Table of Contents

Introduction

The MHA HIPAA Policy

Policies;

Uses and Disclosures:

1 For treatment, payment, and Health Care Operations (TPO)

2 Authorizations

3 Opportunity for the Individual to Agree or Object

4 No Permission Required

5 Business Associate

6 The Designated Record Set and PHI

7 Privacy Notice

8 Minimum Necessary

9 De-Identification Limited Data Sets

Individual's Rights:

10 Individual's Right to Access

11 Individual's Right to Amendment PHI

12 Individual's Right to an Accounting of Disclosures of PHI

13 Other Individual Rights —Right to Restrict Uses and Disclosures of PHI

14 Other Individual Rights - Confidential Communications

Administrative-requirements:

15 Documentation

16 Complaint Process

17 Training of the Workforce

Administrative Safeguards

I8 Personnel

19 Chain of Trust Agreements

20 Contingency Planning

21 Audit Controls and Internal Audit

22 Workforce-related Security Measures

23 Access Control

24 Data and Entity Authentication

Appendices:

A. Glossary of Key HIPAA — Related Terms

B. Health Privacy Project Reports
Connecticut
Massachusetts

C. Notice of Privacy Practices [see Policy 7] and Summary of MHA Notice of Privacy Practices [Abbreviated Notice for Discussion Purposes]

D. Acknowledgement of Review of Notice of Privacy Practices

E. Matrix of Disclosure [supplement to Policy 4]

F. Model Authorization Form plus Model Substance Abuse Re-disclosure Notice [see Policy 2)

G. Generic Authorization for Disclosure of Protected Health Information plus Model Substance Abuse Re-disclosure Notice [alternative to Form F)

Revised by MHA 07/15/09

H. Clear and Present Danger Disposition Sheet A: Danger to Self *[Optional]* [see Policy 4]

I. Clear and Present Danger Disposition Sheet B: Danger to Others *[Optional]* [see Policy 4]

J. Request for Accounting of PHI Disclosed by Agency [see Policy 12]

K. Client Restriction on Uses and Disclosures of PHI for Treatment, Payment or Operations [see Policy 13)

L. Form 1 & 2— Business Associate Agreement [see Policy 5]

M. Acknowledgement of Review of MHA Privacy Policies and Procedures [see Policy 17

INTRODUCTION

The Mental Health Association, Inc. has produced this manual for Directors of Programs as a resource to use in implementing the Health Insurance Portability and Accountability Act (HIPAA) throughout the agency.

The first section in this manual is the MHA HIPAA Policy, which presents the overall agency policy regarding client or consumer rights and the agency's rights and responsibilities related to health care information. That policy also recognizes the key role of the Director in overseeing and administering the uses and disclosures of protected health information (PHI) and in managing our work environment to adequately safeguard information. Our policy also recognizes that in Massachusetts and Connecticut, state law which pre-existed HIPAA may impose higher standards upon us than does HIPAA, and that we have an obligation to uphold those higher state standards.

The main body of this manual contains 24 policies, grouped into four areas:

- Uses and Disclosures of Protected Health Information (PHI),
- Individuals' Rights Related to their own PHI,
- Administrative Requirements of the Agency, and
- Administrative Safeguards.

The policies are intended to be brief, however, of legal necessity, some are a bit lengthy. Please refer to these when you have specific questions on policy. Each of the 24 policies is tabbed numerically for ease of reference.

The final section of the manual includes appendices with various components. The first appendix provides a glossary of key HIPAA terms, to clarify some of the jargon specific to this law. The next section includes reports from the Health Privacy Project of Georgetown University. These reports explain as briefly as possible the areas of Massachusetts and Connecticut state laws, which pre-exist HIPAA and govern privacy of health related information. These are the best available resources to help you when confronted with an apparent "conflict of laws." This section also includes a matrix for quick reference on the various categories of information disclosure and how to handle each. Forms comprise the bulk of this section; each form is referenced to the specific policy, which requires its use. Of all the forms, the most critical is the "Notice of Privacy Practices"; please read this and become familiar with its contents, as the 24 policies all relate to this one notice. The appendix sections are tabbed alphabetically.

Revised by MHA 07/15/09

Policy: MHA HIPAA

Applicability: All Staff

Purpose: To comply with the Health Insurance and Portability Act of 1996, generally known as HIPAA.

Effective Date: January 2010

The services delivered by MHA to its clients and consumers bring the agency under the jurisdiction of the Health Insurance and Portability Act of 1996, generally known as HIPAA. The purpose of HIPAA is to enumerate and protect the rights of individuals' privacy in matters of their health care and information pertaining to it, and to enumerate the responsibilities of entities which deliver health care services and process personal individually identifiable health care information because MHA considers itself a "covered entity" under HIPAA, it intends to comply with the Administrative Simplification Provisions of HIPAA which encompass:

- Privacy of Individually Identifiable Health Information Standards,
- Security and Electronic Signature Standards, and
- Electronic Transactions and Code Set Standards.

To comply with these provisions of HIPAA, MHA and its programs will adapt the above standards, and insure that their employees are aware of these standards and adhere to them in the conduct of our business. Furthermore, MHA will hold those business entities which qualify as its "business associates" to adhere to the same standards, and to enter into Business Associate Agreements and, as necessary, Chain of Trust Agreements, which will contractually bind such parties to uphold the standards promulgated under HIPAA.

In accordance with implementation dates set by the federal government, MHA will implement the Privacy and Security Standards effective January 1, 2010, and the Electronic Transaction and Code Set Standards effective January 1, 2010. MHA will provide its programs with a core set of HIPAA Policies which provide in detail the elements of HIPAA standards which apply to MHA, as well as standard forms which must be used to assure uniform compliance with HIPAA requirements for notice and accountability. At the program level, the Director of Programs is responsible for HIPAA compliance, and as such serve in the capacity of a "privacy officials" for the programs.

Specifically MHA Programs will:

- Review and as necessary update their policies and procedures to ensure that they meet minimum HIPAA standards.
- Post privacy notices in appropriate places and ensure that each new and continuing client

is offered a copy of the notice, a short explanation of its main points, and completes a sign-off document.

- Identify any program-specific business associates and ensure that a business associate agreement is signed either by January 1, 2010 or thereafter before beginning the business relationships.

- Ensure that each new and existing staff person receives training on the privacy and security issues appropriate for their program.

It is understood that programs of MHA operate under various licensing requirements of Massachusetts and Connecticut, which may impose more rigorous standards than the federal government promulgates under HIPAA.

MHA will assign specific roles designated in HIPAA to individuals whose existing job responsibilities align most closely with those newly defined roles. The Human Rights Officer will serve as the "Complaints Officer", the Director of Finance will serve as the 'Security Officer", the Director of Programs will serve at the programs and the Director of Finance at the corporate administrative levels will serve respectively as "Privacy Officers".

Policy I Uses and Disclosures: Treatment, Payment and Health Care Operations (TPO)

Purpose

To comply with the Privacy Rule of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the uses and disclosures of PHI from individuals with whom it has a direct treatment relationship.

Policy

MHA will use and disclose PHI of clients for treatment, payment, and health care operations without obtaining explicit permission from those clients. We will use our best efforts to obtain a written acknowledgement from each client that they have received a copy of our Privacy Notice prior to providing treatment.

Individuals receiving treatment have the right to request that we restrict our uses and disclosures of their PHI for treatment, payment, and health care operations. We are not obliged to agree to those restrictions, but, if we do, we must abide by them. Therefore, restrictions will not be granted without the express permission of the Director of Programs, who will evaluate an individual's request and determine:
(a) if the restrictions are reasonable and (b) if it is possible to implement the restriction in our practice. Should the request be granted, the Restriction Form will reflect the restrictions that have been allowed. (See Policy 13 for complete information on Restrictions.)

In all cases where a personal representative requests PHI on behalf of a client, MHA will consider the appropriateness of the request. In any case where we elect not to treat a person as a legal representative, we will do so because:

1. we have a reasonable belief that the client has been or may be subjected to domestic violence, abuse, or neglect by such person; or

2. in the exercise of professional judgment, we decide that it is not in the best interest of the client to treat the person as the client's legal representative.

In any such case, it is our policy to document that decision in the client record.

Federal Regulations governing the confidentiality of substance abuse information (42 CFR, Part 2) are generally more restrictive than HIPAA. Regarding clients of federally-assisted alcohol or drug abuse programs, MHA will always obtain a specific authorization for each disclosure of client records or other information concerning a client except where otherwise permitted by governing federal law.

Documentation retention requirements:
Policies and procedures for use and disclosure of PHI for treatment, payment, and heath care operations.

Policy 2 Uses and Disclosures: Authorizations

Purpose

To comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, this policy sets out the conditions for obtaining from individuals, with whom MHA has a direct treatment relationship, authorization for any use and/or disclosure of PHI that (a) is not related to treatment, payment, or operations, or (b) is not otherwise permitted or required under the Privacy Rule.

Policy

MHA will obtain a signed authorization from clients prior to using or disclosing PHI in those situations in which the Privacy Rules require them. Such authorizations will be in a form that meets the standards of the Privacy Rules and will contain:

1. A description which identifies in a specific and meaningful fashion the information to be used or disclosed;
2. The name or specific ID of the person(s), or class of persons, authorized to make the requested use or disclosure;
3. The name or other specific ID of the person(s), or class of persons, to whom MHA may make the requested use or disclosure; -
4. A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when a client initiates the authorization and does not, or elects not to, provide a statement of the purpose;
5. An expiration date or event that relates to the client and/or the purpose of the use or disclosure. The statement "end of the research study', "none", or similar language is sufficient if the authorization is for a use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository.
6. The signature of the client and the date. If signed by a personal representative, a
- description of the authority of that person to act for the client must be provided

In addition to the core elements listed above, an authorization must contain statements that put the client on notice of all of the following:

1. The client's right to revoke authorization in writing and the exceptions to the right to revoke along with a description of how to revoke. If this information is contained in MHA's Privacy Notice, a reference to the Privacy Notice will suffice.
2. MHA may only condition treatment on obtaining a signed authorization when:

a. It is providing research-related treatment, and the authorization provides for the use or disclosure of PHI for such research; or

b. It is providing treatment solely for the purpose of creating PHI for disclosure to a third party, and the authorization is for the disclosure of PHI to that third party.

3. The potential for PHI disclosed pursuant to the authorization could be subject to redisclosure by the recipient and no longer be protected by the Privacy Rule. (Note: for Substance Abuse PHI, redisclosure is **expressly prohibited**.)

We reserve the right to amend the authorization form as long as it is written in plain English and contains the above, required elements. An authorization that lacks any of these elements is defective and will have no effect therefore, we require that all of these elements be in place in any version of the authorization form that may be developed in the future.

Individuals seeking treatment have the right to refuse to provide authorizations for use and disclosure of their PHI. We may not refuse to treat individuals who withhold their authorization with two exceptions:

1. We may refuse to provide research-related treatment conducted for the use or disclosure of PHI thus created.
2. We may refuse to provide treatment for the purpose of creating PHI to be disclosed to a third party.

Our clients may revoke an authorization at anytime. The revocation must be in writing. Any actions we have taken in reliance on a client's consent will not be affected by the revocation. We are not required, for example, to retrieve PHI that we have disclosed prior to the revocation. Should any employee be informed verbally that a client has revoked an authorization provided to another entity, that employee should immediately inform the Director of Programs.

In accordance with Massachusetts law, MHA will not disclose PHI involving HIV information without first obtaining the client's "written informed consent" for each requested release of the results of an individual's HTLV-III antibody or antigen test or for release of any medical records containing such information. The consent must state the purpose for which the information is being requested and shall be distinguished from written consent for the release of any other medical information.

In any situation where the relevant PHI will require extensive redaction, the individual will be given their entire record so that they can redact prior to disclosure to the requestor of the information. (Note that the client must be permitted to have access, under the Privacy Rules, to

their entire designated record set in these cases or they will not be allowed to perform the redaction.)

In any situation where we have conflicts between two or more authorizations or other forms of legal permission in our possession for the same individual for the use and disclosure of the same PHI, we will attempt to obtain a new conforming written authorization that resolves the conflict between the other documents. When a new authorization cannot be obtained, we will rely upon the most restrictive form of permission in our possession.

Federal regulations governing the confidentiality of substance abuse information (42 CFR, Part 2) are generally more restrictive than HIPAA therefore, we will follow these regulatory requirements concerning disclosure of the PHI of any client in a federally-assisted alcohol or drug abuse program. In any of our federally-assisted alcohol or drug abuse programs, we must always obtain specific authorization for each disclosure of client records or other information concerning a client, unless one of the regulatory exceptions applies. (See Policy I, Uses and Disclosures — the section for Substance Abuse Providers.) The authorization form (called a "consent" form in the substance abuse federal regulations) will meet the regulatory requirements incorporated in the Form attached to this Policy.

Documentation retention requirements include:

Signed authorizations for each requested use and disclosure.

Policies and procedures for authorizations and any changes thereto.

Revocations.

Policy 3 Uses and Disclosures: Opportunity for the Individual to Agree or Object

Purpose

To comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, MHA sets out, in this policy, the conditions for providing clients with an advance opportunity to agree to a particular use or disclosure, or to prevent or restrict it, when the use or disclosure of PHI is (a) involving other people in the individual's care.

or (b) for notification about a client's location, general condition, or death.

Policy

MHA will verbally inform each client, during the intake process, of their right to prevent or restrict us from: (a) disclosing PHI about them to persons involved in their care; and (b) notifying persons about their location, general condition, or death.

With regard to clients who are present and have the capacity to make decisions, PHI may only be disclosed to people involved in their care (meaning relatives, friends, or community support people) if, after informing the client in advance of the anticipated disclosure of PHI, we obtain the client's agreement to disclose PHI to those who may be involved in their care.

If a client has a valid health care proxy appointing an agent to make health care decisions on his/her behalf (See Advance Directive Policy) and it has been determined that the client lacks the capacity to make or communicate health care decisions, the health care agent may be provided any PHI necessary to make informed decisions regarding the clients health care; provided, however, that if the proxy contains a limitation on the agent's decision-making authority, PHI related to the excluded decisions should not be revealed to the health care agent.

A client lacks the capacity to make health care decisions when he/she is unable to understand and appreciate the nature and consequences of health care decisions, including the benefits and risks of, and alternatives to, any proposed health care, and to reach an informed decision. The decision of incapacity must be made by a physician in compliance with the Massachusetts Health Care Proxy law.

If a court has appointed a guardian of the client's person, PHI may be disclosed to the guardian to the extent that the PHI is related to treatment to which the guardian is authorized to consent. Similarly, if a court has duly appointed an anti-psychotic medication monitor, the monitor may have access to any PHI needed to monitor the treatment plan.

If a client is a ward of the state, e.g., DCF has been granted custody of a minor, we will provide PHI to the responsible state agency only as permitted by law.

With regard to clients who are (a) not present or (b) incapacitated or (c) in an emergency situation, we will disclose the minimum necessary PHI to persons involved in the client's care, if we determine in the exercise of our professional judgment that it is in the client's best interests, unless the client is a ward of the state, or has a valid health care proxy, or a court-appointed guardian or medication monitor.

If we decide to disclose PHI to a person involved in the client's care, that person must be a spouse (unless the client is legally separated), a loving family member or partner, or a person identified and authorized by the client to receive PHI about him/her.

When disclosing PHI to persons involved in the client's care, we will limit disclosures to PHI about the current circumstance. In addition, should the care provider believe, in the exercise of their professional judgment, that a disclosure of PHI might cause the patient serious harm, the care provider may withhold PHI from the person involved in their care. Care providers should use their professional judgment about the scope of the persons involvement in the clients care — both to the length of time of that person's involvement and to the depth of disclosure of PHI that is appropriate in a particular circumstance.

In disaster situations, no individual agreement will be required prior to disclosure of PHI to federal, state, or local agencies involved in disaster relief activities. This policy also applies to any private disaster relief organization that is authorized by law or their charters to assist in disaster relief efforts.

Documentation retention requirements include:

1. Policies and procedures for opportunity to agree or object and any changes thereto.

Other policies and procedures to review that are related to this policy:

Privacy notice
Uses and Disclosures for Treatment, Payment and Health Care Operations
Authorizations
Administrative requirements — documentation retention

Policy 4 Uses and Disclosures: No Permission Required

Purpose

To comply with the Privacy Rule of HIPAA's Administrative Simplification provisions, MHA sets out in this policy the conditions for responding to requests for disclosure of PHI in compliance with law and limited to the relevant requirements of the law that do not require the initial authorization by the client.

Policy ~j

MHA has designated its Director of Programs to be responsible for processing all requests for disclosures of PHI related to their respective program's clients from external authorities in compliance with law and limited to the relevant requirements of that law. The MHA Compliance Officer serves as an agency wide resource to assist in decisions on disclosure of PHI in these instances. We recognize that we are not compelled to make disclosures by the Privacy Rule, but that we may do so without fear of further penalty under the Privacy Rule.

Documentation retention requirements include:

1. Policies and procedures for disclosures with no permission required.

Other policies and procedures to review that are related to this policy:

Privacy notice
Authorizations
Administrative requirements — documentation retention

Policy 5 Uses and Disclosures: Business Associates

Purpose

To comply with the Privacy Rule of HIPAA's Administrative Simplification provisions, MHA sets out in this policy the nature of the third party relationships that will be considered to be Business Associates and the requirements for contracting with them.

Policy

Any vendor or independent contractor who proposes to do business with MHA will be subjected to procedures to determine if the vendor or subcontractor is a Business Associate. We will consider any vendor or independent contractor to be a Business Associate if:

1. they perform a function or activity on our behalf that involves the use or disclosure of PHI or provide any legal, actuarial, accounting, consulting, data aggregation or management, administrative, accreditation, or financial services to or for us;

2. they are not involved in the treatment of a client; and

3. they are not providing client-conducted financial transactions.

Any vendor or independent contractor (but not any member of our workforce) who qualifies as a Business Associate will be required to sign a Business Associate Agreement. The Agreement will be in the form attached to this policy.

We will require of our Business Associates assurances of their ability to conduct operations in accordance with the privacy and security standards.

Amendments to the Business Associates Agreement may not be made without the approval of legal counsel.

Protection of our client's health information is important to us, therefore we require our employees to be sensitive to the behavior of our Business Associates and to report any conduct that appears inappropriate.

Documentation retention requirements include:

1. Policies and procedures for Business Associates.
2. Business Associate Agreement template.
3. Executed Business Associate Agreements.

Policy 6 The Designated Record Set and PHI

Purpose

To comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy MHA sets out the elements of the designated record set and the creation and maintenance of data sources that contain protected health information (PHI). This Policy mandates that MHA maintain accurate and complete medical and billing records for each of our clients, so that they can exercise their rights to access, review, and amend their PHI maintained in a designated record set as required under HIPAA.

Policy

MHA requires each program to define its designated record set: and to maintain the defined elements accurately and completely so clients can exercise their rights to access, review, and amend the PHI maintained in their designated record set as required under HIPAA

PHI may be kept in many forms throughout our agency. It is MHA's policy to identify, document, and approve for usage each of the existing repositories of PHI. Unsanctioned maintenance of PHI in any form will lead to disciplinary action.

Examples of PHI are attached for guidance in defining designated record sets.

Examples of PHI and Designated Record Sets

A designated record set which serves as a medical record would include all of the items listed below, and any other records of care that would be appropriate:

1. the clinical diagnostic assessment
2. the psychiatric diagnostic assessment
3. the treatment plan
4. consents for treatment
5. reports from indirect treatment providers
6. functional status assessments
7. medication profiles
8. progress notes and documentation of care provided (for both treatment and reimbursement purposes). (This would not include all residential shift notes or other notes kept in the residential record or in a log book maintained at the site.)
9. multidisciplinary progress notes/documentation
10. content of any consultation with internal or external individuals regarding the client's care
11. nursing assessments
12. orders for diagnostic tests and diagnostic study results
13. practice guidelines that imbed patient data
14. records of physical history and examinations

15. respiratory therapy, physical therapy, speech therapy, occupational therapy records, and any other records of services provided by specialty providers
16. telephone consultation records
17. telephone orders
18. discharge instructions
19. discharge summaries
20. legal documents and correspondence between the agency and the client or others involved in the client's care
21. utilization management or utilization review forms that are used to determine or review level of care decisions including admission, continuing stay, and discharge

The components of the Billing Record designated record set would include:

1. Signature on file
2. Consent to bill third parties
3. Individual Financial Hardship Assessment
4. Copies of any insurance cards and other data on insurance coverage
5. Fee Agreement
6. Requests for prior authorization of services
7. Authorizations for services or other written acknowledgements of client eligibility for services
8. Billing records including dates, services provided, provider, billing and payment records, and other information used to bill or to record and report encounters or services.

Documentation retention requirements include:

Policies and procedures for medical records and PHI

Comments on Definitions

The Privacy Rule contains standards for the use and disclosure of an individual's protected health information (PHI) by covered entities (CEs). It refers often to the terms "designated record set" and "protected health information." These terms are specifically defined in the Privacy Rule and have special meanings that are critical to the rights of individuals to access their records and to the application of privacy protection to health information.

The definition of designated record set includes medical and billing records of individuals that are maintained by or for a health care provider. In addition, the designated record set encompasses enrollment, payment, billing, claims adjudication, case or medical management records systems maintained by or for a health plan. The designated record set also includes any other information that is used, in whole or in part, to make decisions about individuals.

The definition of designated record set generally excludes information used for quality control or peer review — information that is not used to make decisions about individuals from the designated record set. Regardless of its exclusion from the designated record set, it is still PHI.

Protected health information (PHI) is a definition that is built on two other definitions — that of "health information" and of "individually identifiable health information" (IIHI). Both of these definitions are wider in scope than the designated record set and refer to information, oral or recorded in any form or medium, that relates to the provision of healthcare, the payment of healthcare services, or the physical or mental health or condition of an individual (it also includes demographic information). While many aspects of the Privacy Rule apply to all PHI, whether or not it is in a designated record set, certain provisions apply only to the designated record set.

A clear definition of the designated record set and PHI will aid greatly in the administration of the access, accounting and amendment requirements of the Privacy Rule.

Policy 7 Privacy Notice

Purpose

To comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy MHA sets out the conditions for providing notice to clients of our privacy practices.

Policy

The Mental Health Association, Inc. will post a copy of our Privacy Notice, in English and, at the discretion of the Director of Programs, in any other languages deemed necessary to communicate effectively to the cultures we serve, in a prominent position at the front desk or intake area of our program sites. In addition, written copies of these Notices will be available in those locations upon request. Any individual who is unable to read can request that the Notice be read to them.

