 of this Contract.

C. Designated Record Set. "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 C.F.R. § 164.501.

D. Individual. "Individual" shall have the same meaning as the term "individual"' in 45 C.F.R. 164.501 and shall include a person who qualifies as a personal representative as defined in 45 C.F.R. § 164.502(g).

E. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and parts 164, subparts A and E.

F. Protected Health Information. "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in 45 C.F.R. § 164.501, limited to information created or received by the Business Associate from or on behalf of the Covered Entity.

G. Required by Law. "Required by Law"' shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.501.

H. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

I. More Stringent. "More stringent" shall have the same meaning as the term "more stringent" in 45 C.F.R. § 160.103.

J. Section of Contract. "(T)his Section of the Contract" refers to the HIPAA Provisions stated herein, in their entirety.

II. Obligations and Activities of Business Associate

A. Business Associate agrees not to use or disclose PHI other than as permitted or required by this Section of the Contract or as Required by Law

B. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for in this Section of the Contract.

C. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of PHI by Business Associate in violation of this Section of the Contract.

D. Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this Section of the Contract of which it becomes aware.

E. Business Associate agrees to insure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate, on behalf of the Covered Entity, agrees to the same restrictions and conditions that apply through this Section of the Contract to Business Associate with respect to such information.

F. Business Associate agrees to provide access, at the request of the Covered Entity, and in the time and manner agreed to by the parties, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524.

G. Business Associate agrees to make any amendments to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of the Covered Entity, and in the time and manner agreed to by the parties.

H. Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by, Business Associate on behalf of Covered Entity, available to Covered Entity or to the Secretary in a time and manner agreed to by the parties or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

I. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

J. Business Associate agrees to provide to Covered Entity, in a time and manner agreed to by the parties, information collected in accordance with paragraph I of this Section of the Contract, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

K. Business Associate agrees to comply with any state law that is more stringent than the Privacy Rule.

III. Permitted Uses and Disclosures by Business Associate

A. General Use and Disclosure Provisions: Except as otherwise limited in this Section of the Contract, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in this Contract, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

B. Specific Use and Disclosure Provisions:

1. Except as otherwise limited in this Section of the Contract, Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

2. Except as otherwise limited in this Section of the Contract, Business Associate may disclose PHI for the proper management and administration of

Business Associate, provided that disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3. Except as otherwise limited in this Section of the Contract, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. § 154.514(e)(2)(i)(B).

IV. Obligations of Covered Entity

A. Covered Entity shall notify Business Associate of any limitations in its notice of privacy practices of Covered Entity, in accordance with 45 C.F.R. 164.520, or to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

B. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

C. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

V. Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by the Covered Entity, except that Business Associate may use and disclose PHI for data aggregation, and management and administrative activities of Business Associate, as permitted under this Section of the Contract.

VI. Term and Termination

A. **Term.** The Term of this Section of the Contract shall be effective as of the date the Contract is effective and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.

B. **Termination for Cause**. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Contract if Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity; or

2. Immediately terminate the Contract if Business Associate has breached a material term of this Section of the Contract and cure is not possible; or

3. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

C. Effect of Termination.

1. Except as provided in paragraph (2) of this subsection C, upon termination of this Contract, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

2. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon documentation by Business Associate that return of destruction of PHI is infeasible, Business Associate shall extend the protections of this Section of the Contract to such PHI and limit further uses and disclosures of PHI to those purposes that make return or destruction infeasible, for as long as Business Associate maintains such PHI. Infeasibility of the return or destruction of PHI includes, but is not limited to, requirements under state or federal law that the Business Associate maintains or preserves the PHI or copies thereof.

VII. Miscellaneous Provisions

A. Regulatory References. A reference in this Section of the Contract to a section in the Privacy Rule means the section as in effect or as amended.

B. Amendment. The Parties agree to take such action as in necessary to amend this Section of the Contract from time to time as is necessary for Covered Entity to comply with requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

C. Survival. The respective rights and obligations of Business Associate under Section VI, Subsection C of this Section of the Contract shall survive the termination of this Contract.

D. Effect on Contract. Except as specifically required to implement the purposes of this Section of the Contract, all other terms of the contract shall remain in force and effect.