We will obtain a written acknowledgment of receipt of the Privacy Notice from each individual no later than the date of their first service. Should we fail to obtain the written acknowledgment, we will document the good faith effort we made to obtain the acknowledgment and the reason why we were unable to obtain it.

The Privacy Notice that is in effect will be the Notice that is attached to this Policy. This version of the Notice reflects the privacy practices in place at this time in our Agency.

It is our policy to conform our Privacy Notice to the content specified in the HIPAA Privacy Rule.

We require that revision of our privacy practices may only occur after deliberation by the designated senior management group. Any changes arising from the revision process will be incorporated into the Privacy Notice and distributed to clients before those practices are effective.

Documentation retention requirements include:

- Policies and procedures for the privacy notice
- Each version of the privacy notice appropriately dated
- Acknowledgements of receipt of privacy notice

Attachment to Policy 7: Required Content of Privacy Notice

At the present time, any version of our Privacy Notice must contain all of these items:

1. Header:
   "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.'
2. A description, including sufficient detail to place the individual on notice, and at least one example of the types of uses and disclosures for each of the following purposes — treatment, payment, and health care operations.
3. A description, including sufficient detail to place the individual on notice, of each of the other purposes a covered entity is either required or permitted to use or disclose PHI without the individual's written consent or authorization.

4. A description of any prohibitions or material limitations required by more stringent law.
5. A statement that other uses and disclosures will be made only with the individual's written authorization and that such authorization may be revoked.
6. A statement of the individual's rights with respect to uses and disclosures of PHI and a description of how they may be exercised including:
   a. the right to request restrictions — including a statement that the covered entity is not required to agree to such a restriction;
   b. the right to receive confidential communications of PHI;
   c. the right to inspect and copy PHI;
   d. the right to amend PHI;
   e. the right to receive an accounting of disclosures of PHI; and
   f. the right to obtain a paper copy of the notice upon request.

7. A statement about the covered entity's duties to:
   a. maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices relative to PHI;
   b. abide by the terms of the privacy notice currently in effect; and
   c. when retroactively applying a change in the notice, to provide a statement that it reserves the right to change the terms of its notice and to make the new notice effective for all PHI it maintains; and how it intends to provide individuals with a revised notice

8. A statement that individuals may complain (to the covered entity or DHHS) if they believe their rights have been violated; a brief description of how to file a complaint with the covered entity; and a statement that there will be no retaliation against the individual if a complaint is made.

9. The name, title, and telephone number of the person or office designated as responsible for receiving complaints and providing additional information.

10. The date on which the notice is first in effect which may not be earlier than the date on which the privacy notice is printed or otherwise published.

Summary of the MHA
Notice of Privacy Practices

The MHA Notice of Privacy Practices addresses health information we have about your physical or mental health condition, the provision of your health care, and payment for your health care services. This is called "protected health information" or PHI. This Notice describes how we may use and disclose your PHI. This Notice also describes your rights regarding the PHI we maintain about you. We are required to maintain the privacy of your PHI, and we are required to comply with the terms of our current Notice of Privacy Practices.

We will use and disclose your protected health information (PHI) for:

1. your care and **treatment**, and to assist others involved in your health care,
2. billing or receiving payment for your care, including determining eligibility for coverage under insurance,
3. performing necessary administrative, educational, quality assurance, and business **operations**.

We may use and disclose your PHI, but you may limit this, in special situations, to persons involved in your care, such as family, personal representatives or someone who helps pay for your care, or for disaster relief.

Sometimes **we may be required or permitted by law to use or disclose your PHI without your permission**. For example:

- In emergencies
- For approved research
- As required by federal, state or local law
- To avert a serious threat to health or safety
- For organ and tissue donation, if you are a donor
- Public health activities
- To a health oversight agency for activities authorized by law
- In legal proceedings when required
- For law enforcement
- To medical examiners or funeral directors
- For military and veterans matters
- National security and protective services
- To correctional facilities regarding inmates
- To comply with Workers Compensation law.

Other uses and disclosures of your PHI may be made with your written "authorization," which you have the right to revoke at any time.

Regarding your health information, you have the right to:

- Inspect and copy your PHI upon written request
- Request, in writing, an amendment of your PHI
- Request, in writing, an accounting of disclosures of your PHI
- Request, in writing, a restriction of on use or disclose of your PHI
- Request, in writing, that you wish to be contacted by us using confidential communications.
- Obtain a paper copy of MHA's Notice of Privacy Practices

For individuals who have received treatment, diagnosis or referral for treatment in drug or alcohol abuse programs, **the confidentiality of drug or alcohol abuse records is protected by federal law and regulations.**

If you believe your privacy rights have been violated, you may file a complaint in writing with us or with the Secretary of the U.S. Department of Health and Human Services. To file a complaint with us, contact our Complaint Officer at MHA, 995 Worthington Street, Springfield, MA 01109. We will not retaliate against you for filing a complaint.

We reserve the right to change the terms of our Notice of Privacy Practices.
We will post a copy of the current Notice of Privacy Practices at our main office and at each site where we provide care.

This is a brief summary of the contents of MHA's Notice of Privacy Practices. It does not give a full explanation of the rights and responsibilities addressed in the Notice. You are encouraged to refer to the MHA Notice of Privacy Practices for more information.

Policy 8 Minimum Necessary

Purpose

To comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the process for applying the minimum necessary standards to uses, disclosures, and requests for PHI.

Policy

The minimum necessary standard states that a covered entity must make reasonable efforts to limit the amount of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. Entire medical records cannot be provided for uses, disclosures, or requests where the minimum necessary standards apply — unless the provision of the entire medical record can be specifically justified as being the amount that is reasonably necessary.

MHA will apply the minimum necessary standards to all uses, disclosures, and requests for PHI, except for:

1. disclosures to, or requests, by, a healthcare provider for the purpose of treatment;
2. disclosures to the client;
3. disclosures made pursuant to their authorization;
4. disclosures required to comply with the Privacy Rule; and
5. uses and disclosures required by law to the extent that such disclosure complies with and is limited to the relevant requirements of the law.

Any request we make for entire medical records, other than for treatment purposes, must be justified in writing and made part of the clients [medical) record.

MHA requires all staff to comply with the minimum necessary standard, and if in doubt as to applying that standard to a use, disclosure or request, to seek the counsel of the Director of Programs or the Compliance Officer.

Non-routine, non-recurring disclosures of PHI will be reviewed, prior to release of PHI, by an authorized clinical person, who will make a determination that the minimum necessary PHI is being used or disclosed in accordance with our criteria for non-routine, non-recurring disclosures.

When we receive requests for PHI from external sources, we will generally rely upon the written representation of the requestor that it is requesting the minimum PHI necessary for its purpose. We will rely on the representation of the requestor only when reliance is reasonable. If in our opinion, reliance on the representation of the requestor is not reasonable, we may disregard the representation and make our own determination of the minimum amount of PHI that is necessary for the purpose.

Documentation retention requirements include:

Policies and procedures for minimum necessary

Policy 9 De-identification and Limited Data Sets

Purpose

To comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the process for creating and using de-identified health information and limited data sets.

MHA will create de-identified health information for use or disclosure in any circumstance where that information can be used, effectively and efficiently, in place of PHI. We will consider PHI to be de-identified health information if it meets one of the two following criteria:

1. A qualified statistician, applying generally accepted statistical and scientific principles and methods, has determined that the risk is very small that the information could be used alone, or in combination with other reasonably available information, by an anticipated recipient to identify an individual, and he/she documents the methods and results of the analysis that justify such determination.
2. All of the Critical Identifiers (see list) have been removed and we don't have actual knowledge that the remaining information could be used, alone or with other information, to identify an individual who is the subject of the information.

MHA will create limited data sets for use or disclosure in any circumstance where that information can be used, effectively and efficiently for research, public health or health care operations. We will consider PHI to be in the form of a limited data set if it excludes Critical Identifiers (see list) of our clients, their relatives, employers, or household members.

Any use or disclosure that we make of a limited data set must take place pursuant to a data use agreement, which must include the following requirements:

1. that the limited data set recipient(s) will use or disclose the information for the limited purposes described in the agreement and not further disclose the information in a way that would be inconsistent with the privacy regulation as it would apply to our Agency itself;
2. that only the recipient(s) specified in the agreement may use or receive the limited data set;
3. that the recipient(s) will not use or further disclose the information in a manner that violates the data use agreement or the law and will use appropriate safeguards to prevent any uses or disclosures other than the permitted uses or disclosures;
4. that the recipient(s) will report to the covered entity any use or disclosure of PHI in the limited data set, which is not included in the data use agreement, of which it becomes aware;
5. that the recipient(s) will assure that any subcontractor who is provided with a limited data set agrees to the same restrictions and conditions as apply to the recipient(s); and
6. that the recipient(s) will not identify the information or contact the individuals.

Should we become aware of a pattern of activity or practice by a recipient that constitutes a

material breach of the data use agreement, we will discontinue disclosure to that recipient and report the problem to the Secretary of HHS.

Documentation retention requirements include:

Policies and procedures for de-identification

Statistical documentation supporting a de-identified record set

Critical Identifiers:

1. Names of individual, relatives, or household members;
2. Postal address information, other than town or city, state, but including the last 2 digits of zip code for a geographic area with more than 20,000 people;
3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers
7. Device identifiers and serial numbers;
8. Web Universal Resource Locators (URLs);
9. Internet Protocol address numbers;
10. Biometric identifiers, including finger and voice prints; and full face photographic images and any comparable images.
11. Medical record numbers;
12. Health plan beneficiary numbers;
13. Account numbers;
14. Certificate/license numbers;
15. Vehicle identifiers and serial numbers, including license plate numbers;
16. All elements of dates (including birth, admission and discharge dates, and dates of death), except for the year for all individuals under 90, and all elements of dates for those over 90 except for presentation as a single over-90 category;

    Note: Excluded from Critical Identifiers is a re-identification code, if it is not derived from or related to information about the individual and may not be otherwise translatable to identify the individual. Explanation of the code is not to be included with any information sets which use or include codes.

Policy 10 Individual's Right to Access

Purpose

To comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the processes for requesting, granting, denying, and review of denial, of client requests for access to PHI.

Policy

MHA will consider all requests from our clients, or previous clients, for access to their PHI that is maintained in their designated record set and that is dated after January 1, 2010 We will consider client requests to either inspect or obtain a copy of their PHI for as long as we maintain their PHI in the designated record set.

We will require that clients make their request in writing using the form that has been designed for that purpose (the Access Request Form).

We will deny a client access to PHI — and that denial will not be subject to review — if:

1. the PHI requested is contained in:
    a. psychotherapy notes;
    b. records or documents compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; or
    c. records or documents from clinical laboratories subject to or exempt from the Clinical Laboratory Improvement Act.
2. the PHI is subject to the Federal Privacy Act;
3. the information was obtained under the promise of confidentiality from another person (not a healthcare provider) and the access requested would be reasonably likely to reveal the source of that information;
4. the information was created or obtained in the course of research that involves treatment when the individual agreed to the denial of access for the duration of the research (that includes treatment) when consenting to participate in the research and the client has been informed that access will be reinstated upon completion of the research; or
5. an inmate requests a copy of PHI and it is determined that such a copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or other inmates or the safety of an officer or other person responsible for transporting the inmate. We will provide an inmate with the right to inspect his PHI unless other grounds for denial exist.

We will deny access to any PHI that a licensed healthcare professional determines:

1. exercising professional judgment, is reasonably likely to endanger the life or physical safety of the client or another person;
2. exercising professional judgment, makes reference to another person (not a health care provider) and access is reasonably likely to cause substantial harm to that other person; or
3. has been requested by a personal representative and access by that person is reasonably likely to cause substantial harm to the client or another person.

When denying a client access for any of these three reasons, these denials will be subject to review as described below. In addition, if access to the entire record is denied and the client requests a review of the decision, we will make the entire record available to the client's attorney, with the consent of the client, or to a psychotherapist designated by the individual.

It is our policy to deny clients access to their PHI only infrequently and in unusual circumstances and, when access is denied, it must be for one of the specific reasons listed above. Furthermore, we will provide access, to the extent possible, to any other requested PHI that is not part of the PHI to which access has been denied. We will make an effort to redact the denied PHI from the designated record set and allow inspection or copying of any remaining information.

When a client has been denied access for one of the reasons that is subject to review, it will be our policy to respond in writing giving the basis for denial in plain language within the time period set forth below. We will also inform them of their right to request a review of the denial of access and provide a description of how the client may file a complaint with us or with the Secretary of DHHS.

In any case where the client requests a review, we will promptly refer the denial to another licensed healthcare professional, who has not been directly involved in the denial, for their review. We will also promptly inform the client, in writing, if the reviewer upholds the denial. In those cases where the reviewer permits access, the client will be informed.

When we have agreed to grant access to PHI, we will notify the client and arrange for access within 30 days from the date of the request. Should the PHI requested be maintained off-site, we can take longer to respond, but no more than 60 days from the date of the request. In either case, we can obtain a single, 30-day extension of time in those rare cases where we are unable to respond in the initial time period. We will notify the client of the reasons for delay and the date of completion by means of a written statement.

When we have agreed to inspection of the designated record set, we will arrange a mutually agreeable time and place for the inspection.

When we have agreed to provide copies of the requested PHI, we will confer with the client and determine their preference for the media in which to receive it — paper or electronic (where available). If we cannot agree on how the PHI will be produced then we will produce the PHI in readable hard copy. We will charge a fee for copying the material and for postage, if the copies are to be mailed, and the client will be notified of that charge in the Access Request Form. However, if the individual is requesting the PHI for the purpose of supporting a claim or appeal under the Social Security Actor any Federal or state financial need-based benefit program, we will furnish the PHI within 30 days of the request at no charge to the individual.

It will be our policy to charge for the cost of making the copies both the labor and machine and paper cost — but we will not include in our charges the cost of the retrieval and handling of information nor will we charge for the costs of processing the request. However, if the PHI is prepared by a licensed physician, the copying charge may not exceed $25 per page and the labor costs may not exceed $20 per hour.

We will provide summaries of PHI in those cases where the individual has requested them. We will charge for the costs associated with producing the summary and the client will be notified of that charge in the Access Request Form.

In those cases where we receive a request for PHI that we do not maintain, but we know where it is maintained, we will inform the client of the location of the PHI.

Documentation retention requirements include:

- Policies and procedures for access
- Access Request Form
- Notifications
- Review documentation

Contents of Access Request Form:

1. identification of the specific PHI that the client wishes to access;
2. the reason for their request (this is optional for the client);
3. whether they wish to inspect or obtain copies of the PHI;
4. notification of the cost we will charge for copying and postage; and
5. notification of their right to obtain a summary or explanation of their information, along with the cost of that service.

Policy 11 Individual's Right to Amendment of PHI

Purpose

To comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the process for providing clients with an opportunity to amend their PHI that is maintained in a designated record set.

Policy

MHA will consider all requests from clients, or former clients, to amend their PHI that is maintained in a designated record set for as long as we maintain it. We will require that all requests for amendment be in writing and preferably be prepared using the Request for Amendment form. In any case where our form cannot be obtained, we will provide the client or former client with the information they need to submit in lieu of the form. We will require that the individual inform us, in writing, as to the reason for the amendment. We will notify our clients of our policies for requesting amendments in our Privacy Notice. We will require such requests to be directed to the Director of Programs, who will determine the response to the request.

We will respond to requests for amendment within 60 days from the date of the request. Should, in rare circumstances, we be unable to respond within 60 days, we will notify the individual prior to the expiration of the 60-day period, in writing, and provide them with the reason that we need additional time and give them the date (no more than 30 days beyond the original 60 days) by which we expect to complete action on their request.

In those instances where we grant the request for amendment, we will do the following**:**

1. inform the client in writing;
2. obtain their agreement about the list of people or organizations that they and you believe should be informed of the amendment; and
3. notify those identified in the above-referenced list of the amendment.

(Note: it is our policy to identify anyone who we know may have relied upon the subject PHI in the past, or who might reasonably be expected to rely upon it in the future and attempt to obtain agreement from the client about their notification.)

In those instances where we deny the request for amendment, we will do the following:

1. provide the client with a written denial that is in plain language and that:
   a. contains the basis for the denial; and
   b. the notification that the individual has the right to provide a written statement disagreeing with the denial and how they might file such a statement.
2. describe to the client the procedure for filing a complaint either with:
   a. DHHS or
   b. With the person or office in our organization who is responsible for receiving complaints - including their name or title and their telephone number.

Revised by MHA 07/15/09

3. inform the individual that they may file a statement of disagreement with our denial that does not exceed 250 words.
4. inform the individual that they may request, should they not file a statement of disagreement, that their request for amendment and the related denial be attached to all future disclosures of the subject PHI.

We will prepare rebuttals in those instances where a licensed healthcare professional determines that a rebuttal is necessary to add clarity to the other material created around this request for amendment.

Designated Record Set

It is our policy to take the following actions with respect to the designated record set in amendment situations:

1. when the amendment request has been granted:
    a. identify the subject PHI in the designated record set; and
    b. append the amendment to the PHI or
    c. provide a link to the location in the file of the amendment.
2. when the amendment request has been denied and the client requests it:
    a. identify the subject PHI in the designated record set; and
    b. append the request for amendment and the denial to the PHI or
    c. provide a link to the location in the file of the request and the denial.
3. when the amendment request has been denied and the client has filed a statement of disagreement, and we have or have not prepared a rebuttal:
    a. identify the subject PHI in the designated record set; and
    b. append the request for amendment, the denial, the statement of disagreement, and, if prepared, our rebuttal to the PHI or
    c. provide a link to the location in the file of all of the items listed in b.

Documentation retention requirements include:

Policies and procedures for individual's right to amendment of PHI
Amendment Request Form
Notifications
Amendment requests and all related documentation

Policy 12 Individual's Right to an Accounting of Disclosures of PHI

Purpose

To comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the process for providing clients with an opportunity to receive an accounting of the disclosures made of their PHI.

Policy

MHA will consider all requests from clients, or former clients, to receive an accounting of certain disclosures of their PHI that have occurred in the six year period prior to their request, or from the effective date of the Privacy Rule, whichever is shorter. We will require that all requests for an accounting be in writing preferably using the Request for Accounting form. (Should a client need assistance in completing the form, we will provide that assistance.) Requests should be directed to the Director of Programs. We will notify our clients of our policies for requesting an accounting in our Privacy Notice.

It will be our policy to respond to requests for an accounting within 60 days from the date of the request. Should, in rare circumstances, we be unable to respond within 60 days, we will notify the individual, in writing during the initial 60-day period and provide them with the reason(s) that we need additional time and give them the date (no more than 30 days beyond the original 60 days) by which we expect to complete action on their request.

We will account for all uses and disclosures of our clients' PHI except for those in the following categories:

1. disclosures to carry out treatment, payment, and health care operations (this includes disclosures made by business associates for these purposes as well);
2. disclosures made to the individual;
3. disclosures made incident to a use or disclosure that is otherwise permitted or required;
4. disclosures made pursuant to an authorization;
5. for disclosures made to the Secretary of HHS for compliance purposes and for any other disclosures allowed to be made without the individual's permission;
6. disclosures for national security or intelligence purposes; and
7. disclosures to correctional institutions or law enforcement officials when individual is an inmate;
8. disclosures made as part of a limited data set;
9. disclosures that occurred prior to January 1, 2010
10. disclosures to persons involved in the individual's care or other permitted notification purposes.

If we have made disclosures to a health oversight or law enforcement agency as permitted by the No Permission Policy, and that agency has provided us with a written statement that inclusion of

such disclosures would be reasonably likely to impede their activities for a specific time period, then we will exclude those disclosures from any accounting requested by the subject client. At the end of that period, our policy will be to include any disclosures made to the agency during that period in any future accountings.

Should the health oversight or law enforcement agency provide us with an oral statement that a disclosure would be reasonably likely to impede their activities, our policy will be to withhold disclosures for a 30 day period, after which we will include the disclosures in requested accountings, unless a written statement requesting a longer time period has been provided during the 30 day period.

Our policy will be to include the following items in every accounting except for those related to certain research projects:

1. the date of the disclosure;
2. the name and address (if known) of the person or organization receiving the PHI;
3. a brief description of the PHI disclosed; and
4. a brief statement that reasonably informs the client of the purpose for the disclosure.

Our policy with respect to multiple disclosures of a client's PHI to the same person or entity for the same purpose will be to present all of the information listed above for the first disclosure in the accounting period. In addition, we will present the frequency, periodicity, or number of disclosures made during the accounting period and the date of the most recent disclosure.

Our policy with respect to disclosures of PHI for a particular research purpose where 50 or more individuals participated will be to provide:

1. the name of the protocol or other research activity;
2. a description, in plain language, of the research protocol or other research activity, including the purpose and criteria for selection of particular records;
3. a description of the type of PHI that was disclosed;
4. the date or period of time during which such disclosure occurred, or may have occurred, including the date of the last disclosure during the accounting period;
5. the name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
6. a statement that the PHI may or may not have been disclosed.

In the event that it is reasonably likely that the PHI of a particular client has been disclosed for such a protocol or research activity, we will, if requested by the client, assist him/her in contacting the entity that sponsored the research and the researcher.

It will be our policy to provide the first accounting in each 12 month period, beginning with the client's first request for an accounting, at no charge. Any additional request for accounting from the same client during their 12 month period will be made subject to the client's agreement to pay a reasonable, cost-based fee for the additional accounting. Our policy will be to inform the client of the fee on the Request for Accounting form and obtain their written agreement to pay the fee prior to preparing the accounting. We will offer the client an opportunity to withdraw or modify their request in order to avoid or reduce the fee.

Documentation retention requirements include:

- Policies and procedures for individual's right to an accounting of disclosures of PHI
- Accounting Request Form
- Copies of accountings provided
- Titles of persons responsible for receiving and processing accounting requests

Policy 13 Other Individual Rights - Right to Restrict Uses and Disclosures of PHI

Purpose

To comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the conditions for agreeing to client-requested restrictions on the use and disclosure of PHI for treatment, payment, and operations.

Policy

MHA will consider a client's request for restriction of the uses and disclosures that we make for purposes of treatment, payment, and operations. It will be our policy to discuss with the client the potential difficulties that are inherent in the restrictions that the client requests, such as those that might interfere with the client's ability to obtain appropriate treatment.

We will use the Request for Restrictions form to document the request and, ultimately, the restriction that has been granted to the client. While we are not required by the Privacy Rule to agree to client-requested restrictions, it will be our policy to grant those restrictions that we believe, in our sole discretion to be in the best interests of our clients.

We will abide by all of the restrictions that we grant, except as described below.

When the individual is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, our policy will be to make disclosure of the PHI that is required for treatment and to attach to the PHI documentation of our requirement that there be no further uses or disclosures of the restricted PHI. In non-emergency situations, when we receive a request for PHI that is restricted but required for appropriate treatment, we will discuss with the client the need to send the PHI and attempt to obtain their agreement. The client's agreement should be documented by a note in their medical record.

In any case where we believe the client's restriction can no longer be honored, we will terminate the restriction. It will be our policy to discuss the change of circumstance with the client and ask for their agreement and to document that agreement on the Request for Restrictions form that is in the medical record.

Should the client refuse to agree to the termination of the restriction, it will be our policy to implement a unilateral termination. This will also be documented on the Request for Restrictions form. The PHI that we created or received during the term of the restriction will be flagged to assure that futures uses and disclosures of it are made in accordance with the restrictions in place for that period.

Documentation retention requirements include:

1. Policies and procedures for restrictions to use and disclosure of PHI.
2. Restrictions granted.
3. Terminations.

Policy 14 Other Individual Rights — Confidential Communications

Purpose

To comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the conditions for accommodating a client's request for confidential communications.

Policy

MHA will consider a client's request for confidential communications upon request.

We will document the alternative information and the approval in the client's record and equivalent electronic form.

It will be our policy to grant reasonable requests. Reasonableness will be judged by the administrative difficulty of complying with the request.

We will not ask the client to explain why they wish to have us communicate with them by alternative means or to alternative locations.

We will not comply with the client's request unless they have provided us with complete information to enable us to communicate with them — i.e., a complete address or other method of contact.

We will provide adequate notice of the request to those employees who may need to contact the client by flagging the medical record and, where possible, other client databases.

Documentation retention requirements include:

Policies and procedures for confidential communications of PHI

Policy 15 Administrative Requirements -- Documentation

Purpose

To comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the standards it will maintain to fulfill the documentation retention requirements.

Policy

MHA will retain all documentation as described in the Privacy Rules for a period of thirty years from its creation or from the date it was last in effect, whichever is later.

The Director of Programs will assure that all documentation is preserved for the appropriate retention period in whatever medium is considered appropriate for each required item.

The material subject to documentation retention requirements is set out in each individual Privacy Policy. The list that follows summarizes these requirements:

1. the notice of privacy practices, with copies of the notices maintained by implementation dates by version;
2. all policies and procedures, with copies of each policy and procedure maintained through each of its iterations;
3. workforce training efforts;
4. restrictions to uses and disclosures of PHI that were granted;
5. the designated record set;
6. personnel roles related to Privacy Rules — the Director of Programs and/or other designated Privacy Officer the person or office designated to receive complaints, the titles of person(s) or office(s) who are responsible for receiving and processing requests for access by individuals, the titles of person(s) or office(s) responsible for receiving and processing requests for amendments and accountings of PHI;
7. for each accounting provided to an individual - the date of disclosure, the name and address of entity or person who received the PHI, a description of the PHI disclosed, a briefly stated purpose for the disclosure, and the; written accounting that was provided;
8. all signed, written acknowledgements of receipt of the Privacy Notice or documentation of good faith efforts made to obtain such acknowledgement in those cases where a signed, written acknowledgement could not be obtained;
9. any signed authorization;
10. all complaints received and their disposition;
11. any sanctions against members of the workforce that have been applied as a result of non-compliance; and
12. any of PHI for research made without the individual's authorization and any approval or alteration or waiver of PHI for research in accordance with the requirements of §164.512(i)(2).

Documentation retention requirements include:

Policies and procedures for documentation retention.

Policy 16 Administrative Requirements — Complaint Process

Purpose

In an effort to comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the process it will establish to receive complaints from clients.

Policy

MHA designates its Human Rights Officer to receive and be responsible for complaints about: (a) privacy policies and procedures required by the Privacy Rule, and (b) compliance with such policies and procedures and with the Privacy Rule. All privacy complaints, as defined above, received by us will be directed to this individual for proper processing and handling.

With regard to any privacy complaints, the Human Rights Officer will:

1. retain the original copy of every complaint;
2. enter the complaint in a log book maintained chronologically;
3. request the complainant to submit the complaint in writing and, if requested, will assist the complainant in writing a complaint.
4. send a letter to the complainant within 5 days of receipt of complaint acknowledging receipt of the complaint, thanking them for their assistance in strengthening our privacy practices, providing a copy of the procedures for processing the complaint, establishing the time frame for responding and an address for correspondence and a statement that the complainant always has the right to complain to the Secretary of HHS as well as the information needed to make that contact;
5. review the complaint;
6. investigate the complaint;
7. report results of the investigation to the appropriate individuals; and
8. periodically submit a summary report of activity to the CEO and others as designated by the CEO.

We will inform clients in writing at the time of the complaint of their right to complain directly to the Secretary of Health and Human Services and will give them the contact information.

Any complaint that deals with a breach of privacy practices must be reported to the Director of Programs and/or designated Privacy Officer for appropriate follow-up.

Documentation retention requirements include:

1. Policies and procedures for the complaint process.
2. All complaints received.
3. The disposition of all complaints, including the agency's written response.

Policy 17 Administrative Requirements — Training of the Workforce

Purpose

To comply with the Privacy Rule of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the requirements for workforce training in our privacy practices.

Policy

MHA will train all of our workforce members (full and part time employees, interns, and volunteers) in our privacy practices.

All members will be trained on or before the effective date of the Privacy Rule. We will train employees in accordance with their role in the Agency and their functions with regard to PHI.

All workforce members who join the Agency subsequent to the effective date will receive their privacy training as part of their orientation to the Agency.

Whenever there are material changes to our privacy practices, the Privacy Official will determine the workforce groups affected by the changes and coordinate the training of those groups.

All trainings presented will be documented as to content and attendance.

Workforce members who fail to attend their assigned trainings will be required to receive training at the earliest possible time and may be subject to disciplinary action.

Documentation retention requirements include:

1. Policies and procedures for workforce training.
2. Evidence that trainings were presented to the workforce.

Policy 18 Administrative Safeguards — Personnel

Purpose

To comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the requirements for safeguarding PHI in all media.

Policy

MHA will assign responsibility for all safeguarding matters to an Officer of Information Security. This position will be responsible for assuring that all PHI, whether in oral, written, or electronic form, is reasonably secure (a) from accidental or intentional uses and disclosures that violate the Privacy Rules and (b) from inadvertent disclosures to other than the intended recipient.

The Officer of Information Security will maintain the Policies and Procedures, for all media, around security measures to protect PHI.

The Officer of Information Security will also be responsible for monitoring the appropriate and consistent implementation of the policies and procedures that control the conduct of the workforce, subcontractors, and business associates with regard to the protection of data. The Officer of Information Security will assure that breaches of security are investigated and that members of the workforce who are responsible for those breaches will be subject to the appropriate sanctions. In addition, the Officer of Information Security will assure that any system weakness uncovered during such investigations will be corrected.

Documentation retention requirements include:

1. Policies and procedures for Personnel
2. Personnel assignments

Policy 19 Administrative Safeguards — Chain of Trust Agreements

Purpose

To comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the requirements for safeguarding PHI in MHA HIPAA Policy

Policy

Chain of Trust Agreements

MHA will obtain agreements, commonly referred to as "Chain of Trust Agreements", with any third party through whom it processes electronic data. This agreement will assure that at least the same level of security present within our Agency will be maintained at all points in the movement of PHI to ensure its security, accuracy, and authentication.

The Chain of Trust Agreement is a form of Business Associate Agreement and will be in the form attached to this policy.

We will identify the specific attributes that we will require from our electronic data vendors and the steps we will take in performing due diligence with these vendors. The process in the Business Associates Policy and Procedure is the guidance for minimum procedures around electronic data vendors.

Documentation retention requirements include:

1. Policies and procedures for Chain of Trust agreements.
2. Business Associate -— Chain of Trust Agreement template.
3. Executed Business Associate.- Chain of Trust Agreements.

Policy 20 Administrative Safeguards — Contingency Planning

Purpose

To comply with the Privacy Rules of HIPPA's Administrative Simplification provisions, in this policy, MHA sets out the requirements for safeguarding PHI through contingency planning.

Policy

MHA will maintain contingency plans in accordance with the five required plans set forth in the proposed Security Rule.

It will be our policy to maintain, in a timely manner, documentation of our applications and data criticality that includes:

1. network architecture diagrams and systems flowcharts showing current structure, equipment addresses, communication providers and system interdependencies;
2. critical business processes surrounding PHI;
3. key applications and systems used to support critical business processes:
4. key applications and systems and their recovery time objectives;
5. internal and external interfaces with key applications and systems;
6. the adequacy of redundancies within the network infrastructure; and
7. mitigating controls, in place and tested, for any single points of failure for which redundancies cannot be established.

It will be our policy to assure, by means of a Data Backup Plan that we have adequate (regular and periodic) backup of critical information as prioritized in the data criticality analysis. Backup and restore procedures will be updated regularly to reflect changes within the organization for the documentation listed above. In addition, we will assure that the backup data can be accessed quickly. We will maintain offsite storage of critical documentation and assure access to those materials.

We will maintain a Disaster Recovery Plan that documents all elements of the Plan and that is updated on a regular basis. The Plan will cover the full range of information and activities needed to assure that the Plan will function smoothly in situations where it is needed.

We will maintain an Continuation of Operations Plan that will enable us to operate effectively in emergency conditions. The Plan will include any information, activities, and assignments that are needed such as: identification of crisis management team members, a command center for emergency purposes, a process for acquiring additional personnel with needed skill sets, alternate processing and work space, and health and safety issues.

We will test and revise procedures as necessary to assure that they function as planned and that they are effective**.**

Documentation retention requirements include:

1. Policies and procedures for Contingency Planning.
2. Applications and data criticality analysis.
3. Disaster Recovery Plan
4. Continuation of Operations Plan
5. Testing and revision documentation

Policy 21 Administrative Safeguards — Audit Controls and Internal Audit

Purpose

In an effort to comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the requirements for safeguarding PHI through audit controls and internal auditing.

Policy

MHA will establish and maintain ongoing processes to review records of systems activity, such as log-ins, file accesses, and security incidents, for PHI in all media. We will establish documented procedures for auditing this information for the purpose of identifying security breaches and for assuring that users comply with access controls. We will assign specific individuals or job functions that will be responsible for such internal audit activity.

We will also establish audit controls that will define users, data sources, data accessed, the client, the date and time of the access, and other information we consider appropriate.

We will also establish procedures to audit configuration management practices that have been established to assure that changes to hardware and software systems do not contribute to, or create, security weaknesses.

Access to audit logs will be limited to those assigned to the internal audit and control function as described above.

Documentation retention requirements include:

1. Policies and procedures for audit controls and internal audit.
2. Personnel assignments.

Policy 22 Administrative Safeguards — Workforce-related Security Measures

Purpose

In an effort to comply with the Privacy Rules of HIPAAs Administrative Simplification provisions, in this policy, MHA sets out the requirements for safeguarding PHI. This Policy recognizes that our workforce is the foundation for our security environment.

Policy

MHA will create and maintain procedures directed toward the behavior of our workforce that promote an environment for PHI that is reasonably secure from accidental, intentional, or inadvertent disclosures that violate the Privacy Rule.

It is our policy to create, document, and maintain guidelines on the use of information technology which will address proper uses in the workplace and necessary attributes of the physical environment in which the technology is used. The Officer of Information Security will oversee this process and assure that the workforce is trained on these guidelines expediently.

It is be our policy to provide security awareness training to all members of the workforce with access to electronic information technology and to any independent contractors who have access to our workplace and systems. Awareness training will be directed at all of these individuals, regardless of their roles or access to PHI; its purpose is to educate on at least these topics: password maintenance, login practices, security incident reporting, computer viruses and other forms of destructive software, addition of unauthorized hardware or software to the system, and securing workstations when absent. The Officer of Information Security will oversee the development of awareness training in conjunction with Human Resources.

We will establish procedures in conjunction with Human Resources for terminated workforce members and for members of the workforce whose positions and work assignments have changed. These procedures will cover security for PHI in all media. We will address: facility access, removal of general and user system access privileges, and the collection of keys or other objects that allow access.

Documentation retention requirements include:

1. Policies and procedures for audit controls and internal audit.

Policy 23 Administrative Safeguards —Access Control

Purpose

In an effort to comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the requirements for safeguarding PHI by controlling access to our facilities and electronic systems.

Policy

MHA will create and maintain procedures to safeguard all of our locations from unauthorized physical access and to safeguard hardware and other equipment from unauthorized physical access, theft, and interference.

We will limit and control physical access to any and all parts of the designated record set. To the extent possible, our paper client files will be placed in limited access spaces and access to those records will be controlled by designated responsible staff.

Electronic files will be subject to access controls that will limit user access to that PHI for which they have clearance. Data access will be established by supervisors and managers responsible for security of such data.

Our systems will maintain an access authorization record to document and review the level of access granted to a user, program, or procedure.

We will assure that systems maintenance personnel have proper access authorization.

We will not transmit PHI over the Internet (open network) without some form of encryption intended to limit access to information.

Documentation retention requirements include:

1. Policies and procedures for access controls.

Policy 24 Administrative Safeguards — Data and Entity Authentication

Purpose

In an effort to comply with the Privacy Rules of HIPAA's Administrative Simplification provisions, in this policy, MHA sets out the requirements for safeguarding PHI by assuring that PHI is transmitted to or from the appropriate person or entity and that the data being processed or transmitted has not been modified intentionally or inadvertently.

Policy

MHA will establish and maintain procedures for assuring that recipients of PHI via electronic or other means are the intended recipients.

We will also establish and maintain procedures for data authentication to assure that PHI contained in messages or files has not been altered or modified inappropriately.

Documentation retention requirements include:

1. Policies and procedures for data and entity authentication.

GLOSSARY OF KEY HIPAA-RELATED TERMS

Business Associate

(1) ... business associate means, with respect to a Covered Entity, a person who:

(i) On behalf of such Covered Entity ... but other than in the capacity of a member of the Workforce of such Covered Entity ... performs, or assists in the performance of:

(A) A function or activity involving the Use or Disclosure of Individually Identifiable Health Information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the Workforce of such Covered Entity, legal, actuarial, accounting, consulting, Data Aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity, . where the provision of the service involves the Disclosure of Individually Identifiable Health Information from such Covered Entity or Arrangement, or from another business associate of such Covered Entity or Arrangement, to the person. -

Covered Entity means one of the following:

(3) A Health Care Provider who transmits any Health Information in electronic form in connection with a Transaction covered by this subchapter

Health Care means care, services, or supplies furnished to an Individual and related to the health of the Individual. Health Care includes 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.

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

Health Care Provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or other health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for Health Care in the normal course of business.

Health Information means any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a Health Care Provider.., and

(2) Relates to the past, present, or future physical or mental health or condition of an Individual; the provision of Health Care to an Individual; or the past, present, or future payment for the provision of Health Care to an Individual.

Designated Record Set means:

(1) A group of records maintained by or for a Covered Entity that is:

(i) The medical records and billing records about Individuals maintained by or for a covered Health Care Provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a Health Plan; or

(iii) Used, in whole or in part, by or for the Covered Entity to make decisions about Individuals.

(2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for a Covered Entity.

Individually Identifiable Health Information is information that is a subset of Health Information, including demographic information collected from an Individual, and:

(1) Is created or received by a Health Care Provider.. and

(2) Relates to the past, present, or future physical or mental health or condition of an Individual; the provision of Health Care to an Individual; or the past, present, or future payment for the provision of Health Care to an Individual; and

(i) That identifies the Individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

Protected Health Information means Individually Identifiable Health Information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by Electronic Media;

(ii) Maintained in any medium described in the definition of Electronic Media at Sec. 162.103 of this subchapter; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected Health Information excludes Individually Identifiable Health Information in.. Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and Records described at 20 U.S.C. 1232g(a)(4)(B)~v).

Revised by MHA 07/15/09

CONNECTICUT

Connecticut statutorily grants patients the right of access to their medical records maintained by health care providers, health care institutions, insurance entities and other specified entities. The state does not have a general, comprehensive statute prohibiting the disclosure of confidential medical information. Rather, these privacy protections are addressed in statutes governing specific entities or medical conditions.

I. PATIENT ACCESS

A. Employers

Within a reasonable time after receipt of a written request from an employee, an employer must permit an inspection of any medical records pertaining to the employee that the employer maintains. [Conn. Gen. Stat. ~ 31-128c.] The inspection must take place during regular business hours at a location at or reasonably near the employee's place of employment. Access must be given to either a physician chosen by the employee or by a physician chosen by the employer with the employee's consent. An employer must allow the inspection of any particular employee's medical records no more than twice during a calendar year. [Conn. Gen. Stat. **§** 31-128h.]

Similarly, an employer must provide an employee's physician with a copy of the employees medical records within a reasonable lime after receipt of a written request from the employee. The request must be in writing and reasonably identify the materials to be copied. [Conn. Gen. Stat. **§** ^{31}-128g.] The employer may charge a fee for copying the records. *[Id])* The fee must be reasonably related to the cost of supplying the requested documents. *[Id]*

If an employee disagrees with any of the information contained in his medical records, he may request that the employer remove or correct the information. [Conn. Gen. Stat. ~ 31- 128e.] If the employer does not agree to the removal or correction, the employee may submit a written statement explaining his position. The statement must be maintained as part of the employees medical records and must accompany any transmittal or disclosure made to a third party. *[Id.]*

B. Health Care Providers, Including Physicians, Dentists and Pharmacists

1. Scope

The Health Care Records Act applies to health care providers, including physicians, dentists, pharmacists, chiropractors, and certain other licensed health care providers. [Conn. Gen. Stat. **§ §** 20-7c; 20-7b (defining "provider" as "any person or organization that furnishes health care services and is licensed or certified to furnish such services pursuant to chaps. 370 to 373 (inclusive) 375 to 384a (inclusive), 388, 389, 399 or is licensed or certified under 368d").]

The records encompassed by the Act include bills, x-rays, copies of lab reports, contact lens specifications, records of prescriptions and other technical information used in assessing the patient's health condition. [Conn. Gen. Stat. ~ 20-7c.] These provisions do not apply to health care information related to a psychiatric or psychological condition. [Conn. Gen. Stat. § 20-7c(d)

2. Requirements

Upon request, a health care provider is generally required to supply to a patient complete and current information concerning any diagnosis, treatment and prognosis of the patient that the provider possesses. A provider is also required to notify a patient of any test result in the providers possession that indicates a need for further treatment or diagnosis. [Conn. Gen. Stat. § 20-7c(a).]

A patient (his attorney or authorized representative) may submit a written request for a copy of his health record. The provider must furnish the copy within 30 days of receipt of the request. Conn. Gen. Stat. § 20-7c.]

Copying fees. The maximum charge for furnishing copies is 45 cents per page (which includes any research fees, handling fees or related costs) plus postage. [Conn. Gen. Stat. § 20-7c(b).i The provider may charge a patient the amount necessary to cover the cost of necessary materials for furnishing a copy of an x-ray. *lid.)*

Denial of Access. Access may be denied if the provider reasonably determines that the information is detrimental to the physical or mental health of the patient, or is likely to cause the patient to harm himself or another. [Conn. Gen. Stat. § 20-7c(c).] In this circumstance, the information may be provided to an appropriate third party or another provider who may release the information to the patient. *[Id.]*

3. Remedies and Penalties

Right to Sue. When a patient is denied access to his information because it has been determined that his access may be detrimental to his health or likely to cause harm, the patient has the right to file a petition within 30 days of the refusal with the superior court for an order requiring the provider to disclose the information. (Conn. Gen. Stat. § 20-7c(c).]

C. Health Care Institutions, including Hospitals, Nursing Homes and others

Upon the written request of a patient, his attorney or authorized representative, all licensed health care institutions, including hospitals, nursing homes and others must furnish to the patient a copy of his health record. [Conn. Gen. Stat. § 19a~49Ob. ***See*** also "Hospitals Receiving State Aid," below.] The health records covered by this requirement include, but are not limited to, copies of bills, laboratory reports, prescriptions and other technical information used in assessing the patient's health. *[Id.)* A patient also has the right to designate a health care provider to review original tissue slides or pathology blocks, *lid.]*

The maximum charge for furnishing copies is 65 cents per page plus postage and retrieval expenses. *[Id.]* The health care institution may not deny the patient access to his records due to his inability to pay the required fees. *[Id.]* A patient generally may

show inability to pay by presenting an affidavit attesting to his inability to pay the fees.

D. Hospitals Receiving State Aid

Upon the demand of any patient who has been discharged his physician or authorized attorney, a hospital that receives state aid must permit the patient to examine and copy his hospital records, including the history, bedside notes, charts, pictures and plates. [Conn. Gen. Stat. § 4-104.1

Remedies and Penalties

Right to Sue. If a patient who has been discharged is denied access to his hospital records, he may file a written motion in the Superior Court seeking disclosure and production of the records before the judge. [Conn. Gen. Stat. § 4-105.] The custodian of the hospital records may be imprisoned, fined, or both if he fails to comply with any resulting judicial order to produce the records. *[Id.]*

E. Insurance Entities, Including HMOs

1. Scope

The Connecticut Insurance Information and Privacy Protection Act applies to insurance entities including fee for service insurers, HMOs, insurance agents and insurance support organizations. [Conn, Gen, Stat. §~ 38a-175 (defining "health care center" as including HMOs); 38a-977 (detailing entities and persons covered); 38a-976 (defining "insurance institutions" as including health care centers)*]*

The Act covers "personal information," including "medical record information," which is gathered in connection with an insurance transaction. [Conn. Gen. Stat. § 38a-976 (defining "personal information").] "Medical record information" is personal information that (1) relates to the physical, mental or behavioral health condition, medical history or medical treatment of an individual or his family member, and (2) is obtained from a medical professional, medical care institution, pharmacy, pharmacist or an individual, the individual's spouse, parent or legal guardian, or from the provision of or payment for health care to or on behalf of the individual or his family. [Conn. Gen. Stat. § 38a-976 (defining "medical record information").] The Act does not apply to medical information that has had all personal identifiers removed. Conn. Gen. Stat. § 38a-976(r).]