E. Construction. This Section of the Contract shall be construed as broadly as necessary to implement and comply with the Privacy Standard. Any ambiguity in this Section of the Contract shall be resolved in favor of a meaning that complies, and is consistent with, the Privacy Standard.

F. Disclaimer. Covered Entity makes no warranty or representation that compliance with this Section of the Contract will be adequate or satisfactory for Business Associate's own purposes. Covered Entity shall not be liable to Business Associate for any claim, loss or damage related to or arising from the unauthorized use or disclosure of PHI by Business Associate or any of its officers, directors, employees, contractors or agents, or any third party to whom Business Associate has disclosed PHI pursuant to paragraph II D of this Section of the Contract. Business Associate is solely responsible for all decisions made, and actions taken, by Business Associate regarding the safeguarding, use and disclosure of PHI within its possession, custody or control.

G. Indemnification. The Business Associate shall indemnify and hold the Covered Entity harmless from and against all claims, liabilities, judgments, fines, assessments, penalties, awards, or other expenses, of any kind or nature whatsoever, including, without limitation, attorney's fees, expert witness fees, and costs of investigation, litigation or dispute resolution, relating to or arising out of any violation by the Business Associate and its agents, including subcontractors, of any obligation of Business Associate and its agents, including subcontractors, under this Section of the Contract.

THIS MUST BE INSERTED INTO EACH Purchase of Services Contract on the signature page:

The Contractor herein IS / IS NOT a Business Associate under HIPAA*:
*(circle one**)*

Authorized signatory for the contractor	***Authorized signatory for (agency abbreviation)***
(Typed name and title)	***(Typed name and title)***
Date	***Date***

** per Part I, Section (whatever section of Part I this ends up to be ...) of this contract*

*** Department must make this determination before Contract is signed.*

PERSONAL SERVICE AGREEMENT
HUMAN SERVICE AGREEMENT

BUSINESS ASSOCIATE LANGUAGE

(*insert § # here for contract)* **HIPAA Provisions**

(a.) The Contractor herein is / is not a Business Associate under HIPAA:

Authorized signatory for the contractor	***Authorized signatory for DMHAS***
	Thomas A. Kirk, Jr., Ph.D., Commissioner
(Typed name and title)	***(Typed name and title)***
Date	***Date***

The Contactor, as a Business Associate under HIPAA, must comply with all terms and conditions of this Section of the Contract. *(Delete this sentence if the Contractor is NOT a Business Associate under HIPAA)*

If the Contractor is not a Business Associate under HIPAA, this Section of the Contract does not apply to the Contractor for this Contract.

(b.) The Contractor is required to safeguard the use, publication and disclosure of information on all applicants for, and all clients who receive, services under the contract in accordance "with all applicable federal and state law regarding confidentiality, which includes but is not limited to the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), more specifically with the Privacy Rule at 45 C.F.R. Part 160 and Part 164, subparts A and E; *and*

(c.) The Connecticut Department of Mental Health and Addiction Services (hereinafter "DMHAS**"**) is a "covered entity" as that term is defined in 45 C.F.R. § 160.103; *and*

(d.) The Contractor, on behalf of DMHAS, performs functions that involve the use or disclosure of "individually identifiable health information," as that term is defined in 45 C.F.R. § 160.103; *and*

(e.) The Contractor is a "business associate" of DMHAS, as that term is defined in 45 C.F.R. § 160.103; *and*

(**f.**) The Contractor and DMHAS agree to the following in order to secure compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), more specifically with the Privacy Rule at 45 C.F.R. Part 160 and Part 164, subparts A and E:

I. Definitions

A. Business Associate. "Business Associate" shall mean the Contractor.

B. Covered Entity. "Covered Entity" shall mean DMHAS.

C. Designated Record Set. "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 C.F.R. § 164.501.

D. Individual. "Individual" shall have the same meaning as the term "individual"' in 45 C.F.R. 164.501 and shall include a person who qualifies as a personal representative as defined in 45 C.F.R. § 164.502(g).

E. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and parts 164, subparts A and E.

F. Protected Health Information. "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in 45 C.F.R. § 164.501, limited to information created or received by the Business Associate from or on behalf of the Covered Entity.

G. Required by Law. "Required by Law"' shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.501.

H. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

I. More Stringent. "More stringent" shall have the same meaning as the term "more stringent" in 45 C.F.R. § 160.103.

J. Section of Contract. "(T)his Section of the Contract" refers to the HIPAA Provisions stated herein, in their entirety.