With respect to health insurance, the rights granted by the Act extend to Connecticut residents who are the subject of the information collected, received or maintained in connection with insurance transactions and applicants, individuals or policyholders who engage in or seek to engage in insurance transactions. (Conn. Gen. Stat. § 38a-977.j

2. Requirements

An insurance company, HMO, or other insurance entity must permit the individual to inspect and copy his personal information in person or to obtain a copy of it by mail, whichever the individual prefers, within 30 business days of receiving a written request and proper

identification from an individual. (Conn. Gen. Stat. §~ 38a-983; 38a-976.I If the personal information is in coded form, an accurate translation in plain language must be provided in writing. [Conn. Gen. Stat. § 38a-983(a).]

Copying fees. The insurance entity can impose a reasonable fee to cover copying costs. [Conn. Gen. Stat. § 38a-983(d).]

In addition to giving the individual a copy of his personal information, the insurance entity must also give the individual a list of the persons to whom it has disclosed such personal information within two years prior to the request for access, if that information is recorded. If such an accounting of disclosures is not recorded, the entity must inform the individual of the names of those persons to whom it normally discloses personal information. [Conn. Gen. Stat. § 38a-983(a).]

Medical record information provided to the insurance entity by a medical professional or medical care institution that is requested may be supplied either directly to the requesting individual or to a medical professional designated by the individual, at the option of the insurance entity. [Conn. Gen. Stat. § 38a-983(c).]

Right to Amend. A person has a statutory right to have any factual error corrected and any misrepresented or misleading entry amended or deleted, in accordance with stated procedures. [Conn. Gen. Stat. § 38a-984.] Within 30 business days from the date of receipt of a written request, the insurance institution, agent or support organization must either: (1) correct, amend or delete the portion of recorded personal information in dispute; or (2) notify the individual of its refusal to make the correction, amendment or deletion, the reasons for the refusal, and the individual's right to file a statement of disagreement. ***Id.)***

3. **Remedies and Penalties**

Right to Sue. A person whose rights under this statute are violated has the right to file a civil action seeking equitable relief within two years of the violation. Conn. Gen. Stat. § 38a-995. The court may award costs and reasonable attorney's fees to the prevailing party. [id.]

Fines and Penalties. The Insurance Commissioner may hold hearings **and** impose administrative remedies, including, in the case of intentional violations, monetary fines. [Conn. Gen. Stat. §~ 38a-990 through 38a-993.] A cease and desist order and fine not to exceed $2,000 per violation or $20,000 for multiple negligent violations may be imposed. Conn. Gen. Stat. § 38a-993.J

F. Mental Health Facilities

The Patients' Bill of Rights applies to any hospital, clinic, ward, psychiatrist's office or other facility, public or private, which provides inpatient or outpatient services relating to the diagnosis

or treatment of a patient's mental condition. [Conn. Gen. Stat. §~ 17a-548; 52-146d (defining "mental health facility").]

Under the Patients' Bill of Rights, following discharge from a mental health facility (or in connection with litigation related to hospitalization), any patient treated by a psychiatrist for diagnosis or treatment has the right to inspect and make copies of his records. [Conn. Gen. Stat. §~ 17a-548(b); lla-540(a) and (b) (defining "patient" and "facility").] The patient must submit a written request to view or copy his records.[Conn. Gen. Stat. § 17a-548(b).]

Generally, the facility may deny access to any portion of a patient's record if it determines that disclosure would: create a substantial risk that the patient would inflict life-threatening injury to self or others; cause a severe deterioration in mental state of the patient; constitute an invasion of privacy of another person; or violate an assurance of confidentiality furnished to another person. [Conn. Gen. Stat. § 17a-548(b).] A patient who is seeking access to his records in connection with any litigation related to hospitalization is not subject to the above restrictions on access. *[Id]*

Remedies and Penalties

Right to sue. Any patient aggrieved by a facility's refusal to grant access to his records may petition the Superior Court for relief in accordance with specified procedures. [Conn. Gen. Stat. §~ 17a-548(b); 4-105.1

G. State and Local Government

1. Scope

The Personal Data Act [Conn. Gen. Stat. §~ 4-190 through 4-198) imposes on state agencies a variety of duties related to the personal data that they maintain. The Act applies to every state or municipal board, commission, department or officer, courts, Governor, Lieutenant Governor, Attorney General, and town or regional board of education that maintains a personal data system. [Conn. Gen. Stat. §~ 4-190 (defining "agency") and 4-193. it does not apply to the state legislature. (Conn. Gen. Stat. § 4-190.]

The Act applies to "personal data,' including information about a person's medical or emotional condition or history which because of name, identifying number, mark or description can be readily associated with a particular person.

Persons who have rights under the Personal Data Act include an individual of any age concerning whom personal data is maintained, or a person's attorney or authorized representative. Conn. Gen. Stat. § 4-190 (defining "person").]

2. Requirements

State agencies may maintain only that information about a person that is relevant and necessary to accomplish the lawful purposes of the agency. [Conn. Gen. Stat. § 4-193(e).] Upon written

request, an agency must inform an individual whether it maintains personal data (including medical and mental health information) concerning him and must provide access to that information. *[Id.]* The state agency must respond to the request in writing and in a format that is understandable to the requestor. [Conn. Gen. Stat. *§* 4-193(1).)

Agencies must have procedures that allow a person to contest the accuracy, completeness or relevancy of his personal data, and must have procedures to have it corrected. Conn. Gen. Stat. *§* 4-193(h).I

An agency may refuse to disclose medical, psychiatric or psychological data to a person if it determines that disclosure would be detrimental to that person, or that nondisclosure is otherwise required or permitted by law. [Conn. Gen. Stat. *§* 4-194.1 The agency must advise the person of his right to seek judicial relief in response to such a refusal. *[Id.]* The person has the right to request that a medical doctor be permitted to review the personal data to determine whether it should be disclosed. The agency must comply with the doctor's determination. *[Id.]*

3. **Remedies and Penalties**

Right to Sue. A person has the right to file a civil action for equitable relief, such as an injunction, and for damages against an agency that violates these provisions. [Conn. Gen. Stat. *§* 4-197.] The court may award court costs and reasonable attorney's fees to a person who prevails in such an action. *[Id.)*

When an agency specifically refuses to disclose personal information because of potential endangerment under Section 4-194, the person may petition the superior court within 30 days of the denial for an order requiring the agency to disclose the requested data. [Conn. Gen. Stat. *§* 4-195.]

II. RESTRICTIONS ON DISCLOSURE

A. Employers

In general, an employer may not disclose individually identifiable information in the medical records of any employee without the written authorization of the employee. [Conn. Gen. Stat. *§* 31-128f] There are a number of exceptions to this general rule. Disclosure without the employee's authorization is permitted to other persons employed by or affiliated with the employer; in response to an apparent medical emergency; to apprise the employee's physician of a medical condition of which the employee may not be aware; pursuant to subpoena, court order, summons, warrant, discovery or grand jury request; to comply with federal, state, or local laws or regulations, or where the information is disseminated pursuant to the terms of a collective bargaining agreement. *[Id.]*

With respect to authorizations to disclose medical records, an employer must inform the employee of his right to inspect and correct the information, his right to withhold the authorization, and the effect such withholding has on the employee. *[Id.*

B. Government

1. Freedom of Information Act

Medical files maintained by any public agency are exempt from disclosure under the state's Freedom of Information Act. Conn. Gen. Stat. *§* 1-210(b)(2).1

2. Department of Public Health

All information, records of interviews, written reports, and statements, including data concerning a person's medical or emotional condition or history, procured by the Department of Public Health in connection with studies of morbidity and mortality, or pursuant to statutory reporting requirements are confidential and may be used solely for the purposes of medical or scientific research or for disease prevention and control. [Conn. Gen. Stat. ~ 19a-25.]

This information is not admissible as evidence in any action in any kind in any forum.

[Id.] Confidential medical information may not be disclosed except as may be necessary for the purpose of furthering the research project to which it relates. *[Id.]* The department may exchange personal data with other governmental agencies or private research organizations for the purpose of medical research provided that they do not further disclose the data. *[Id]*

C. Health Care Professionals, Medical Care Centers, Pharmacies, and Pharmaceutical Companies

Health care professionals, medical care centers, pharmacies, pharmaceutical companies and their contractors, agents and employees are prohibited from selling medical record information and from disclosing such information for marketing purposes without the prior written consent of the individual. [Conn. Gen. Stat. *§* 38a-988a.] "Medical-record information" is defined as information which: relates to the physical, mental or behavioral health condition, medical history or medical treatment of an individual or a member of the individual's family; and which is obtained from a medical professional or institution, from a pharmacy or pharmacist, from the individual, or from the individual's spouse, parent or legal guardian or from the provision of or payment for health care to or on behalf of an individual or a member of the individual's family. [Conn. Gen. Stat. *§*~ 38a-988a; 38a-976 (defining medical record information"fl The term does not include information that does not identify the patient. [Conn. Gen. Stat. § 38a-976.] This restriction does not prohibit the transfer of individually identifiable medical record information to another as part of a sale or merger of a business. Conn. Gen. Stat. *§* 38a-988a.]

Remedies and Penalties

Right to Sue. A person whose medical record information is improperly sold or disclosed for marketing without his authorization in violation of this section may bring an action for equitable relief, damages or both. (Conn. Gen, Stat. *§* 38a-988a.] A person who violates these provisions is liable for double damages, costs and reasonable attorneys' fees.

Hospitals Receiving State Aid
Generally, a hospital that receives state aid may not disclose a patient's hospital records to any person or entity without patient authorization. [Conn. Gen. Stat. § 4-104.) Records may be disclosed without authorization upon a subpoena or an order by a judge of the court. [*Id.]*

E. Insurance Entities, Including HMOs

1. Scope

The Connecticut Insurance Information and Privacy Protection Act (IIPPA) applies to insurance entities including fee for service insurers, HMOs, insurance agents and insurance support organizations. [Conn. Gen. Stat. §~ 38a-175 (defining "health care center" as including HMOs}; 38a-977 (detailing entities and persons covered); 38a-976 (defining "insurance institutions" as including health care centers).]

The Act covers "personal information," including 'medical record information," which is gathered in connection with an insurance transaction. [Conn. Gen. Stat. § 38a-976 (defining "personal information").] "Medical record information" is personal information that (1) relates to the physical, mental or behavioral health condition, medical history or medical treatment of an individual or his family member, and (2) is obtained from a medical professional, medical care institution, pharmacy, pharmacist or an individual, the individual's spouse, parent or legal guardian, or from the provision of or payment for health care to or on behalf of the individual or his family. [Conn. Gen. Stat. § 38a-976 (defining "medical record information"} The Act does not apply to medical information that has had all personal identifiers removed. [Conn. Gen. Stat. § 38a-976(r).]

With respect to health insurance, the protections afforded by the Act extend to Connecticut residents who are the subject of the information collected, received or maintained in connection with insurance transactions and applicants, individuals or policyholders who engage in or seek to engage in insurance transactions. [Conn. Gen. Stat. § 38a-977.]

2. Requirements

a. Authorizations for Obtaining Health Information from Others

If an insurance entity uses an authorization form to obtain health information in connection with an insurance transaction, the authorization form must conform to the requirements of the HIPAA. The authorization form must be written in plain language, specify the types of persons authorized to disclose information concerning the individual, specify the nature of the information authorized to be disclosed, identify who is authorized to receive the information and specify the purposes for which the information is collected. [Conn. Gen. Stat. § 38a-981.] The length of time the authorization remains valid varies with the purpose of obtaining the requested information. An authorization signed in support of an application for health insurance remains valid for 30 months while an authorization signed for the purpose of collecting information in connection with a claim for health benefits is effective for the term of coverage of the policy. *[Id.]*

b. Disclosure Authorization Requirements and Exceptions

Generally, an insurance entity may not disclose medical information about a person that it collected or received in connection with an insurance transaction without that person's written authorization. [Conn. Gen. Stat. § 38a-988.I Authorizations submitted by those *other* than insurance entities must be in writing, signed and dated. [Conn. Gen. Stat. § 38a-988(a).] These authorizations are effective for one year. *[Id.]*

An insurance entity may not disclose information to another insurance entity pursuant to an authorization form unless the form meets the detailed requirements of the statute. *[Ed.] See* Authorizations for Obtaining Health Information from Others, above,

The Act specifically prohibits insurance entities from selling medical record information or from disclosing this type of information for marketing purposes without the prior written consent of the subject of the information. [Conn. Gen. Stat. § 38a-988a.]

Authorization exceptions. There are numerous circumstances under which an insurance entity can disclose information without the individual's authorization including: verifying insurance coverage benefits; for the purpose of conducting business when the disclosure is reasonably necessary; to law enforcement agencies in order to prevent or prosecute fraud; in response to a facially valid search warrant or subpoena or other court order; and others. [Conn. Gen. Stat. § 38a-988.)

c. Notification Requirements

The insurance entity must provide to all applicants and policyholders written notice of its information practices. [Conn. Gen. Stat. § 38a-979.] The insurance entity has the option of providing a detailed notice or an abbreviated notice. The abbreviated notice must advise the individual that (1) personal information may be collected from persons other than the individual proposed for coverage, (2) such information as well as other personal information collected by the insurance entity may in certain circumstances be disclosed to third parties without authorization, (3) a right of access and correction exists with respect to all personal information collected, and (4) that a detailed notice of information practices must be furnished to the individual upon request. *[Id.]*

3. Remedies and Penalties

Right to Sue. A person whose information is disclosed in violation of these provisions has a statutory right to bring a civil action for actual damages sustained as a result of the disclosure. (Conn. Gen. Stat. § 38a-995.] In such an action, the court may award costs and reasonable attorney's fees to the prevailing party. *[Id.]* A person whose medical record information is improperly sold or disclosed for marketing without his authorization may bring an action for equitable relief, damages or both. Conn. Gen. Stat. § 38a-988a.J

Fines and Penalties. The insurance Commissioner may hold hearings and may impose administrative remedies, including, in the case of intentional violations, monetary fines. [Conn. Gen; Stat. §~ 38a-9g0 through 38a-993.] A cease and desist order and fine not to exceed $2,000 per violation or $20,000 for multiple negligent violations may be imposed. [Conn. Gen. Stat. § 38a-993.] For intentional violations of the restrictions on selling and marketing medical record

information, the Commissioner may impose a cease and desist order and fine not to exceed $20,000 per violation or $100,000 for multiple violations. *[Id.]* Any person who knowingly *and* willfully obtains information concerning an individual from an insurance entity under false pretenses is subject to a fine not to exceed $10,000. [Conn. Gen. Stat. §~ 38a-9g7.]

F. Nursing Home Facilities and Chronic Disease Hospitals

Any person admitted as a patient to a nursing home facility or chronic disease hospital must be assured confidential treatment of his personal and medical records. The patient may approve or refuse the release of these records to any individual outside the facility, except in the case of his transfer to another health care institution or as required bylaw or third-party payment contract. [Conn. Gen. Stat. § l9a-550.

Remedies and Penalties

Right to sue. A facility that negligently deprives a patient of his right is liable to the patient in a private cause of action for injuries suffered as a result of such deprivation. Willful or reckless disregard of a patient's right may result in punitive damages. The patient also may bring an action for any other type of relief permitted by law, including injunctive and declaratory relief. *[Id.]*

G. Pharmacists

A pharmacist may not reveal any records about pharmaceutical services rendered to a patient without the patient's written or oral consent. [Conn. Gen. Stat. § 20-626.] When oral consent is given it must be noted in the pharmacist's records. *[Id.]* A patient's pharmaceutical information may be disclosed without the patient's consent to: the patient; the prescribing practitioner; third party payers who pay claims on behalf of the patient; any governmental agency with statutory authority to review the information; any person or agency pursuant to subpoena; and to anyone with a written contract with a pharmacy to access the pharmacy's database provided the information accessed is limited to data which does not identify specific individuals. *[Id.]*

III. PRIVILEGES

Connecticut recognizes a number of health care provider-patient privileges, which prohibit a health care provider from disclosing communications made by or to a patient relating to his diagnosis and treatment. [Conn. Gen. Stat. §~ 52-146c (psychologist-patient); 52-146d though 52-146j (psychiatrist-patient); 52-146k (battered women's or sexual assault counselor-victim); 52-146o (physician-patient); 52-$^{1}4^{6}$p (marital and family therapist); 52-14^{6}(q) (social worker); 52-146(s) (professional counselor).

IV. CONDITION-SPECIFIC REQUIREMENTS

A. Birth Defects

Connecticut maintains a birth defects surveillance program to monitor the frequency and types of birth defects. Conn. Gen. Stat. § 19a-56a.] The Commissioner of Public Health must establish a

system to collect information regarding birth defects and other adverse reproductive outcomes, *lid.]* The Commissioner may not use any patient identifying information contained in hospital discharge records to which he may have access for any use that is not related to the monitoring system. [Conn. Gen. Stat. §~ 19a-56a; 19a-56b.] All patient identifying information collected must remain confidential. [Conn. Gen. Stat. § 19a-56b.] Access to such information is limited to the Department of Public Health and other persons who have a valid scientific interest and qualifications and who are engaged in demographic, epidemiologic or other similar studies related to health. In addition, prior to receiving any identifiable information the person must agree, in writing, to maintain confidentiality as prescribed in this section. The commissioner must maintain an accurate record of all persons who are given access to the information in the system. *[Id.)*

Remedies and Penalties

Any person who, in violation of a written agreement to maintain confidentiality, discloses any information provided pursuant to this section, or who uses information provided pursuant to this section in a manner other than that approved by the department, may be denied further access to any confidential information maintained by the program.

B. HIV/AIDS

A person who receives confidential HIV-related information may not disclose or be compelled to disclose that information without the subjects authorization except in limited circumstances. [Conn. Gen. Stat. § 19a-583j Disclosure without the subject's authorization is permitted to: health officers when disclosure is mandated or authorized by law; a health care provider to provide treatment to the subject or the subjects child; those who, in the course of their professional duties have had a significant exposure to HIV infection; and others. [Id.] A statement must accompany each disclosure, advising individuals to whom disclosure is authorized by this statute that they are prohibited from further disclosing the information. [Conn. Gen. Stat. 19a-585.] With a few specified exceptions, a record of all disclosures must be placed in the medical record. *[Id.]*

Remedies and Penalties

Right to Sue. A person has a civil right of action for damages against a person who willfully violates these provisions. [Conn. Gen. Stat. § 19a-590.] In such a suit, damages are to be assessed in an amount sufficient to compensate an individual for the injuries he sustained as a result of the violation. *[Id.]*

C. Drug Abuse

Connecticut maintains programs to treat individuals, who are alcohol dependent, drug dependent or intoxicated as defined by Conn. Gen. Stat. § 680. [Conn. Gen. Stat. § 673] Treatment facilities and hospital may not disclose or allow the disclosure of information that identifies alcohol or drug dependent individuals. [Conn. Gen. Stat. §~ 17a-6S8.] Information regarding the treatment of an alcohol dependent, drug dependent or intoxicated minor may not be disclosed to the minor's parent or guardian. *[Id.]* The Commissioner of Public Health may disclose alcohol and drug related treatment information to researchers as long as no patient identifying information is

released. *[Id.]*

D. Genetic Test Results

An employer, employment agency or a labor organization may not request or require genetic information from an employee, person applying for employment, or a labor organization member or otherwise discriminate against an individual on the basis of genetic information. [Conn. Gen. Stat. *§* 46a-60.]

E. Mental Health

All communications and records of communications relating to diagnosis or treatment of **a** patients *mental* condition between a patient and a psychiatrist are confidential. [Conn. Gen. Stat. *§*~ **52-146d; 52-146e.]** Except as expressly provided by statute, no person may disclose or transmit any communications and records that identify a patient to anyone else without the patients consent. [Conn. Gen. Stat. *§* 52-146e,}

The consent must specify to whom the information is to be disclosed and to what use it will be put. [Id.] Future treatment generally cannot be conditioned on the patients signing a consent to disclose his mental health information. *[Id.]* The patient may withdraw the consent at any time, in writing addressed to the person or office in which the original consent was filed. [*id.]*

Disclosure without the patients consent *may* be made: to others involved in the diagnosis or treatment of the patient; when the psychiatrist determines there is a substantial risk of imminent physical injury by the patient to himself or others; as necessary to place the patient in a mental health facility; to a limited extent, to collect fees; and in other situations. [Conn. Gen. Stat. *§* 52-146f.]

A person engaged in research may have access to patient identifying mental health records where needed for research if the research plan is submitted to and approved by the director of the mental health facility. [Conn. Gen. Stat. *§* 52-146g] Records containing identifiable data may not be removed from the mental health facility. *[Id.]*

Remedies and Penalties

Right to sue. A person aggrieved by a violation of these provisions may petition the superior court for appropriate relief, including temporary and permanent injunctions. [Conn. Gen. Stat. *§* 52-146i.] Such a petition is privileged with respect to assignment for trial. Additionally, a person who is injured may bring a civil action against those who violate these provisions. *[Id.]*

MASSACHUSETTS

Massachusetts statutorily grants a patient the right of access to his medical records maintained by health care providers, hospitals, clinics, other facilities and insurance entities. The disclosure of confidential medical information is restricted by a statutory right of privacy as well as by statutes governing specific entities and medical conditions.

I. PATIENT ACCESS

A. Health Care Providers

Upon request, a health care provider must provide a patient access to and a copy of his medical records. [Mass. Gen. Laws oh. 112, *§* 12CC.] This provision applies to a person or entity providing medical care or services, including but not limited to, physicians, surgeons, therapists, dentists, nurses, and psychologists. *[Id.]*

The patient must pay a reasonable fee for copies. *[Id.]* No fee may be charged to those seeking their records to pursue claims or appeals under the Social Security Act or any other federal or state needs-based benefit program. *lid.]*

A psychotherapist may provide a summary of the record if, in his professional judgment, providing the entire record would adversely affect the patient. *[Id.]If* the psychotherapist elects to provide only a summary, the patient may designate an attorney or another psychotherapist to receive the entire record, *lid.]*

B. Hospitals & Clinics

A patient or his authorized representative has the right to review his hospital or clinic records and must be given a copy of them upon request and payment of a reasonable fee. [Mass. Gen. Laws ch. 111, *§* 70.] No fee may be charged for copies of hospital or clinic records when they are requested to support a claim or appeal under the Social Security Act or any other federal or state needs-based program. [Id.] This right of access applies to records maintained by hospitals or clinics subject to licensure by the department of public health or supported in whole or in part by the commonwealth. In the case of a hospital or clinic under the control of the department of mental health, the records will only be disclosed to the patient when the commissioner of mental health has made a determination that a disclosure would be in the best interest of a patient. [*id.]*

C. Insurance Entities, Including HMOs

1. Scope

The Massachusetts Insurance Information and Privacy Protection Act applies to insurance institutions (defined to include any entity engaged in the business of insurance, HMOs, medical or hospital service plans, preferred provider arrangements and others); insurance representatives (defined to include agents, brokers, advisors and others); and insurance-support organizations. [Mass. Gen. Laws ch. 1751, *§* 8 (detailing entities and persons covered); § 2 (definitions).]

Revised by MHA 07/15/09

The Act covers "personal information," including "medical-record information," which is gathered in connection with an "insurance transaction." [Mass. Gen. Laws ch. 175I, *§* 2 (defining "personal information," "medical-record information" and "insurance transaction").] "Medical-record information" is personal information that: (1) relates to the physical or mental condition, medical history or medical treatment of an individual; and (2) is obtained from a medical professional (broadly defined to include physicians, nurses, pharmacists, clinical psychologists and others); a medical-care institution (broadly defined to include hospitals, clinics, skilled nursing facilities and other institutions); the individual; or the individual's spouse, parent or legal guardian. *[Id.* (defining "medical-record information," "medical professional" and "medical-care institution").] "Medical-record information" includes information concerning the diagnosis or treatment of AIDS or AIDS related complex, but it does not include counseling for these conditions. *[Id.* (defining "medical-record information").]

The access provisions only apply to information that is reasonably locatable and retrievable by the insurance entity. [Mass. Gen. Laws ch. 1751, *§* 8.]

With respect to health insurance, the rights granted by the Act extend to Massachusetts residents who are the subject of the information collected, received or maintained in connection with insurance transactions, as well as applicants, individuals or policyholders who engage in or seek to engage in insurance transactions. [Mass. Gen. Laws ch. 1751, *§* 1.]

2. Requirements

Insurance entities (including HMOs) must permit the individual to inspect and copy his personal information in person or obtain a copy of it by mail, whichever the individual prefers, within 30 business days of receiving a written request. [Mass. Gen. Laws ch. 175, § 8.] If the personal information is in coded form, an accurate translation in plain language must be provided in writing. [Mass. Gen. Laws ch. 1751, *§* 8(bfl2).] In addition to giving the individual a copy of his personal information, the insurance entity must also give the individual a list of the persons to whom it has disclosed such personal information within two years prior to the request for access, if that information is recorded. If the identity of the recipients is not recorded, the entity must inform the individual of the names of those persons to whom it normally discloses personal information. [Mass. Gen. Laws ch. 1751, *§* 8(b)(3).]

Fees. The insurance entity can impose a reasonable fee to cover the costs incurred in providing a copy. [Mass. Gen. Laws ch. 1751, *§*~ 8(e); 10.]

Medical-record information that has been provided to the insurance entity by a medical professional or medical-care institution that is requested by an individual may be supplied either directly to the requesting individual or to a medical professional designated by the individual, at the option of the individual. [Mass. Gen. Laws ch. 1751, § 8(d).]

Mental health record information may be provided to the individual only with the approval of the treating professional.

Right to Amend. A person has a statutory right to have any factual error corrected and any

misrepresentation or misleading entry amended or deleted, in accordance with stated procedures. [Mass. Gen. Laws ch1751, *§* 9.] Within 30 business days from the date of receipt of a written request, the insurance entity must either: (1) correct, amend or delete the portion of recorded personal information in dispute; or (2) after reinvestigating the issue, notify the individual of its refusal to make the correction, amendment or deletion, the reasons for the refusal, and the individual's right to file a statement of disagreement and request review by the insurance commissioner. *[Id]*

The insurance entity must furnish any correction, amendment, fact of deletion, or statement of disagreement (where the insurer has refused to make the change) to:

- any person specifically designated by the individual who may have, within the preceding 2 years, received recorded personal information about the individual;
- to any insurance support organization that has systematically received recorded personal information from the insurance institution within the preceding 7 years; and
- to the insurance-support organization that furnished the personal information that has been corrected, amended, or deleted. [Mass. Gen, Laws ch. 1751, *§ 9.]*

If the insurance entity has refused to take the requested action, it must also file the individual's statement of disagreement with the disputed personal information and provide a means by which anyone reviewing the disputed personal information will be made aware of the statement and have access to it. Additionally, in any subsequent disclosure by the insurance entity of the information that is the subject of disagreement, the insurance entity must clearly identify the matter in dispute and provide the individuals statement along with the recorded personal information being disclosed. *[Id.]*

3. **Remedies and Penalties**

Right to Sue. A person whose rights under these provisions are violated has the right to file a civil action seeking equitable relief within two years of the violation. [Mass. Gen. Laws ch. 1751, *§* 20] The court may award costs and reasonable attorney's fees to the prevailing party. [Id.]

Fines and Penalties. Additionally, the insurance commissioner may hold hearings and impose administrative remedies, including monetary penalties. [Mass. Gen. Laws ch.1751, §~ 15; 17; 18.]

D. State Government

The Fair Information Practices Act (Mass. Gen. Laws ch. 66A, § 1 through *§* 3) imposes on state agencies a variety of duties related to the personal data that they maintain. The Act applies to every agency of the executive branch of the government, including but not limited to any constitutional or other office, executive office, department, division, bureau, board, commission or committee having either statewide or local jurisdiction. [Mass. Gen. Laws ch. 66A, *§* 1 (defining "agency").]

The Act applies to "personal data," which generally is defined as information concerning an individual which, because of name, identifying number, mark or description can be readily

associated with **a** particular individual, [id. (defining "personal data").]

Rights under the Fair Information Practices Act may be exercised by the "data subject," the individual to whom personal data refers. *[Id.* (defining "data subject")]

1. Patient Access Requirements

Upon written request, an agency must inform an individual whether it maintains personal data concerning him and must make that data fully available to the subject or his authorized representative. [Mass. Gen. Laws ch. 66A, *§* 2,] The agency must respond to the request in writing and in a format that is understandable to the requestor. *[Id.]* To the extent it has maintained such information, the agency must also make available to an individual, upon his request, a list of the uses made of his personal data, including the identity of all persons and organizations which have gained access to the data. *[Id.]*

Agencies must also have procedures that allow an individual to contest the denial of access to his personal data. [id.]

Right to Amend. Agencies must have procedures that allow a data subject or his representative to contest the accuracy, completeness, pertinence, timeliness or relevance of his personal data. They must also have procedures that permit the data to be corrected or amended when requested and there is no disagreement. When there is **a** disagreement, the data subject's claim must be noted and included as part of the personal data and included in any subsequent disclosure or dissemination of the disputed data. [Mass. Gen. Laws ch, 66A, § 2.]

2. Other Requirements

Agencies may not collect or maintain more personal data than are reasonably necessary for the performance of the agency's statutory functions. [Mass. Gen. Laws ch. 66A, *§* 2.] Personal data that is collected must be maintained with such accuracy, completeness, timeliness, pertinence and relevance as is necessary to assure fair determination of a data subject's qualifications, character, rights, opportunities, or benefits when such determinations are based upon such data. *[Id.]* An agency may not rely on any exceptions in the Freedom of Information Act to deny a subject access to his own information that would otherwise be accessible under the Fair Information Practices Act. *[id.]*

II. RESTRICTIONS ON DISCLOSURE

A. General Right of Privacy

Under Massachusetts law, a person has a statutory right against unreasonable, substantial or serious interference with his privacy. [Mass. Gen. Laws ch. 214, § lB.] Medical records and information are generally encompassed in this right.

There are statutory exceptions to the right of privacy that explicitly allow disclosure of medical information. For example, physicians, health care facilities, nursing homes and other medical providers may, without patient consent, disclose to certain government agencies information

concerning the diagnosis, treatment or condition of a patient in connection with establishing eligibility for, or entitlement to, government benefits (such as veteran's benefits and aid to dependent children) or in connection with mandatory health department reports or reports required by other laws. [Mass. Gen. Laws ch. 112, *§* 12G.]

Remedies and Penalties

Right to Sue. A person has the right to maintain a civil suit in equity to enforce his right of privacy and to seek damages. [Mass. Gen. Laws ch. 214, § lB.]

B. Hospitals & Other Facilities

The records of hospitals and other licensed facilities are confidential "to the extent provided by law," a phrase which is not explicated in the statute. [Mass. Gen. Laws ch. 111, *§* 70E.] This provision applies to hospitals, clinics, nursing homes, institutions for the care of unwed mothers, infirmaries maintained in a town, rest homes, and charitable homes for the aged; any state hospital operated by the department; any private, county or municipal facility, department or ward which is licensed or subject to licensing by the department of mental health or by the department of mental retardation; and other enumerated types of facilities. [Id.]

This statute includes two exceptions to this general promise of confidentiality: (1) third-party reimbursers are permitted to inspect and copy any and all records relating to diagnosis, treatment or other services provided to any person for which coverage benefit or reimbursement is claimed, so long as the policy or certificate under which the claim is made provides that such access to such records is permitted; and (2) this section does not preclude disclosure of facility records for peer review or utilization review procedures applied and implemented in good faith. [Mass. Gen. Laws ch. Ill, § 70E.]

Health facilities must provide patients, upon admission, a notice of their statutory rights, including their general right to confidentiality. [*ld.]*

Remedies and Penalties

Right to Sue. Any person whose rights under this section are violated may bring, in addition to any other action allowed by law, a civil action pursuant to the statutory provisions governing malpractice claims. [Mass. Gen. Laws ch. 111,§7OE.]

C. Insurance Entities, Including HMOs

1. Scope

The Massachusetts Insurance Information and Privacy Protection Act applies to insurance institutions (defined to include any entity engaged in the business of insurance, HMOs, medical or hospital service plans, preferred provider arrangements and others); insurance representatives (defined to include agents, brokers, advisors and others); and insurance-support organizations. [Mass. Gen. Laws ch. 1751, *§* S {detailing entities and persons covered); *§* 2 definitions).]

The Act covers "personal information," including "medical-record information," which is gathered in connection with an "insurance transaction." [Mass. Gen. Laws ch. 1751, *§* 2 (defining "personal information," "medical-record information" and "insurance transaction").]

"Medical-record information" is personal information that: (1) relates to the physical or mental condition, medical history or medical treatment of an individual; and (2) is obtained from a medical professional (broadly defined to include physicians, nurses, pharmacists, clinical psychologists and others); a medical-care institution (broadly defined to include hospitals, clinics, skilled nursing facilities and other institutions); the individual; or the individual's spouse, parent or legal guardian. *[Id.* (defining ~medical-record information," "medical professional" and "medical-care institutions).] "Medical-record information" includes information concerning the diagnosis or treatment of AIDS or ARC, but it does not include other aspects of the definition of "counseling" for AIDS or ARC issued by the Centers for Disease Control and Prevention, [*id.* (defining "medical-record information").]

With respect to health insurance, the rights granted by the Act extend to Massachusetts residents who are the subject of the information collected, received or maintained in connection with insurance transactions, as well as applicants, individuals or policyholders who engage in or seek to engage in insurance transactions. [Mass. Gen. Laws ch. 1751, *§* 1.]

2. Requirements

a. Authorizations for Obtaining Health Information from Others

If an insurance entity uses an authorization form to obtain health information in connection with an insurance transaction, the authorization form must conform to the requirements of the statute. [Mass. Gen. Laws ch. 1751, *§* 6.] The authorization form must be dated and written in plain language. It must specify the types of persons authorized to disclose information concerning the individual; specify the nature of the information authorized to be disclosed; identify who is authorized to receive the information; specify the purposes for which the information is collected; specify the length of time such authorization shall remain valid (which will vary depending on the purpose of the authorization); and advise the individual of the right to receive a copy of the authorization form. [Mass. Gen. Laws ch. 1751, *§* 6.]

b. Disclosure Authorization Requirements and Exceptions Generally, an insurance entity may not disclose personal or privileged information about an individual that it collected or received in connection with an insurance transaction without that individual's written authorization. [Mass. Gen. Laws ch 1751, § 13.] Authorizations submitted by those *other* than insurance entities must be in writing, signed and dated, and they are effective for up to one year. [Mass. Gen. Laws ch. 1751, *§* 13(1).]

An insurance entity may not disclose information to another insurance entity pursuant to an authorization form unless the form meets the detailed requirements of the statute. *[Id.]* See "Authorizations for Obtaining Health Information from Others," above. However, there are several circumstances where an authorization is not required before one insurance entity discloses information to another. [Mass. Gen. Laws ch. 1731, *§* 13(3).]

The Act prohibits insurance entities from disclosing medical-record information for marketing purposes without the written authorization of the subject of the information. [Mass. Gen Laws ch. 1751, *§* 13(11).]

Authorization exceptions. There are numerous circumstances under which an insurance entity can disclose information without the individual's authorization. These include disclosures to law enforcement agencies in order to prevent or prosecute fraud; disclosures pursuant to a facially valid search warrant, subpoena or other court order; disclosures made for research purposes; and others. [Mass. Gen. Laws ch. 1751, *§* 13.]

c. **Notice Requirements**

Some types of insurance entities (insurance institutions and insurance representatives) must provide to all applicants and policyholders written notice of their information practices. [Mass. Gen. Laws ch. 1751, *§* 4.] The notice must be in writing and must state:

- The categories of personal information that may be collected from persons other than the individual proposed for coverage;
- The type of disclosure permitted by the Act and the circumstances under which such disclosure may be made without prior authorization (to the extent that the disclosures occur with such frequency as to indicate a general business practice);
- A description of the rights to see, copy and amend personal information and how those rights may be exercised
- Other specified items.

[Id.] The insurance entity has the option of providing an abbreviated notice. *[Id.]*

3. Remedies and Penalties

Right to Sue. A person whose information is disclosed in violation of these provisions has a statutory right to bring a civil action for special and compensatory damages sustained as a result of the disclosure. [Mass. Gen. Laws ch. 1751, *§* 20.] In such an action, the court may award costs and reasonable attorney's fees to the prevailing party. *[Id.]* The individual cannot bring any other cause of action in the nature of defamation, invasion of privacy or negligence except against a person who discloses false information with malice or willful intent to injure, or against a person who misidentifies an individual as the subject of information and who discloses such misidentified information to others. [Mass. Gen. Laws ch. 1751, *§* 21.]

Fines and Penalties. Additionally, the insurance commissioner may hold hearings and impose administrative remedies, including monetary penalties.[Mass. Gen. Laws ch. 1751, §~ 15; 17; 18.] Any person who knowingly and willfully obtains information concerning an individual from an insurance entity under false pretenses is subject to a fine not to exceed $10,000 or 1 year imprisonment or both. {Mass. Gen. Laws cit 1751, § 22.]

D. State Government

1. Freedom of Information Act.

Government-maintained medical files and information are not considered to be "public records" open to inspection under the Freedom of Information Act. [Mass. Gen. Laws ch.4, §7, cl.26.]

2. Fair Information Practices Act

a. **Scope**

The Fair Information Practices Act (Mass. Gen. Laws ch. 66A, *§* 1 through *§* 3} imposes on state agencies a variety of duties related to the personal data that they maintain. The Act applies to every agency of the executive branch of the government, including but not limited to any constitutional or other office, executive office, department, division, bureau, board, commission or committee having either statewide or local jurisdiction. [Mass. Gen. Laws ch. 66A, *§* 1 (defining "agency").]

The Act applies to 'personal data," which generally is defined as information concerning an individual which, because of name, identifying number, mark or description can be readily associated with a particular individual. *[Id.* (defining personal data").]

b. **Disclosure Requirements**

Under the Fair Information Practices Act, government agencies that hold medical information must ensure that other agencies or individuals are not provided access to personal information unless otherwise allowed by statute or is approved by the individual whose personal data are sought. [Mass. Gen, Laws ch. 66A, *§* 2.] Agencies must comply with a data subject's request to disseminate his data to a third person if practicable. *[Id.]* The agency may charge a reasonable fee if necessary. [*Id.]*

Medical or psychiatric data may be provided to a treating physician in an emergency where the patient is unable to provide consent, however, the patient must be notified of the disclosure once the emergency has ended, *[id.]*

Agencies must maintain procedures to ensure that no personal data are made available in response to a demand for data made by means of compulsory legal process, unless the data subject has been notified of such demand in reasonable time that he may seek to have the process quashed. [*id.]*

Agencies must also maintain a complete and accurate record of every access to and every use of any personal data by persons or organizations outside of or other than the holder of the data, including the identity of all such persons and organizations which have gained access to the personal data and their intended use of such data. [Id.] The holder of the information does not need to record any such access of its employees acting within their official duties. [*id.]*

c. Other Requirements

Agencies must undertake a number of administrative steps to protect the privacy of personal information. For example, each agency must identify one individual immediately responsible for the personal data system whose duty it is to insure that the requirements of this chapter for preventing access to or dissemination of personal data are followed. [Mass. Gen. Laws ch. 66A, *§* 2.] Additionally, each agency must inform relevant employees of the rules concerning the use and disclosure of personal information, and potential penalties for failure to comply with the law. *[Id.]* They must also take reasonable precautions to protect personal data from dangers of fire, theft, flood, natural disaster, or other physical threat.

Revised by MHA 07/15/09

III. PRIVILEGES

Massachusetts recognizes mental health provider-patient privileges under which a patient in any court proceeding can refuse to disclose and can prevent others from disclosing confidential conversations made with the therapist for purposes of diagnosis or treatment. [Mass Gen. Laws ch. 233, *§* 2GB.] This evidentiary privilege extends to psychiatrists, psychologists, and certified psychiatric nurse mental health clinical specialists and their respective patients *[Id.],* as well as to licensed social workers and sexual assault counselors. [Mass Gen. Laws ch.1 12, *§* 135B; ch. 233, *§* 20J].

IV. CONDITION-SPECIFIC REQUIREMENTS

A. Cancer

Massachusetts maintains a cancer registry for the purpose of conducting epidemiological surveys and applying appropriate preventive and control measures. [Mass. Gen. Laws ch. 111, *§* 1113.] All mandatory reports are confidential and may only be released upon written request of the patient or his authorized representative. [id.] Identifiable information may also be released without authorization to researchers, but no research studies shall identify the subjects of these records or reports. *[Id.]*

B. Contagious Diseases

Reports that the health department requires to be filed concerning infectious diseases (including AIDS) *must* be kept confidential by the department and are not open for public inspection or copying by any other governmental agency or by any other person. [Mass. Gen. Laws ch.111D, *§* 6; Mass. Regs. Code title. 105, *§* 300.140 (listing AIDS as a reportable disease).] Any person who makes a report that is required by the department may not be held liable in a civil proceeding for having violated a trust or confidential relationship. [Mass. Gen. Laws ch. ii 1D, *§* 6.]

C. Genetic Information & Testing

Massachusetts has a number of provisions that restrict the use and disclosure of genetic information and that govern genetic testing. It is important to note that these provisions use varying definitions of the terms “genetic information” and “genetic test.”

1. Employers

Massachusetts restricts employers’ collection, use and disclosure of genetic information. For purposes of the provisions applying to employers, “genetic test’ is defined as a test of human DNA, RNA, mitochondrial DNA, chromosomes or proteins for the purpose of identifying genes, inherited or acquired genetic abnormalities, or the presence or absence of inherited or acquired characteristics in genetic material. [Mass. Gen. Laws ch. 1513, *§* 1 (22) & (23).] “Genetic information” means any written, recorded individually identifiable result of a genetic test or explanation of such a result or family history pertaining to the presence, absence, variation, alteration, or modification of a human gene or genes. The term does not include information

pertaining to the abuse of drugs or alcohol which is derived from tests given for the exclusive purpose of determining the abuse of drugs or alcohol. *[Id]*

An employer may not collect, solicit or require disclosure of genetic information as a condition of employment; require or administer a genetic test as a condition of employment; offer a person an inducement to undergo a genetic test or otherwise disclose genetic information; inquire about a person's genetic information (or that of family members) or about previous genetic testing; seek, receive or maintain genetic information for non-medical purposes; or use the results of a genetic test to affect an individual's employment. [Mass. Gen. Laws ch. 151B, *§* 4 (19).] These prohibitions also apply to employment agencies, labor organizations and licensing agencies. *[Id.]*

2. Health Care Providers and Others

Massachusetts restricts the manner in which genetic tests may be undertaken and in which genetic information may be used and disclosed by health care providers, health care facilities, genetic testing agencies and others. For purposes of these restrictions, "genetic test" is defined as a test of human DNA, RNA, mitochondrial DNA, chromosomes or proteins for the purpose of identifying genes, inherited or acquired genetic abnormalities, or the presence or absence of inherited or acquired characteristics in genetic material. The term genetic test does not include tests given for drugs, alcohol, cholesterol, or HIV; or any test for the purpose of diagnosing or detecting an existing disease, illness, impairment or disorder. [Mass. Gen, Laws ch, 111, *§* 70G.] "Genetic information" is defined as any written or recorded individually identifiable result of a genetic test or explanation of such a result. [Mass. Gen. Laws ch. 111, *§* 70G.] The term genetic information does not include any information about an identifiable person that is taken: as a biopsy, autopsy, or clinical specimen solely for the purpose of conducting an immediate clinical or diagnostic test that is not a genetic test (as defined above); as a blood sample solely for blood banking; as a newborn screening; as confidential research information for use in research conducted for the purpose of generating scientific knowledge about genes and other specified purposes; or as information pertaining to the abuse of drugs or alcohol which is derived from tests given for the exclusive purpose of determining the abuse of drugs or alcohol, [id.]

The records and reports of any hospital, dispensary, laboratory, hospital-affiliated registry, physician, insurance institution, insurance support organization, or insurance representative, and commercial genetic testing company, agency, or association that pertain to any genetic information are not public records. [Mass. Gen, Laws ch. 111, *§* 70G] The contents of these records and reports may not be divulged without the informed written consent of the individual. *[Id.]* Genetic information may be disclosed without the test subject's authorization in a number of instances including, but not limited to: upon proper judicial order; to a person whose official duties, in the opinion of the commissioner of health, entitles receipt of the information; and for use in epidemiological or clinical research conducted for the purpose of generating scientific knowledge about genes or learning about the genetic basis of disease or for developing pharmaceutical and other treatments of disease. *[Id.]*

Similarly, no facility (broadly defined in Mass. Gen. Laws ch. 111, *§* 70E] and no physician or health care provider may test any person for genetic information or disclose the results of a genetic test without obtaining the prior written consent of the individual. [Mass. Gen. Laws ch. 111, *§* 700.] This law includes exceptions relating to epidemiological or clinical research, law

enforcement officials, and health care personnel or others executing official duties pursuant to chapter 22E (which relates to the state DNA database). *Id.]*

Remedies and Penalties

Right to Sue. Any person whose rights under these provisions have been violated, interfered with, or attempted to be interfered with may institute a civil action for injunctive and other equitable relief. [Mass. Gen. Laws ch. ill, *§* 70G] The attorney general is also authorized to institute relief on behalf of the commonwealth. *[Id.I*

3. **Health Plans**

Massachusetts statutorily restricts the manner in which health insurers and other types of health plans can acquire genetic test information. For the most part, a "genetic test" is a test of human DNA, RNA, mitochondrial DNA, chromosomes or proteins for the purpose of identifying the genes or genetic abnormalities, or the presence or absence of inherited or acquired characteristics in genetic material. [Mass. Gen. Laws ch. 175, *§* 108H; ch. 176A, *§* SB; cit 176B, *§* 5B; ch. 176G, *§* 24; ch. 1761, § 4A.]. In the case of an insurance company or broker the term does not include tests given for the exclusive purposes of determining the abuse of drugs or alcohol. [Mass. Gen. Laws ch. 175, § 108H.] The term "genetic information" means a written recorded individually identifiable result of a genetic test or explanation of such a result.