II. Obligations and Activities of Business Associate

A. Business Associate agrees not to use or disclose PHI other than as permitted or required by this Section of the Contract or as Required by Law

B. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for in this Section of the Contract.

C. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of PHI by Business Associate in violation of this Section of the Contract.

D. Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this Section of the Contract of which it becomes aware.

E. Business Associate agrees to insure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate, on behalf of the Covered Entity, agrees to the same restrictions and conditions that apply through this Section of the Contract to Business Associate with respect to such information.

F. Business Associate agrees to provide access, at the request of the Covered Entity, and in the time and manner agreed to by the parties, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524.

G. Business Associate agrees to make any amendments to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of the Covered Entity, and in the time and manner agreed to by the parties.

H. Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by, Business Associate on behalf of Covered Entity, available to Covered Entity or to the Secretary in a time and manner agreed to by the parties or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

I. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

J. Business Associate agrees to provide to Covered Entity, in a time and manner agreed to by the parties, information collected in accordance with paragraph I of this Section of the Contract, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

K. Business Associate agrees to comply with any state law that is more stringent than the Privacy Rule.

III. Permitted Uses and Disclosures by Business Associate

A. General Use and Disclosure Provisions: Except as otherwise limited in this Section, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in this Contract, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

B. Specific Use and Disclosure Provisions:

1. Except as otherwise limited in this Section of the Contract, Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

2. Except as otherwise limited in this Section of the Contract, Business Associate may disclose PHI for the proper management and administration of Business Associate, provided that disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3. Except as otherwise limited in this Section of the Contract, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. § 154.514(e)(2)(i)(B).

IV. Obligations of Covered Entity

A. Covered Entity shall notify Business Associate of any limitations in its notice of privacy practices of Covered Entity, in accordance with 45 C.F.R. 164.520, or to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

B. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

C. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

V. Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by the Covered Entity, except that Business Associate may use and disclose PHI for data aggregation,

and management and administrative activities of Business Associate, as permitted under this Section.

VI. Term and Termination

A. Term. The Term of this Section of the Contract shall be effective as of the date the Contract is effective and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.

B. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Contract if Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity; or

2. Immediately terminate the Contract if Business Associate has breached a material term of this Section of the Contract and cure is not possible; or

3. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

C. Effect of Termination.

1. Except as provided in paragraph (2) of this subsection C, upon termination of this Contract, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

2. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon documentation by Business Associate that return of destruction of PHI is infeasible, Business Associate shall extend the protections of this Section of the Contract to such PHI and limit further uses and disclosures of PHI to those purposes that make return or destruction infeasible, for as long as Business Associate maintains such PHI. Infeasibility of the return or destruction of PHI includes, but is not limited to, requirements under state or federal law that the Business Associate maintains or preserves the PHI or copies thereof.

VII. Miscellaneous Provisions

A. Regulatory References. A reference in this Section of the Contract to a section in the Privacy Rule means the section as in effect or as amended.

B. Amendment. The Parties agree to take such action as in necessary to amend this Section of the Contract from time to time as is necessary for Covered Entity to comply with requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

C. Survival. The respective rights and obligations of Business Associate under Section VI, Subsection C of this Section of the Contract shall survive the termination of this Contract.

D. Effect on Contract. Except as specifically required to implement the purposes of this Section of the Contract, all other terms of the contract shall remain in force and effect.

E. Construction. This Section of the Contract shall be construed as broadly as necessary to implement and comply with the Privacy Standard. Any ambiguity in this Section of the Contract shall be resolved in favor of a meaning that complies, and is consistent with, the Privacy Standard.

F. Disclaimer. Covered Entity makes no warranty or representation that compliance with this Section of the Contract will be adequate or satisfactory for Business Associate's own purposes. Covered Entity shall not be liable to Business Associate for any claim, loss or damage related to or arising from the unauthorized use or disclosure of PHI by Business Associate or any of its officers, directors, employees, contractors or agents, or any third party to whom Business Associate has disclosed PHI pursuant to paragraph II D of this Section. Business Associate is solely responsible for all decisions made, and actions taken, by Business Associate regarding the safeguarding, use and disclosure of PHI within its possession, custody or control.