No insurance company or insurance broker may require genetic tests or genetic information as a condition of the issuance or renewal of an individual or group policy of accident or sickness insurance. [Mass. Gen. Laws ch. 175, *§* 108H.]

No insurer, agent or broker authorized to issue policies against disability from injury or disease or for long term care shall require an applicant to undergo a genetic test as a condition of the issuance or renewal of such policy. [Mass. Gen. Laws ch. 175, *§* 108I.] These entities may ask an applicant whether or not the applicant has taken a genetic test, [id.] The applicant is not required to answer such a question on an application, but the failure to do so may result in an increased rate or denial of coverage. *[Id.]*

No hospital service corporation, medical service corporation, health maintenance organization or preferred provider organization may require genetic tests or private genetic information as a condition of the issuance or renewal or their respective plans. [Mass. Gen. Laws ch. 176A, *§* 3B; ch. l76B, *§* 5B; ch. 1760, *§* 24; ch. 1761, *§* 4A.]

D. HIV/AIDS.

Physicians, other health care providers, hospitals, clinics and other facilities (broadly defined) are prohibited from conducting an HIV test, disclosing the test results, or identifying the subject of such a test without the prior written informed consent of the patient. [Mass. Gen. Laws ch. 111, *§* 70F.] The consent must be separate from a general authorization to release other medical information. *[Id.]* In addition, no employer shall require the HIV test as a condition of employment. *[Id.)* This statute actually refers to the "HTLV-lll" test, an early name for HIV, but is understood to encompass HIV testing.

E. Mental Health

Generally, a psychologist needs a patient's written consent to disclose any confidential communications about that patient, including the fact that the patient is undergoing treatment. [Mass. Gen. Laws ch. 112, § 129A.] Disclosure without the patient's consent is allowed: where the patient poses an imminent danger to himself or others; when the psychologist is attempting to collect amounts owed (but only the nature of services provided, dates of services and other financial data can be disclosed); for peer review and utilization review purposes; and in other circumstances. *[Id.]* This provision does not prevent a nonprofit hospital service or medical service corporation from inspecting and copying any and all records relating to diagnosis, treatment or other services provided to any person for which coverage, benefit or reimbursement is claimed, so long as the policy or certificate under which the claim is made provides that such access to the records is permitted. [*id.]*

Records of those admitted to mental health facilities under state supervision are private and not open to public inspection. [Mass. Gen. Laws ch. 123, § 36.] These records may be disclosed: upon proper judicial order, whether or not in connection with pending judicial proceedings; to the patient's attorney upon request by the patient or attorney; when in the best interest of the patient as provided in the rules and regulations of the department of mental health; and as required by statutory provisions governing sex offenses. This section governs the patient records of the department notwithstanding any other provision of law, [id.]

An HMO is prohibited from conditioning the receipt of benefits upon a member's provision of consent to disclose information regarding services for mental disorders. [Mass. Gen. Laws, ch. 176G, § 4B.] This provision does not prohibit the disclosure of non-privileged information; aggregate patient data; patient utilization data in connection with an investigation into fraud (by the patient or provider) or professional misconduct; patient information needed for coordination of benefits, subrogation, peer review or utilization review; or of certain patient information to self-insured plans. *[Id,]*

A medical service corporation may not disclose information it acquires about any subscriber or covered family member pertaining to outpatient diagnosis or treatment of a mental or nervous condition without the informed written consent of the covered individual. [Mass. Gen. Laws, ch. 176G, § 20.] The corporation may not condition the receipt of covered benefits upon the provision of such consent. *[Id.]* This provision does not prohibit the disclosure of non-privileged information; aggregate patient data; patient utilization data in connection with an investigation into fraud (by the patient or provider) or professional misconduct; patient information needed for coordination of benefits, subrogation, peer review or utilization review; or of certain patient information to self-insured plans. *[Id]*

An insurance company (providing accident or health insurance) may not condition the receipt of benefits upon an insured's provision of consent to disclose information pertaining to outpatient diagnosis or treatment of a mental or nervous condition. [Mass. Gen. Laws ch. 175, § 108E.) This provision does not prohibit the disclosure of non-privileged information; aggregate patient data; patient utilization data in connection with an investigation into fraud (by the patient or provider) or professional misconduct; patient information needed for coordination of benefits, subrogation, peer review or utilization review; or of certain patient information to self-insured plans. *[Id.]*

See Section 1 (A through C) above for discussion of access to mental health records.

F. Substance Abuse

Treatment facilities must maintain the confidentiality of each patient's treatment records. [Mass. Gen. Laws, ch. 111E, *§* 18] Disclosure is only permitted with a judicial order or with the patient's informed written consent. *[Id.]* A consent must be signed by the patient, state the name of the person or entity to whom the disclosure will be made, the type of information to be disclosed and the purpose of the disclosure. *[Id.]*

NOTICE OF PRIVACY PRACTICES

Program Address:_____

_____

_____

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.

If you have any questions about this Privacy Notice, please contact our Director of Programs at _____<Phone Number>.

I. Introduction

This Notice of Privacy Practices describes how we may use and disclose your protected health information to carry out treatment, payment or health care operations and for other purposes that are permitted or required by law. This Notice also describes your rights regarding health information we maintain about you and a brief description of how you may exercise these rights. This Notice further states the obligations we have to protect your health information.

Protected health information means health information (including identifying information about you) we have collected from you or received from your health care providers, health plans, your employer or a health care clearinghouse. It may include information about your past, present or future physical or mental health or condition, the provision of your health care, and payment for your health care services.

We are required by law to maintain the privacy of your health information and to provide you with this notice of our legal duties and privacy practices with respect to your health information. We are also required to comply with the terms of our current Notice of Privacy Practices.

II. How We Will Use and Disclose Your Health Information

We will use and disclose your health information as described in each category listed below. For each category, we will explain what we mean in general, but not describe all specific uses or disclosures of health information.

Revised by MHA 07/15/09

A. Uses and Disclosures That May Be Made For Treatment, Payment and Operations

1. For Treatment. We will use and disclosure your health information without your authorization to provide your health care and any related services. We will also use and disclose your health information to coordinate and manage your health care and related services. For example, we may need to disclose information to a case manager who is responsible for coordinating your care.

We may also disclose your health information without your authorization among our clinicians and other staff (including clinicians other than your therapist or principal clinician), who work at MHA. For example, our staff may discuss your care at a case conference.

In addition, we may disclose your health information to another health care provider (e.g., your primary care physician or a laboratory) who is involved in your care but is working outside of MHA.

2. For Payment. We may use or disclose your health information without your authorization so that the treatment and services you receive are billed to, and payment is collected from, your health plan or other third party payer. By way of example, we may disclose your health information to permit your health plan to take certain actions before your health plan approves or pays for your services. These actions may include:

- making a determination of eligibility for services
- reviewing your services for purposes of utilization review, to ensure the appropriateness of your care, or to justify the charges for your care.

For example, your third party payor may ask us to share your health information in order to determine if services are billable on a certain day.

3. For Health Care Operations. We may use and disclose health information about you without your authorization for our health care operations. These uses and disclosures are necessary to run our organization and make sure that our consumers receive quality care. These activities may include, by way of example, quality assessment and improvement, reviewing the performance or qualifications of our clinicians, training students in clinical activities, licensing, accreditation, business planning and development and general administrative activities. We may combine health information of many of our consumers to decide what additional services we should offer, what services are no longer needed, and whether certain new treatments are effective. We may also combine our health information with health information from other providers to compare how we are doing and see where we can make improvements in our services. When we combine our health information with information of other providers, we will remove identifying information so others may use it to study health care or health care delivery without identifying specific clients.

We may also use and disclose your health information to contact you to remind you of your appointment.

Finally, we may use and disclose your health information to inform you about possible treatment options or alternatives that may be of interest to you.

4. Health-Related Benefits and Services. We may use and disclose health information to tell you about health-related benefits or services that may be of interest to you. If you

do not want us to provide you with information about health-related benefits or services, you must notify the Director of Programs in writing at the address provided on page one of this notice. Please state clearly that you do not want to receive materials about health-related benefits or services.

B. Uses and Disclosures That May be Made Without Your Authorization, But For Which You Will Have an Opportunity to Object

Persons Involved in Your Care. We may provide health information about you to someone who helps pay for your care. We may use or disclose your health information to notify or assist in notifying a family member, personal representative or any other person that is responsible for your care of your location, general condition or death. We may also use or disclose your health information to an entity assisting in disaster relief efforts and to coordinate uses and disclosures for this purpose to family or other individuals involved in your health care. In limited circumstances, we may disclose health information about you to a friend or family member who is involved in your care. If you are physically present and have the capacity to make health care decisions, your health information may only be disclosed with your agreement to persons you designate to be involved in your care.

But, if you are in an emergency situation, we may disclose your health information to a spouse, a family member, or a friend so that such person may assist in your care. In this case we will determine whether the disclosure is in your best interest and, if so, only disclose information that is directly relevant to participation in your care.

And, if you are not in an emergency situation but are unable to make health care decisions, we will disclose your health information to:

- your health care agent if we have received a valid health care proxy from you**,**
- your guardian or medication monitor if one has been appointed by a court, or
- if applicable, the state agency responsible for consenting to your care.

C. Uses and Disclosures That May be Made Without Your Authorization or Opportunity to Object

1. Emergencies. We may use and disclose your health information without your authorization in an emergency treatment situation. By way of example, we may provide your health information to a paramedic who is transporting you in an ambulance. If a clinician is required by law to treat you and your treating clinician has attempted to obtain your authorization but is unable to do so, the treating clinician may nevertheless use or disclose your health information to treat you.

2. Research. We may disclose your health information to researchers when their research has been approved by an Institutional Review Board or a similar privacy board that has reviewed the research proposal and established protocols to protect the privacy of your health information.

3. As Required By Law. We will disclose health information about you when required to do so by federal, state or local law.

4. To Avert a Serious Threat to Health or Safety. We may use and disclose health information about you when necessary to prevent a serious and imminent threat to your health or safety or to the health or safety of the public or another person. Under these circumstances, we will only disclose health information to someone who is able to help prevent or lessen the threat.

5. **Organ and Tissue Donation.** If you are an organ donor, we may release your health information to an organ procurement organization or to an entity that conducts organ, eye or tissue transplantation, or serves as an organ donation, bank, as necessary to facilitate organ, eye or tissue donation and transplantation.

6. Public Health Activities. We may disclose health information about you as necessary for public health activities including, by way of example, disclosures to:

> report to public health authorities for the purpose of preventing or controlling disease, injury or disability;

> report vital events such as birth or death;

> conduct public health surveillance or investigations;

> report child abuse or neglect;

> report certain events to the Food and Drug Administration (FDA) by a person subject to the jurisdiction of the FDA including information about defective products or problems with medications;

< notify consumers about FDA-initiated product recalls;

> notify a person who may have been exposed to a communicable disease or who is at risk of contracting or spreading a disease or condition;

> notify the appropriate government agency if we believe an adult has been a victim of abuse, neglect or domestic violence. We will only notify an agency if we obtain your agreement or if we are required or authorized by law to report such abuse, neglect or domestic violence.

7. Health Oversight Activities. We may disclose health information about you to **a** health oversight agency for activities authorized by law. Oversight agencies include government agencies that oversee the health care system, government benefit programs such as Medicare or Medicaid, other government programs regulating health care and civil rights laws.

8. **Disclosures in Legal Proceedings**. We may disclose health information about you to a court when a judge orders us to do so. We also may disclose health information about you in legal proceedings without your permission or a judge's order when:

> you are a party to a legal proceeding and we receive a subpoena for your health information. Normally, we will not provide this information in response to a subpoena without your authorization if the request is for substance abuse records or for information relating to AIDS or HIV status or genetic testing;

> your health information involves communications made during a court ordered psychiatric examination;

> you introduce your mental or emotional condition in evidence in support of your claim or defense in any proceeding and the judge approves our disclosure of your health information;

> you sue any of our clinicians or staff for malpractice or initiate a complaint with a licensing board against any of our clinicians;

> the legal proceeding involves child custody, adoption or dispensing with consent to adoption and the judge approves our disclosure of your health information;
> one of our social workers brings a proceeding, or is asked to testify in a proceeding, involving foster care of a child or commitment of a child to the custody of the Massachusetts Department of Children and Families.

9. Law Enforcement Activities. We may disclose health information to a law enforcement official for law enforcement purposes when:

> you agree to the disclosure; or
> when the information is provided in response to an order of a court; or
> we determine that the law enforcement purpose is to respond to a threat of an imminently dangerous activity by you against yourself or another person; or
> the disclosure is otherwise required by law.

We may also disclose health information about a client who is a victim of a crime, without a court order or without being required to do so by law. However, we will do so only if the disclosure has been requested by a law enforcement official and the victim agrees to the disclosure or, in the case of the victim's incapacity, the following occurs:

> the law enforcement official represents to us that (i) the victim is not the subject of the investigation and (ii) an immediate law enforcement activity to meet a serious danger to the victim or others depends upon the disclosure; and
> we determine that the disclosure is in the victim's best interest.

10. Medical Examiners or Funeral Directors. We may provide health information about our consumers to a medical examiner. Medical examiners are appointed by law to assist in identifying deceased persons and to determine the cause of death in certain circumstances. We may also disclose health information about our consumers to funeral directors as necessary to carry out their duties.

11. Military and Veterans. If you are a member of the armed forces, we may disclose your health information as required by military command authorities. We may also disclose your health information for the purpose of determining your eligibility for benefits provided by the Department of Veterans Affairs. Finally, if you are a member of a foreign military service, we may disclose your health information to that foreign military authority.

12. National Security and Protective Services for the President and Others. We may disclose medical information about you to authorized federal officials for intelligence, counter-intelligence, and other national security activities authorized by law. We may also disclose health information about you to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or so they may conduct special investigations.

13. Inmates. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may disclose health information about you to the correctional institution or law enforcement official.

14. Workers' Compensation. We may disclose health information about you to comply with the Massachusetts Workers' Compensation Law. These disclosures will usually be made only when we have received a court order or, sometimes, when we have received a subpoena for the information.

Ill. <u>Uses and Disclosures of</u> <u>Your Health Information with Your Permission</u>. Uses and

disclosures not described in Section II of this Notice of Privacy Practices will generally only be made with your written permission, called an "authorization." You have the right to revoke an authorization at any time. If you revoke your authorization we will not make any further uses or disclosures of your health information under that authorization, unless we have already taken an action relying upon the uses or disclosures you have previously authorized.

IV. Your Rights Regarding Your Health Information.

A. Right to Inspect and Copy.

You have the right to request an opportunity to inspect or copy health information used to make decisions about your care — whether they are decisions about your treatment or payment of your care. Usually, this would include clinical and billing records, but not psychotherapy notes.

You must submit your request in writing to our Director of Programs at the address provided on page one of this notice. If you request a copy of the information, we may charge a fee for the cost of copying, mailing and supplies associated with your request.

We may deny your request to inspect or copy your health information in certain limited circumstances. In some cases, you will have the right to have the denial reviewed by a licensed health care professional not directly involved in the original decision to deny access. We will inform you in writing if the denial of your request may be reviewed. Once the review is completed, we will honor the decision made by the licensed health care professional reviewer.

B. Right to Amend.

For as long as we keep records about you, you have the right to request us to amend any health information used to make decisions about your care — whether they are decisions about your treatment or payment of your care. Usually, this would include clinical and billing records, but not psychotherapy notes.

To request an amendment, you must submit a written document to our Director of Programs at the address provided on page one of this notice and tell us why you believe the information is incorrect or inaccurate.

We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. We may also deny your request if you ask us to amend health information that:

> was not created by us, unless the person or entity that created the health information is no longer available to make the amendment;
> is not part of the health information we maintain to make decisions about your care;
> is not part of the health information that you would be permitted to inspect or copy; or
> is accurate and complete.

If we deny your request to amend, we will send you a written notice of the denial stating the basis for the denial and offering you the opportunity to provide a written statement disagreeing with the denial. If you do not wish to prepare a written statement of disagreement, you may ask that the requested amendment and our denial be attached to all

future disclosures of the health information that is the subject of your request.

If you choose to submit a written statement of disagreement, we have the right to prepare a written rebuttal to your statement of disagreement. In this case, we will attach the written request and the rebuttal (as well as the original request and denial) to all future disclosures of the health information that are the subject of your request.

C. Right to an Accounting of Disclosures.

You have the right to request that we provide you with an accounting of disclosures we have made of your health information. An accounting is a list of disclosures. But this list will not include certain disclosures of your health information, by way of example, those we have made for purposes of treatment, payment, and health care operations.

To request an accounting of disclosures, you must submit your request in writing to the Director of Programs at the address provided on page one of this notice. For your convenience, you may submit your request on a form called a "Request For Accounting,' which you may obtain from our Director of Programs. The request should state the time period for which you wish to receive an accounting. This time period should not be longer than six years and not include dates before January 1, 2010.

The first accounting you request within a twelve month period will be free. For additional requests during the same 12 month period, we will charge you for the costs of providing the accounting. We will notify you of the amount we will charge and you may choose to withdraw or notify your request before we incur any costs.

D. Right to Request Restrictions.

You have the right to request a restriction on the health information we use or disclose about you for treatment, payment or health care operations. You may also ask that any part (or all) of your health information not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in Section II(B)(2) of this Notice of Privacy Practices.

You must request the restriction in writing and addressed to the Director of Programs at the address provided on page one of this notice. The Director of Programs will ask you to fill out a Request for Restriction Form, which you should complete and return to the Director of Programs.

We are not required to agree to a restriction that you may request. If we do agree, we will honor your request unless the restricted health information is needed to provide you with emergency treatment.

E. Right to Request Confidential Communications.

You have the right to request that we communicate with you about your health care only in a certain location or through a certain method. For example, you may request that we contact you only at work or by e-mail. To request such a confidential communication; you must make your request in writing to the Director of Programs at the address provided on page one of this notice. We will accommodate all reasonable requests. You do not need to give us a reason for the request; but your request must specify how and where you wish to be contacted.

F. Right to a Paper Copy of this Notice.

You have the right to obtain a paper copy of this Notice of Privacy Practices at any time.

Even if you have agreed to receive this Notice of Privacy Practices electronically, you may still obtain a paper copy. To obtain a paper copy, contact our Director of Programs at the address provided on page one of this notice.

V. Confidentiality of Substance Abuse Records

For individuals who have received treatment, diagnosis or referral for treatment from our drug or alcohol abuse programs, the confidentiality of drug or alcohol abuse records is protected by federal law and regulations. As a general rule, we may not tell a person outside the programs that you attend any of these programs, or disclose any information identifying you as an alcohol or drug abuser, unless:

- you authorize the disclosure in writing; or
- the disclosure is permitted by a court order; or
- the disclosure is made to medical personnel in a medical emergency or to qualified personnel for research, audit or program evaluation purposes; or
- you threaten to commit a crime either at the drug abuse or alcohol program or against any person who works for our drug abuse or alcohol programs.

A violation by us of the federal law and regulations governing drug or alcohol abuse is a crime. Suspected violations may be reported to the Unites States Attorney in the district where the violation occurs.

Federal law and regulations governing confidentiality of drug or alcohol abuse permit us to report suspected child abuse or neglect under state law to appropriate state or local authorities.

Please see 42 U.S.C. **§** 290dd-2 for federal law and 42 C.F.R., Part 2 for federal regulations governing confidentiality of alcohol and drug abuse patient records.

VI. Complaints

If you believe your privacy rights have been violated, you may file a complaint with us or with the Secretary of the U.S. Department of Health and Human Services. To file a complaint with us, contact our Complaint Officer at MHA, 995 Worthington Street, Springfield, MA 01109. All complaints must be submitted in writing.

Our Director of Programs, who can be contacted at the address provided on page one of this notice, will assist you with writing your complaint, if you request such assistance.

We will not retaliate against you for filing a complaint.

VII. Changes to this Notice

We reserve the right to change the terms of our Notice of Privacy Practices. We also reserve the right to make the revised or changed Notice of Privacy Practices effective for all health information we already have about you as well as any health information we receive in the future. We will post a copy of the current Notice of Privacy Practices at our main office and at each site where we provide care. You may also obtain a copy of the current Notice of Privacy Practices by requesting of our Director of Programs, at the address provided on page one of this notice, that a copy be sent to you in the mail or by asking for one any time you are at our offices.

Revised by MHA 07/15/09

ACKNOWLEDGEMENT OF REVIEW OF
MHA NOTICE OF PRIVACY PRACTICES

I acknowledge that I have reviewed MHAs Notice of Privacy Practices and that my signature below indicates that I have reviewed and understand MHA's Notice of Privacy Practices.

_____ _____

Signature Date

_____

Printed Name

_____

Program

Revised by MHA 07/15/09

Matrix of Disclosure
(supplement to policy 4)
See pages 125 and 126 of this document

Revised by MHA 07/15/09

MODEL AUTHORIZATION FORM
Mental Health Association, Inc.
995 Worthington Street, Springfield, MA 01109

SECTION A: USE OR DISCLOSURE OF HEALTH INFORMATION

By signing this Authorization, I authorize the use or disclosure of my individually-identifiable health information maintained by

The Provider **[Person/Organization(s) providing the information]:**

_____
Print Name

_____
Print Address

My health information may be disclosed under this Authorization to:

The recipient [Person/Organization(s) receiving the information]:

_____
Print Name

_____
Print Address

Health information includes information collected from me or created by the Provider, or information received by the Provider from another health care provider, a health plan, my employer or *a* health care clearinghouse. Health information may relate to my past, present or future physical or mental health or condition the provision of my health care, or payment for my health care services.

Any provider that operates a federally-assisted alcohol or drug abuse program is prohibited from disclosing information about treatment for alcohol or drug abuse without my specific written authorization unless a disclosure is otherwise authorized by federal regulations governing Confidentiality of Alcohol and Drug Abuse Patient Records (42 CFR, Part 2).

I further understand that under state law the Provider is prohibited from disclosing information about my HIV status without my specific written authorization. The Provider is also prohibited under state law from disclosing the results of a genetic test (including the identity of a person being tested) without first obtaining an authorization that constitutes

"informed written consent", except when the test results disclosed will be used only as confidential research information for use in epidemiological or clinical research conducted for the purpose of generating scientific knowledge about genes or learning about the genetic basis of disease or for developing pharmaceutical and other treatments of disease.

Policy 2

SECTION B: SCOPE OF USE OR DISCLOSURE

Check One:

Health information that may be used or disclosed through this Authorization is as follows:

O All health information about me, including my clinical records, created or received by the Provider. This information may include, if applicable:

- Information pertaining to the identity, diagnosis, prognosis or treatment for alcohol or drug abuse maintained by a federally-assisted alcohol or drug abuse program; or;
- Information regarding AIDS, ARC or HIV including, for example, a test for the presence of HIV antibodies or antigens, regardless of whether (i) this test is ordered, performed, or reported and (ii) the test results are positive or negative.
- information regarding the results of a genetic test.

O All health information about me as described in the preceding checkbox, **excluding the following:**

_____

_____

O Specific health information including only: _____

_____

_____

Note: *Describe the health information to be excluded or included in a specific and meaningful fashion.*

SECTION C: PURPOSE OF THE USE OR DISCLOSURE

The purpose(s) of this Authorization is (are):
Check one:

☐ **Specifically, the following purpose(s) _____**

_____

_____; or

☐ **The request for information to be used or disclosed has been initiated by the Client and the Client does not elect to disclose its purpose.**
Note: This box may NOT *be checked if the information to be used or disclosed pertains to alcohol or drug abuse identity, diagnosis prognosis or treatment*

SECTION D: EXPIRATION

This Authorization
expires: _____
(Insert applicable event or date — mm/dd/yy)
Note: if an expiration event is used, the event must relate to the Client or the purpose of the use or disclosure.

SECTION E: OTHER IMPORTANT INFORMATION

1. I understand that the Provider cannot guarantee that the Recipient will not redisclose my health information to a third party. The Recipient may not be subject to federal laws governing privacy of health information. However if the disclosure consists of treatment information about a client in a federally-assisted alcohol or drug abuse program, the Recipient is prohibited under federal law from making any further disclosure of such information unless further disclosure is expressly permitted by written consent of the Client or as otherwise permitted under federal law governing Confidentiality of Alcohol and Drug Abuse Patient Records (42 CFR, Part 2).

2. I understand that I may refuse to sign this Authorization and that my refusal to sign will not affect my ability to obtain treatment (or payment, if applicable) from Mental Health Association except when I am (i) receiving research-related treatment or (ii) receiving health care solely for the purpose of creating information for disclosure to a third party. If either of these exceptions apply, my refusal to sign an authorization will result in my not obtaining treatment (or payment, if applicable) from the Provider.

3. I understand that I may revoke this Authorization in writing at any time, except that the revocation will not have any effect on any action taken by the Provider in reliance on this Authorization before written notice of revocation is received by the Provider. I further understand that that I must provide any notice of revocation in writing to the Director of Programs at Mental Health Association. The address of the Director of Programs is:

_____

_____

_____

****

I have read and understand the terms of this Authorization. I have had an opportunity to ask questions about the use or disclosure of my health information**.**

Client's signature**:**_____ Date of signature**:** _____

Print Client's full name: _____

Clients Home
Address: _____

Client's Home Telephone**:**_____ Date of Birth:_____

When client is not competent to give consent, the signature of a parent, guardian, health care agent (proxy) or other representative is required.

Signature of legal representative**:** _____ Date of signature**:**_____

Print name: _____

Relationship of representative to client:_____

Optional: Photo ID. # of Signator _____ Witness: _____

The Client should be provided with a copy of the signed Authorization.

Revised by MHA 07/15/09

MODEL SUBSTANCE ABUSE REDISCLOSURE NOTICE

Mental Health Association, Inc.
995 Worthington Street, Springfield, MA 01109

PROHIBITION ON REDISCLOSURE OF CONFIDENTIAL INFORMATION

This notice accompanies a disclosure of information concerning a client in an alcohol or drug abuse treatment program, made to you with the consent of such client.

This information has been disclosed to you from records protected by federal confidentiality rules governing federally-assisted drug or alcohol abuse programs (42 C.F.R., Part 2). The federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 C.F.R., Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose.

The federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse client.

Revised by MHA 07/15/09

Authorization for Disclosure of Protected Health Information

I, _____ authorize the disclosure of my protected health information as described herein. I understand that this authorization is voluntary and made to confirm my direction. I understand that, if the person(s) or organization(s) that I authorize to receive my protected health information are not subject to federal and state health information privacy laws,[2] subsequent disclosure by such person(s) or organization(s) may not be protected by those laws.

1. I authorize the following person(s) and/or organization(s) to disclose my protected health information (as specified below):

   Name(s)_____

   Organization(s)_____

   Address_____

2. I authorize the following person(s) and/or organization(s) to receive my protected health information, as disclosed by the person(s) and/or organization(s) above.

   Name(s)_____

   Address_____

   Organization(s) _____

3. Specific description of the protected health information that I authorize for disclosure (authorization to disclose psychotherapy notes must be separate):

4. Specific description of the purpose for each use or disclosure (or write "At the request of the individual" in this space):

5. I understand that I may revoke this authorization in writing at any time, except to the extent that the person(s) and/or organization(s) named above have taken action in reliance on this authorization

Revised by MHA 07/15/09

6. This authorization expires on _____, or in the event that
(date)
_____which ever occurs first.
(event)

I have had the opportunity to read and consider the contents of this authorization. I confirm that the contents are consistent with my direction.

_____ _____
Signed Date

Name:_____

Address:_____

Telephone:_____ Social Security No.:_____

_____
Relationship or Authority of Personal Representative
(if applicable)

_____
[1].Protected health information ('PHI") is health information that is created or received by a health care provider, health plan, or health care clearinghouse which relates to: 1) the past, present, or [future physical or mental health of an individual; 2) the provision of health care to an individual; or 3) the past, present, or future payment for the provision of health care to an individual. To be protected, the information must be such that it identifies the individual or provides a reasonable basis to believe that the information can identify the individual. *45* C,F.R.164.508. -

[2]. These laws apply to health plans, health care providers, and health care clearinghouses.

Revised by MHA 07/15/09

MODEL SUBSTANCE ABUSE REDISCLOSURE NOTICE

Mental Health Association, Inc.
995 Worthington Street, Springfield, MA 01107

PROHIBITION ON REDISCLOSURE OF CONFIDENTIAL INFORMATION

This notice accompanies a disclosure of information concerning a client in an alcohol or drug abuse treatment program, made to you with the consent of such client.

This information has been disclosed to you from records protected by federal confidentiality rules governing federally-assisted drug or alcohol abuse programs (42 C.FR., Part 2). The federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 C.F.R., Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose.

The federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse client.

Revised by MHA 07/15/09

Clear and Present Danger Disposition Sheet A
Danger to Self

Name of Client:_____

Name of Clinician:_____

Date of Completion:_____

****

This form should be completed by a licensed treating clinician whenever confronted by the situation described below. The treating clinician should complete the relevant section of this form, sign the form indicating that the required actions have been taken, and place the form in the client record. In taking the required actions, the counselor should **ONLY** *disclose to a third party information essential to the protection of the rights and safety of others. Also, a treating clinician should never take any action (even those outlined in this Disposition Sheet) which, in the exercise of reasonable professional judgment, would endanger him or herself or increase the danger to a potential victim. If the treating clinician believes this is likely to occur, the treating clinician should document why he or she believes the danger will be enhanced and consult with the Assistant Executive Director/Director of Program Operations* _____

****

Situation: A client presents a clear and present danger to him/herself and refuses explicitly or by his/her behavior to voluntarily accept further appropriate treatment. **A** client presents a clear and present danger to his/herself when (a) the treating clinician, in the exercise of his/her professional judgment, believes the client presents a substantial risk of physical impairment or injury to him/herself as manifested by evidence of threats of, or attempts at, suicide or serious bodily harm, or (b) the treating clinician, in the exercise of his/her professional judgment, believes that the client presents a very substantial risk of physical impairment or injury to him/herself as manifested by evidence that such person's judgment is so affected that he or she is unable to protect him or herself in the community and that reasonable provision for his/her protection is not available in the community.

Revised by MHA 07/15/09

Complete the following:

a. The nature of the clear and present dangers:

b. How was this danger communicated to you? (Please include dates information was communicated to you.)

c. Please briefly describe any conversation you may have had with the client about the danger (including the date thereof). If you were unable to speak to the client, please so indicate and describe your efforts to contact the client or, alternatively, document your reasons for not contacting the client.

d. How did the client manifest his or her intention not to accept further treatment (include description of communications, if any, and actions of client, along with the relevant dates)?

e. If you have a reasonable basis to believe that the client can be committed to a hospital under Chapter 123 of the Massachusetts General Laws, you have

a duty in this situation to seek a commitment. In any event, please provide documentation for one of the following actions:

1. Describe all efforts made to seek a commitment of the client to a psychiatric hospital (include persons contacted, date and outcome of contact):

2. Alternatively, describe the basis for believing that the client cannot be committed to a hospital.

_____

Signature of a Licensed Treating Clinician

Revised by MHA 07/15/09

Clear and Present Danger Disposition Sheet B
Danger to Others

Name of Client:_____

Name of Clinician:_____

Date of Completion:_____

****

This form should be completed by a licensed treating clinician whenever confronted by one of the two situations described below. In each case, the treating clinician should complete the relevant section of this form, sign the form indicating that the required actions have been taken, and place the form in the client record. in taking the required actions, the counselor should ONLY disclose to *a third party information essential to the protection* of *the rights and safety of others. Also, a treating clinician should never take any action (even those outlined in this Disposition Sheet) which, in the exercise of reasonable professional judgment, would endanger him or herself or increase the danger to a potential victim. If the treating clinician believes this is likely to occur, the treating clinician should document why he or she believes the danger will be enhanced and consult with the Assistant Executive Director/Director of Program Operations.*

****

Situation 1: A client has communicated to the treating clinician an explicit threat to kill or inflict serious bodily injury upon a reasonably identified person and the client has the apparent intent and ability to carry out the threat.

Complete the following:

A. Please describe the nature of the threat, as well as how and when it was communicated to you:

_____
_____
_____
_____
_____

B. The "reasonably identified person" is:

Revised by MHA 07/15/09

C. Please describe why you believe the client has the apparent intent and ability to carry out the threat:

_____
_____
_____
_____
_____
_____

D. In the event situation #1 has occurred, a treating clinician has a duty to take reasonable precautions, which means making reasonable efforts to take one or more (as appropriate to the circumstances) of the following actions:

1. Communicate the threat to the reasonably identified person. (Please document the nature of such communication, including dates.):

2. Notify the appropriate law enforcement agency in the vicinity of where the client or potential victim resides. (Please document names of officers at any law enforcement agency contacted and the date of contact.)

3. Arrange for the client to be hospitalized voluntarily. (Please document efforts to have client admit him/herself to a psychiatric treatment unit.)

4. Take appropriate steps to initiate proceedings for involuntary hospitalization. (Please document steps taken to initiate proceedings.)

Revised by MHA 07/15/09

Situation 2: When the client has a history of physical violence which is known to the treating clinician and the treating clinician has a reasonable basis to believe that there is a clear and present danger that the client will attempt to kill or inflict serious bodily injury upon a reasonably identified person. This will occur when, in the exercise of professional judgment, the treating clinician believes that the client's words or behavior strongly suggest that there is a reasonable possibility that the client will attempt to kill or inflict serious bodily injury on a reasonably identified victim whom the client's words or behavior or history have clearly identified as a likely target of such behavior.

Complete the following:

A. Please document the known history of physical violence including the source of your knowledge thereof:

B, Please describe your basis for believing there is a clear and present danger that the client will attempt to kill or inflict serious injury upon a reasonably identified person:

C. The 'reasonably identified person" is:

E. In the event situation #2 has occurred, a treating clinician has a duty to take reasonable precautions, which means making reasonable efforts to take one or more (as appropriate to the circumstances) of the following actions:

1. Communicate the threat to the "reasonably identified person." (Please document the nature of such communication, including dates.):

Revised by MHA 07/15/09

2. Notify the appropriate law enforcement agency in the vicinity of where the client or potential victim resides. (Please document names of officers at any law enforcement agency contacted and the date of contact.)

3. Arrange for the client to be hospitalized voluntarily. (Please document efforts to have client admit him/herself to a psychiatric treatment unit.)

4. Take appropriate steps to initiate proceedings for involuntary hospitalization. (Please document steps taken to initiate proceedings.)

_____

Signature of Licensed Treating Clinician

Revised by MHA 07/15/09

Request for Accounting of PHI Disclosed by *Agency*

I request an accounting of all PHI disclosed by Mental Health Association, Inc. pursuant to the requirements of the Privacy Rule. I understand that this accounting will not include disclosures that were:

1. made to me or my personal representative
2. made to carry out the treatment, payment or operational activities of the organization.
3. for facility directory purposes, to discuss my healthcare with a family member or other individual involved in my care, or for other permitted notification purposes.
4. made for national security and intelligence purposes
5. made to a correctional institution or to law enforcement and I am currently an inmate
6. made incident to a use or disclosure that is otherwise permitted.
7. made pursuant to an authorization
8. made as part of a limited data set
9. occurred prior to January 1, 2010

The period of time I am requesting the accounting for is from:

_____ to _____

I understand that this period of time can be for no longer than 6 years and cannot include any time period before January 1, 2010, the date the Privacy Rule became effective. I also understand that the first accounting I request in any 12 month period will be given to me for no charge.

Signed: _____

Date:_____

Revised by MHA 07/15/09

Print Name Below

For a client requesting more than one accounting in a 12 month period the following additional signature should be obtained:

I understand that because I have requested more than one accounting in a 12 month period that I will be charged the cost to the AGENCY for completing this accounting. I understand that this cost will be _____ and that payment must be made at the time I receive the accounting or prior to the accounting being mailed to me.

Agreed and
accepted:_____Date:_____

_____
Print Name

Revised by MHA 07/15/09

PHI Disclosure to be Included in Client's Accounting

If this disclosure was made:

1. To the client:
2. To carry out our treatment, payment or operational activities;
3. For facility directory purposes, to discuss their healthcare with a family member or other individual involved in their care, or for other permitted notification purposes;
4. For national security or intelligence purposes; or
5. To a correctional institution or to law enforcement and the client is currently an inmate;
6. Incident to a use or disclosure that is otherwise permitted;
7. Pursuant to an authorization;
8. As part of a limited data set;
9. Prior to January 1, 2010

STOP — DO NOT COMPLETE THIS FORM!

For all other disclosures:

Date of disclosure: _____

Name of person and organization receiving disclosure:

Address of person/organization receiving this disclosure:
Description of what information was disclosed:

Brief statement of purpose of disclosure:

Signature of staff person making disclosure: _____
Date of Disclosure: _____

Revised by MHA 07/15/09

<Letterhead of Organization>

Client Restriction on the Uses and Disclosures of PHI for Treatment, Payment or Operations

Client Name:_____

Client Number: _____

Social Security Number:_____

Address:_____

Telephone Number:_____

Restriction requested:_____
_____
_____
_____

This restriction reviewed with client on:

Date:_____

By:_____

(Name and Position of Individual Reviewing Restriction with Client)
Face to Face:_____ Phone call: _____
Restriction Approved: Yes □
No □

Date: _____

Signature of employee approving/denying restriction: _____

Name of employee approving/denying restriction: _____

Signature of Client (required):_____

Revised by MHA 07/15/09

Signature of Director of Programs:_____Date:_____

Form I — Business Associate Agreement — New Contracts

BUSINESS ASSOCIATE AGREEMENT
With [Full Legal Name of Business Associate]
Effective Date: [Insert Effective Date of this Agreement]

This Business Associate and Chain of Trust Agreement (the "Agreement") is made as of the Effective Date set forth above, by and between [Insert full legal name of your entity] ("Health Care Provider) with a principal office at (Insert address of your principal office] and Insert full legal name of Business Associate] ("Business Associate") with a principal office at [Insert address of Business Associate].

Whereas, Health Care Provider desires to disclose, and Business Associate desires to use, disclose, create, and/or receive, Individually Identifiable Health Information (i) on behalf of the Health Care Provider in the performance of certain functions or activities involving Individually Identifiable Health Information, or (ii) while providing certain designated services (including legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services) to or for the Health Care Provider;

Whereas, Health Care Provider and Business Associate wish to comply with the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. §1320(d)) ("HIPAA') including without limitation the Standards for Privacy of Individually Identifiable Health Information (42 C.F.R., Fart 160 and 164), the Standards for Electronic Transactions (45 C.F.R., Part 160 and 162), the Security Standards (45 C.F.R., Part 142) and Massachusetts Data Privacy laws (M.G.L 93H 201 CMR 17 and Executive Order 504) (collectively, the "Standards") promulgated or to be promulgated by the Secretary of Health and Human Services (the "Secretary").

I. Definitions.
The following terms, as used in this Agreement, shall have the meanings set forth below:

1.1 "Data Aggregation" means, with respect to Protected Health Information created or received by Business Associate in its capacity as the business associate of Health Care Provider, the combining of such Protected Health Information by Business Associate with the Protected Health Information received by Business Associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

1.2 "Designated Record Set" means a group of records maintained by or for Health Care Provider that is (i) the medical records and billing records about individuals maintained by or for Health Care Provider, (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for Health Care Provider to make decisions about individuals. As used in this Agreement, the term "Record' means any item, collection, or grouping of information that includes Protected Health information and is maintained, collected, used, or disseminated by or for the Health Care Provider.

1.3 "Electronic Media" means the mode of electronic transmissions. It includes the internet, extranet (using internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

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

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

(b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (i) identifies the individual, or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

1.5 "Protected Heath Information" or "PHI" means Individually Identifiable Health Information that is (a) transmitted by electronic media, (b) maintained in any medium constituting Electronic Media; or (c) transmitted or maintained in any other form or medium. "Protected Health Information" excludes individually identifiable health information in: (a) education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. §1232g; (b) records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (c) employment records held by a covered entity in its role as an employer.

II. Obligations of Business Associate With Respect to PHI.

2.1 Use and Disclosure of PHI. Business Associate shall use and disclose PHI only as required to satisfy its obligations under this Agreement or as required bylaw and shall not otherwise use or disclose any PHI. Health Care Provider shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Standards for Individually Identifiable Health Information (hereinafter, the "Privacy Standards") if done by Health Care Provider [Optional; except with respect to uses and disclosures of PHI for data aggregation or management and administrative activities of Business Associate, as provided in Sections 2.12 and 2.13 of this Agreement, respectively].

2.2 Purposes and Limitations on Use or Disclosure of PHI.

2.2.1 Purposes. Except as otherwise provided in this Agreement, Business Associate may use or disclose PHI on behalf of, or to provide services to, Health Care Provider only for the following purposes, so long such use or disclosure of PHI would not violate (a) the minimum necessary policies and procedures of Health Care Provider, and (b) the Privacy Standards if used or disclosed by the Health Care Provider:

[List specific purposes for Business Associate's use or disclosure of PHI] e.g., to conduct a survey and determine the accreditation status of

Health Care Provider; to provide accounting services to Provider; to conduct research services using patient medical records for XYZ purposes, etc.

2.2.2 **Property Rights In PHI**. Business Associate hereby acknowledges that, as between Business Associate and Health Care Provider, all PHI shall be and remain the sole property of Health Care Provider, including any forms of PHI developed by Business Associate in the course of fulfilling its obligations under this Agreement.

2.2.3 **Minimum Necessary**. Business Associate further represents that, to the extent Business Associate requests Health Care Provider to disclose PHI to Business Associate; such request is only for the minimum necessary PHI for the accomplishment of Business Associate's purposes.

2.2.4 **Reporting Violations**. Business Associate may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R.§ 164.502W(1).

2.3 Safeguards and Security.

2.3.1 **Safeguards.** Business Associate agrees to use all appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement or as required by law.

2.3.2. **Security.** Business Associate shall establish security policies, processes and procedures in compliance with the Security Standards including without limitation administrative procedures, physical safeguards, technical security services, and technical security mechanisms, in order to protect the integrity and confidentiality of PHI exchanged electronically. Business Associate acknowledges and agrees that the legal, technical or business requirements for security of PHI may change and that, at any time during the term of this Agreement, Health Care Provider shall have the right to require Business Associate to adopt new policies, processes and procedures, or to require modifications to existing policies, processes and procedures. Health Care Provider shall communicate in writing such new or altered requirements to Business Associate, and Business Associate agrees to promptly implement such requirements. Business Associate shall supply a written copy of its security policies and procedures to Health Care Provider upon the execution of this Agreement.

2.4 **Reporting Disclosures of PHI;** Mitigation. Business Associate shall report any use or disclosure in violation of this Agreement within 2 business days of learning of such violation by Business Associate or its officers, directors, employees, contractors or other agents or by any third party to which Business Associate has disclosed PHI. Business Associate agrees to mitigate promptly at the direction of Health Care Provider any harmful effect of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement. Health Care Provider may, at its sole discretion, access records of Business Associate, direct an investigation of a use or disclosure by Business Associate, and determine the appropriate method of mitigation; Business Associate agrees to cooperate fully with Health Care Provider in any such investigation or mitigation.

2.5 **Employees, Subcontractors, and Agents**. Business Associate hereby represents and warrants that its employees and agents will be specifically advised of, and shall comply

in all respects with, the terms and conditions of this Agreement. Business Associate shall obtain and maintain, in full force and effect, a binding contract with each of its agents including without limitation subcontractors who will have access to PHI and whose PHI is received from, or created or received by, Business Associate on behalf of the Health Care Provider. Business Associate shall further ensure that any such agent agrees in such contract to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such PHI.

2.6 **Accounting of Disclosures**.

2.6.1 **Accounting by Business Associate.** Business Associate agrees to document any disclosures of PHI made by Business Associate, as well as other information related to such disclosures, as would be required for Health Care Provider to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. §184.528. Business Associate also agrees to provide Health Care Provider, in a time and manner designated by Health Provider, information collected in accordance with this section of the Agreement, to permit Health Care Provider to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. §164.525.