G. Indemnification. The Business Associate shall indemnify and hold the Covered Entity harmless from and against all claims, liabilities, judgments, fines, assessments, penalties, awards, or other expenses, of any kind or nature whatsoever, including, without limitation, attorney's fees, expert witness fees, and costs of investigation, litigation or dispute resolution, relating to or arising out of any violation by the Business Associate and its agents, including subcontractors, of any obligation of Business Associate and its agents, including subcontractors, under this Section of the Contract.

MEMORANDUM OF UNDERSTANDING

BUSINESS ASSOCIATE LANGUAGE

MEMORANDUM OF UNDERSTANDING

BETWEEN
(Name of Entity)
AND
THE DEPARTMENT OF MENTAL HEALTH AND ADDICTION SERVICES
AS BUSINESS ASSOCIATES UNDER HIPAA

WHEREAS, the (Name of entity) serves as the entity for certain services provided through the Department of Mental Health and Addiction Services ("DMHAS").

WHEREAS, (Name of entity) is a covered entity as those terms are defined under 45 C.F.R. § 160.103;

WHEREAS, for these purposes DMHAS is a "healthcare provider" and a "covered entity" as those terms are defined in 45 C.F.R. § 160.103;

WHEREAS, (Name of entity), on behalf of DMHAS, performs functions that involve the use or disclosure of "individually identifiable health information," as that term is defined in 45 C.F.R. § 160.103;

WHEREAS, (Name of entity) is a "business associate" of DMHAS, as the term "business associate" is defined in 45 C.F.R. § 160.103;

WHEREAS, (Name of entity) and DMHAS wish to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), more specifically with the Privacy Rule at 45 C.F.R. Part 160 and Part 164, subparts A and E;

NOW THEREFORE, the (Name of entity) and DMHAS agree to the following:

I. **Definitions**

A. Business Associate. "Business Associate" shall mean (Name of entity.)

B. Covered Entity. "Covered Entity" shall mean DMHAS.

C. Designated Record Set. "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 C.F.R. § 164.501.

D. Individual. "Individual" shall have the same meaning as the term "individual"' in 45 C.F.R. § 164.501 and shall include a person who qualifies as a personal representative as defined in 45 C.F.R. § 164.502(g).

E. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, subparts A and E.

F. Protected Health Information. "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in 45 C.F.R. § 164.501, limited to information created or received by the Business Associate from or on behalf of the Covered Entity.

G. Required by Law. "Required by Law"' shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.501.

H. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

II. **Obligations and Activities of Business Associate**

A. Business Associate agrees not to use or disclose PHI other than as permitted or required by this MOU or as Required by Law.

B. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for in this MOU.

C. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of PHI by Business Associate in violation of this MOU.

D. Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this MOU of which it becomes aware.

E. Business Associate agrees to insure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate, on behalf of the Covered Entity, agrees to the same restrictions and conditions that apply through this MOU to Business Associate with respect to such information.

F. Business Associate agrees to provide access, at the request of the Covered Entity, and in the time and manner agreed to by the parties, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524.

G. Business Associate agrees to make any amendments to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of the Covered Entity, and in the time and manner agreed to by the parties.

H. Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by, Business Associate on behalf of Covered Entity, available to Covered Entity or to the Secretary in a time and manner agreed to by the parties or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

I. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

J. Business Associate agrees to provide to Covered Entity, in a time and manner agreed to by the parties, information collected in accordance with paragraph I of this section of the MOU, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

III. Permitted Uses and Disclosures by Business Associate

A. General Use and Disclosure Provisions

Except as otherwise limited in this MOU, Business Associate may use or disclose PHI on behalf of, or to provide services to, the Covered Entity for the following purposes if such use or disclosure of PHI would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

B. Specific Use and Disclosure Provisions

A. Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

B. Business Associate may disclose PHI for the proper management and administration of Business Associate, provided that disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

C. Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. § 154.514(e)(2)(i)(B).

IV. Obligations of Covered Entity

A. Covered Entity shall notify Business Associate of any limitations in its notice of privacy practices of Covered Entity, in accordance with 45 C.F.R. 164.520, or to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

B. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

C. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

V. **Permissible Requests by Covered Entity**

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by the Covered Entity, except that Business Associate may use and disclose PHI for data aggregation, and management and administrative activities of Business Associate, as permitted under this MOU.

VI. **Miscellaneous Provisions**

A. This MOU shall be in effect from the time of its execution and shall automatically renew for each fiscal year period thereafter unless terminated by the mutual written agreement of both parties.

B. Changes to the MOU may be made only by the mutual written agreement of both parties.

C. Business Associate shall provide the Auditors of Public Accounts with a copy of the MOU. Business Associate and Covered Entity shall, respectively, accept responsibility for responding to audit findings that relate to it, arising from areas covered under this MOU.

FOR: (Name of entity)	FOR: DEPARTMENT OF MENTAL HEALTH AND ADDICTION SERVICES
_____ _____ (Signature) Date (Title)	_____ _____ Thomas A. Kirk, Jr., Ph.D. Date Commissioner

GLOSSARY OF DEFINITIONS

Business Associate. A person or entity who on behalf of the Agency, but not in the capacity of a workforce member, performs or assists in the performance of a function or activity involving the use or disclosure of PHI; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services involving disclosure of PHI.

Correctional institution. Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial

Covered Entity (CE). A health plan, a healthcare clearinghouse, or a healthcare provider that transmits any health information in electronic form relating to any healthcare transaction.

Covered functions. Those functions of a covered entity the performance of which makes the entity a health plan, healthcare provider, or healthcare clearinghouse.

Data aggregation. With respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the healthcare operations of the respective covered entities.

Designated Record Set. A group of records maintained by or for a CE that is: the medical and billing records relating to an individual maintained by or for a healthcare provider; the enrollment, payment, claims adjudication, and case or medical management systems maintained by or for a health plan, or; used, in whole or in part, by or for a CE to make decisions about individuals.

Disclosure. The release, transfer, provision of access to, or the divulging in any other manner of information outside the agency holding the information.

Healthcare. Care, services, or supplies related to the health of an individual. Healthcare includes, but is not limited to, the following:
(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription

Healthcare clearinghouse. A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:
(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health information. Any information, whether oral or recorded in any form or medium, that:
(1) Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.

Health Oversight Agency. A governmental agency or authority, or a person or entity acting under a grant of authority from or a contract with such a public agency, including the employees or agents of the public agency, its contractors and those to whom it has granted authority, that is authorized by law to oversee the public or private healthcare system or government programs in which health information is necessary to determine eligibility or compliance.

Hybrid Entity. A single legal entity that is a CE whose covered functions are not its primary functions.

Indirect treatment relationship. A relationship between an individual and a healthcare provider in which:
(1) The healthcare provider delivers healthcare to the individual based on the orders of another healthcare provider; and
(2) The healthcare provider typically provides services or products, or reports the diagnosis or results associated with the healthcare, directly to another healthcare provider, who provides the services or products or reports to the individual.

Individually Identifiable Health Information. Information that is a subset of health information, including demographic information collected from an individual, and that: (1) Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual, and (3) Which identifies the individual, or (4) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual. Note: Individually identifiable health information is to be treated as protected health information.

Personal Representative. A person who has authority under applicable law to make decisions related to healthcare on behalf of a service recipient.

Privacy Notice. The notice of privacy practices relating to the agency's use and disclosure of PHI that is mandated under HIPAA regulations for distribution to all individuals whose information will be collected by or on behalf of the agency.

Protected Health Information (PHI). Individually identifiable information relating to past, present or future physical or mental health or condition of an individual, provision of healthcare to an individual, or the past, present or future payment for healthcare provided to an individual.

Public Health Authority. A governmental agency or authority, or a person or entity acting under a grant of authority from or a contract with such a public agency, including the employees or agents of the public agency, its contractors and those to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Public Official. An employee or agent of a governmental agency or authority, its contractors and those to whom it has granted authority, acting in their official capacity.

Treatment, Payment and Healthcare Operations (TPO). Includes all of the following:

- **Treatment.** The provision, coordination, or management of healthcare and related services, consultation between providers relating to an individual, or referral of an individual to another provider for healthcare.
- **Payment.** Activities undertaken to obtain or provide reimbursement for healthcare, including determinations of eligibility or coverage, billing, collections activities, medical necessity determinations and utilization review.
- **Healthcare Operations.** Includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of healthcare professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities.

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

Workforce Members. Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Agency, is under the direct control of the Agency, regardless of whether they are paid by the Agency.