2.6.2 **Recordkeeping.** Business Associate agrees to implement an adequate record keeping process to enable it to comply with the requirements of this section of the Agreement.

2.7 **Privacy Practices.** Business Associate hereby acknowledges and agrees that Health Care Provider has provided it with a copy of its Notice of Privacy Practices. Business Associate agrees to comply with the practices identified in the Notice of Privacy Practices, to the extent that such practices would apply to Health Care Provider if it were performing Business Associate's functions, and will utilize as appropriate Health Care Provider's form documents. Health Care Provider hereby reserves the right to change the applicable privacy practices and related documents at any time. To the extent that such changes affect the duties and obligations of Business Associate under this Agreement, Business Associate will implement such changes within 10 days of receipt of notice of the change.

2.8 **Revocation or Modification of Consumer Permission**. Health Care Provider shall provide Business Associate with any changes in, or revocation of, permission by an individual to use or disclose PHI, if such changes affect Business Associate's permitted or required uses and disclosures.

2.9 **Consumer Restrictions on Uses and Disclosures**. Health Care Provider shall notify, Business Associate of any restriction to the use or disclosure of PHI that CE 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.

2.10 **Availability of Books and Records**. 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, Health Care Provider available to Health Care Provider, or to the Secretary, in a time and manner designated by Health Care Provider or designated by the Secretary, for purposes of the Secretary determining Health Care Provider's compliance with the Privacy Standards. The provisions of this section shall survive termination of this Agreement.

2.11 **Notice of Request for PHI**. Business Associate agrees to notify Health Care Provider within 2 business days of receipt of any request, subpoena or other legal process to obtain PHI or an accounting of PHI, Health Care Provider in its discretion shall determine whether Business Associate may disclose PHI pursuant to such request, subpoena, or other legal process. Business Associate agrees to cooperate fully with Health Care Provider in any legal challenge initiated by Health Care Provider in response to such request, subpoena, or other legal process. The provisions of this section shall survive the termination of this Agreement.

[Optional: Include the following section only if you intend Business Associate to be able to use PHI in its own management or administration functions.]

2.12 **Proper Management and Administration of Business Associate.**

2.12.1 **Permissible Uses**. Except as otherwise limited in this Agreement Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

2.12.2 **Permissible Disclosures**. Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are required by law, or that 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 the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

[Optional: Include the following section only if you intend Business Associate to perform Data Aggregation functions.]

2.13 **Data Aggregation**. Except as other limited in this Agreement, Business Associate may use PHI to provide Data Aggregation services to Health Care Provider as permitted by 42 C.F.R. **§** 164.5Q4(e)(2)~)(B).

[**Optional: Include the following section only if Business Associate will receive PHI in Designated Record Sets.]**

2.14 **Access to Records in a Designated Record Set**. At the request of Health Care Provider and in the time and manner designated by Health Care Provider, Business Associate agrees to provide access to PHI in a Designated Record Set to Health Care Provider (and its employees and agents) or, as directed by Health Care Provider, to an individual in order to meet the requirements under 45 C.F.R. **§** 164.524.

[Optional: Include the following section only if Business Associate will receive PHl in Designated Record Sets.]

2.15 **Amendment of Records in a Designated Record Set**. At the request of Health Care Provider and in the time and manner designated by Health Care Provider, Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that

the Health Care Provider (or its employees or agents) directs or agrees to pursuant to 45 C.F.R. § 164.526.

III. Other Obligations of Business Associate.

(**Insert Duties and Obligations of Business Associate Not Related to HIPAA]**

IV. Other Obligations of Health Care Provider.

[Insert Duties and Obligations of Health Care Provider Not Related to HIPAA1

V. Term and Termination.

5.1 **Term**.

(Insert provisions relating to term of this Agreement — the Term to commence with the Effective Date. If Business Associate functions are the only activities to be performed under this Agreement, you may use the following provision:]

The term of this Agreement shall commence upon the Effective Date and continue thereafter for a period of [Insert period (in days, months or years) that contract is in effect] or until earlier terminated in accordance with Section 5.2 below.

5.2 **Termination.**

5.2.1 **General Termination Provisions.**

[Insert general provisions relating to the termination of this Agreement. If Business Associate functions *are* the only activities to be performed under this Agreement and you wish to permit Business Associate to terminate this Agreement without cause, you may use the following provision:]

Either Health Care Provider or business Associate may terminate this Agreement at any time without cause with **(Insert number of days of required notice — typically 30 to 120 days, depending upon the time period needed for a transitional** day's prior written notice.

5.2.2 **Termination Upon Breach**. Any other provision of this Agreement notwithstanding, this Agreement may be terminated by Health Care Provider upon 5 business days written notice to Business Associate in the event that the Business Associate breaches any provision (including any covenant, representation, warranty, or condition) contained in Article II of this Agreement or any other such provision of this Agreement that relates to PHI and such breach is not cured within the 5 day notice period; provided, however, that in the event that termination of this Agreement is not feasible in Health Care Provider's sole discretion, Health Care Provider shall report the breach to the Secretary.

5.2.3 **Return or Destruction of PHI upon Termination.**

5.2.3.1 **General Provisions**. Upon termination of this Agreement, Business Associate shall either return or destroy, at the option of Health Care Provider, all PHI received from the Health Care Provider, or created or received by Business Associate on behalf of the Health Care

Provider and which Business Associate still maintains in any form. Business Associate shall not retain any copies of such PHI.

5.2.3.2 **Alternative Arrangement**. Notwithstanding the foregoing, to the extent that the Health Care Provider agrees that it is not feasible to return or destroy such PHI, Business Associate shall provide Health Care Provider with a written acknowledgement and notification of the conditions that make return or destruction infeasible. Business Associate hereby agrees to (a) extend the protections of this Agreement to such PHI only for those purposes that make the return or destruction infeasible, (b) limit further uses and disclosures of such PHI to such purposes, and (c) extend any term or provision of this Agreement relating to PHI so that such term or condition shall survive termination of this Agreement. Thereafter, such PHI shall be used or disclosed solely for such purpose or purposes which prevented the return or destruction of such PHI.

5.2.3.3 **Applicability of Provisions**. The provisions of this section of the Agreement shall apply, to the same extent that it applies to Business Associate, to PHI that is in the possession of agents of Business Associate.

5.2.4 **Health Care Providers Right to Cure**. At the expense of Business Associate, Health Care Provider shall have the right to cure any breach of Business Associate's obligations under this Agreement with respect to PHI. Health Care Provider shall give Business Associate notice of its election to cure any such breach and Business Associate shall cooperate fully in the efforts by the Health Care Provider to cure Business Associate's breach. All requests for payment for such services of the Health Care Provider shall be paid within 30 days of Business Associate's receipt of the request for payment.

VI. Miscellaneous.

6.1 **Indemnification.**

[Insert an indemnification provision for this Agreement. If the only purpose of this Agreement is to comply with HIPAA's business associate requirements, you may use the following indemnification provision.)

Business Associate hereby agrees to indemnify and hold Health Care Provider and its employees and agents harmless from and against any and all loss, liability, or damages, including reasonable attorney's fees, arising out of or in any manner occasioned by a breach of any provision of this Agreement by Business Associate, or its employees or agents.

6.2 **Insurance.**

[Insert insurance provision for this Agreement. If the only purpose of this Agreement is to comply with HIPAA's business associate requirements, you may use the following insurance provision.]

Business Associate shall obtain and maintain, at its sole expense, during the term of this Agreement liability insurance on an occurrence basis with responsible insurance companies covering claims based upon a violation of any of the Standards or any applicable state law or regulation concerning the privacy of patient information and

claims based upon its obligations pursuant to Section 6.1 of this Agreement in amount not less than **[Insert minimum amount of required coverage; for high risk business associates — suggest $1,000,000 per claim.] [Optional, suggest inserting for high or medium risk business associates:**
Such insurance policy shall name Health Care Provider as an additional named insured and shall provide for 30 days prior written notice to Health Care Provider in the event of any decrease, cancellation, or non-renewal of such insurance.] A copy of such policy or a certificate evidencing the policy shall be provided to Health Care Provider upon written request.

6.3 **Injunction.** Business Associate hereby agrees that Health Care Provider will suffer irreparable damage if Business Associate breaches this Agreement and that such damages will be difficult to quantify. Business Associate hereby agrees that Health Care Provider may file an action for an injunction to enforce the terms of this Agreement against Business Associate, in addition to any other remedy Health Care Provider may have.

6.4 **Independent Contractor.** Under this Agreement, Business Associate shall at all times be acting and performing in the status of independent contractor to Health Care Provider.

Business Associate shall not by virtue of this Agreement be deemed a partner or joint venturer of Health Care Provider. No person employed by Business Associate will be an employee of Health Care Provider, and Health Care Provider shall have no liability for payment of any wages, payroll taxes, and other expenses of employment for any employee of Business Associate. Business Associate is constituted the agent of Health Care Provider only for the purpose of, and to the extent necessary to, carrying out its obligations under this Agreement.

6.5 **Authorization for Agreement.** Business Associate represents and warrants that the execution and performance of this Agreement by Business Associate has been duly authorized by all necessary laws, resolutions and corporate action, and this Agreement constitutes the valid and enforceable obligations of the Business Associate in accordance with its terms.

6.6 **Governing Law and Choice of Forum.** The parties agree that this Agreement shall be construed in accordance with the laws of the Commonwealth of Massachusetts, without regard to conflict of laws principles. The parties further agree that any litigation concerning this Agreement shall only be brought in a court of competent jurisdiction within the Commonwealth of Massachusetts. To the extent that the Privacy Standards apply to any provision in this Agreement, any ambiguity shall be resolved to permit Health Care Provider to comply with the Privacy Standards.

6.7 **Binding Agreement; Assignment**. This Agreement shall inure to the benefit and be binding upon the parties hereto and their respective successors and assigns; provided, however, that Business Associate may not assign any rights or obligations under this Agreement without the prior written consent of Health Care Provider.

6.8 **Notices.** Any notice, request, demand, report, approval, election, consent or other communication required or permitted under the terms of this Agreement (collectively, "Notice") shall be in writing and either delivered personally, by registered or certified mail, return receipt requested, postage prepaid, or by reputable overnight courier, addressed as follows:

To Health Care Provider:

[Insert Full Legal Name of Entity]
[Street Address]
[City or Town, State, Zip Code]
Attn: [Insert Title of Officer of your Organization, e,g., President]

With a copy to: [If copy is desired, insert name and address of person to whom copy should be sent.]

To Business Associate:

[Insert Full Legal Name of Entity]
[Street Address]
[City or Town, State, Zip Code]
Attn: [Insert Title of Officer in Business Associate's Organization, e.g., President]

With a copy to: **[If copy is desired, insert name and address of person to whom copy should be sent.]**

or at such other address as either party may designate by Notice. Notice shall be deemed to have been given when received if delivered personally, 3 days after postmarked if sent by certified mail, or one day after deposited with an overnight courier.

6.9 **Integration.** This Agreement constitutes the sole and only agreement of the parties hereto with respect to the subject matter herein. Any and all prior agreements, promises, proposals, negotiations or representations, whether written or oral, which are not expressly set forth in this Agreement are hereby superseded and are of no force or effect.

6.10 **Amendment.** This Agreement may not be amended, modified or terminated orally, and no amendment, modification, termination or attempted waiver shall be valid unless in writing signed by the party against whom the same is sought to be enforced.

6.11 **Severability.** Should any provision of this Agreement or application thereof be held invalid, illegal or unenforceable for any reason whatsoever, then notwithstanding such invalidity, illegality or unenforceability, the remaining terms and provisions of this Agreement shall not be affected and shall continue to be valid and enforceable to the fullest extent permitted by law unless to do so would defeat the purposes of this Agreement.

6.12 **Survival.** All matters that (a) expressly survive the termination of this Agreement including without limitation the provisions of Sections 2.10, 2.11, 5.2.3, and 5.2.4, (b) relate to the termination of this Agreement, or (c) in the normal course would not occur or be effectuated until after any such termination, as well as all rights and obligations of the parties pertaining thereto, shall survive any termination and be given full force and effect notwithstanding any termination of this Agreement.

6.13 **Waiver.** The failure at any time by either party to require or demand performance of any provision of this Agreement shall not constitute a waiver by such party of such provision and shall not affect such party's full right to require performance at any later

time.

6.14 **Legislative, Regulatory or Administrative Changes**. In the event of a change in federal, state or local law, any of which could, in Health Care Provider's reasonable judgment, materially and adversely affect the manner in which either party may perform services under this Agreement, the parties shall immediately amend this Agreement to comply with the law, regulation, or policy and approximate as closely as possible the arrangements set forth in this Agreement as it existed immediately prior to the change in law, regulation or policy.

6.15 **Joint Notices**. If applicable, in this Agreement the term "covered entity" shall include all entities covered by a joint Notice of Privacy Practices.

6.16 **Business Associates That Are Covered Entitles.** In the event a Business Associate is a "covered entity" under the Privacy Standards, Business Associate may designate a "health care component of that entity, pursuant to 45 C.F.R. **§** 164.504(a) as the Business Associate for purposes of this Agreement.

6.17 **No Third Party Beneficiary.** Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties to this Agreement and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

6.18 **Headings.** The headings to the various paragraphs of this Agreement have been inserted for convenient reference only and shall not modify, define, limit or expand the provisions of this Agreement.

6.19 **Counterparts.** This Agreement may be executed in one or more counterparts, all of which shall be considered one and the same instrument.

In Witness Whereof, Health Care Provider and Business Associate have caused this instrument to be duly executed by their authorized representatives as of the Effective Date.

[Insert Full Legal Name of Health Care Provider]

_____

By: [Insert "President" or Title of Other Authorized Officer]

[Insert Full Legal Name of Business Associate]

_____

By: [Insert "President" or Title of Other Authorized Officer]

Form 2— Business Associate Addendum — Amendment to Existing Contract

BUSINESS ASSOCIATE ADDENDUM
With [Full Legal Name of Business Associate]
Effective Date: [Insert Effective Date of this Addendum]

This **Business Associate and Chain of Trust Addendum** (the "Addendum") is made as of the Effective Date set forth above, by and between [**Insert full legal name of your entity**] ('Health Care Provider") and **[Insert full legal name of Business Associate**] ("Business Associate") as a duly executed amendment to [**Insert name of original contract**] originally effective as of **[Insert effective date of original contract**] (the "Agreement").

Whereas, Health Care Provider and Business Associate desire to amend the Agreement with this Addendum in order to permit the use or disclosure of Individually Identifiable Health Information between Health Care Provider and Business Associate and to permit Business Associate as necessary to use, disclose, create and/or receive Individually Identifiable Health Information (i) on behalf of the Health Care Provider in the performance of certain functions or activities involving Individually Identifiable Health Information, or (ii) while providing certain designated services (including legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services) to or for the Health Care Provider;

Whereas, Health Care Provider and Business Associate wish to comply with the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. §1320(d)) ("HIPAA') including without limitation the Standards for Privacy of Individually Identifiable Health Information (42 C.F.R., Fart 160 and 164), the Standards for Electronic Transactions (45 C.F.R., Part 160 and 162), the Security Standards (45 C.F.R., Part 142) and Massachusetts Data Privacy laws (M.G.L 93H 201 CMR 17 and Executive Order 504) (collectively, the "Standards") promulgated or to be promulgated by the Secretary of Health and Human Services (the "Secretary").

I. **Definitions.**

The following terms, as used in this Addendum, shall have the meanings set forth below:

1.1 "**Data Aggregation"** means, with respect to Protected Health Information created or received by Business Associate in its capacity as the business associate of Health Care Provider, the combining of such Protected Health Information by Business Associate with the Protected Health Information received by Business Associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

1.2 **"Designated Record Set"** means a group of records maintained by or for Health Care Provider that is (i) the medical records and billing records about individuals maintained by or for Health Care Provider, (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for Health Care Provider to make decisions about individuals. As used in this Agreement, the term "Record" means any item, collection, or grouping of information that includes Protected Health information and is

maintained, collected, used, or disseminated by or for the Health Care Provider.

1.3 "**Electronic Media"** means the mode of electronic transmissions. It includes the internet, extranet (using internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

1.4 "**Individually Identifiable Health Information**" means information that is a subset of health information, including demographic information collected from an individual, and:

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

(b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (i) identifies the individual, or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual;

1.5 "**Protected Heath Information"** or "PHI" means Individually Identifiable Health Information that is (a) transmitted by electronic media, (b) maintained in any medium constituting Electronic Media; or (c) transmitted or maintained in any other form or medium. "Protected Health Information" excludes individually identifiable health information in: (a) education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. §1232g; (b) records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (c) employment records held by a covered entity in its role as an employer.

II. Integration of Addendum.

2.1 **Effect of this Addendum**. The terms and provisions of this Addendum shall supercede any other conflicting or inconsistent terms and provisions in the Agreement to which this Addendum is attached, including all exhibits or other attachments to, and all documents incorporated by reference in, the Agreement. Without limitation of the foregoing, any limitation or exclusion of damages provisions contained in the Agreement shall not be applicable to this Addendum.

III. Obligations of Business Associate With Respect to PHI.

3.1 Use and Disclosure of PHI. Business Associate shall use and disclose PHI only as required to satisfy its obligations under the Agreement or as required by law and shall not otherwise use or disclose any PHI. Health Care Provider shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Standards for Individually Identifiable Health Information (hereinafter, the "Privacy Standards") if done by Health Care Provider [Optional: except with respect to uses and disclosures of PHI for data aggregation or management and administrative activities of Business Associate, as provided in Sections 3.12 and 3.13 of this Addendum, respectively].

3.2 **Purposes and Limitations on Use or Disclosure of PHI.**

3.2.1 **Purposes**. Except as otherwise provided in this Addendum, Business Associate may use or disclose PHI on behalf of, or to provide services to, Health Care Provider only for the following purposes, so long such use or disclosure of PHI would not violate (a) the minimum necessary policies and procedures of Health Care Provider and (b) the Privacy Standards if used or disclosed by the Health Care Provider:
(List specific purposes for Business Associate's use or disclosure of PHI] e.g., to conduct a survey and determine the accreditation status of Health Care Provider; to provide accounting services to Provider; to conduct research services using patient medical records for XYZ purposes, etc.

3.2.2 **Property Rights in PHI**. Business Associate hereby acknowledges that, as between Business Associate and Health Care Provider, all PHI shall be and remain the sole property of Health Care Provider, including any forms of PHI developed by Business Associate in the course of fulfilling its obligations under this Agreement.

3.2.3 **Minimum Necessary**. Business Associate further represents that, to the extent Business Associate requests Health Care Provider to disclose PHI to Business Associate, such request is only for the minimum necessary PHI for the accomplishment of Business Associate's purposes.

3.2.4 **Reporting Violations**. Business Associate may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. *§* 164.502(j)(1).

3.3 **Safeguards and Security.**

3.3.1 **Safeguards.** Business Associate agrees to use all appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Addendum or as required by law.

3.3.2. **Security.** Business Associate shall establish security policies, processes and procedures in compliance with the Security Standards including without limitation administrative procedures, physical safeguards, technical security services, and technical security mechanisms, in order to protect the integrity and confidentiality of PHI exchanged electronically. Business Associate acknowledges and agrees that the legal, technical or business requirements for security of PHI may change and that, at any time during the term of this Agreement, Health Care Provider shall have the right to require Business Associate to adopt new policies, processes and procedures, or to require modifications to existing policies, processes and procedures. Health Care Provider shall communicate in writing such new or altered requirements to Business Associate, and Business Associate agrees to promptly implement such requirements. Business Associate shall supply a written copy of its security policies and procedures to Health Care Provider upon the execution of this Agreement.

3.4 **Reporting Disclosures of PHI;** Mitigation. Business Associate shall report any use or disclosure in violation of this Addendum within 2 business days of learning of such violation by Business Associate or its officers, directors, employees, contractors or other agents or by any third party to which Business Associate has disclosed PHI. Business Associate agrees to mitigate promptly at the direction of Health Care Provider any harmful effect of a use or disclosure of PHI by Business

Associate in violation of the requirements of this Addendum. Health Care Provider may, at its sole discretion, access records of Business Associate, direct an investigation of a use or disclosure by Business Associate, and determine the appropriate method of mitigation; Business Associate agrees to cooperate fully with Health Care Provider in any such investigation or mitigation.

3.5 **Employees, Subcontractors, and Agents**. Business Associate hereby represents and warrants that its employees and agents will be specifically advised of, and shall comply in all respects with, the terms and conditions of this Addendum. Business Associate shall obtain and maintain, in full force and effect, a binding contract with each of its agents including without limitation subcontractors who will have access to PHI and whose PHI is received from, or created or received by, Business Associate on behalf of the Health Care Provider. Business Associate shall further ensure that any such agent agrees in such contract to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such PHI.

3.6 **Accounting of Disclosures**.

3.6.1 **Accounting by Business Associate**. Business Associate agrees to document any disclosures of PHI made by Business Associate, as well as other information related to such disclosures, as would be required for Health Care Provider to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. §164.525. Business Associate also agrees to provide Health Care Provider, in a time and manner designated by Health Provider, information collected in accordance with this section of the Addendum, to permit Health Care Provider to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C,F.R. §164.528.

3.6.2 **Recordkeeping.** Business Associate agrees to implement an adequate recordkeeping process to enable it to comply with the requirements of this section of the Addendum.

3.7 **Privacy Practices**. Business Associate hereby acknowledges and agrees that Health Care Provider has provided it with a copy of its Notice of Privacy Practices. Business Associate agrees to comply with the practices identified in the Notice of Privacy Practices, to the extent that such practices would apply to Health Care Provider if it were performing Business Associate's functions, and will utilize as appropriate Health Care Provider's form documents. Health Care Provider hereby reserves the right to change the applicable privacy practices and related documents at any time. To the extent that such changes affect the duties and obligations of Business Associate under this Agreement, Business Associate will implement such changes within 10 days of receipt of notice of the change.

3.8 **Revocation or Modification of Consumer Permission**. Health Care Provider shall provide Business Associate with any changes in, or revocation of, permission by an individual to use or disclose PHI, if such changes affect Business Associate's permitted or required uses and disclosures.

3.9 **Consumer Restrictions on Uses and Disclosures**. Health Care Provider shall notify Business Associate of any restriction to the use or disclosure of PHI 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.

3.10 **Availability of Books and Records**. 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, Health Care Provider available to Health Care Provider, or to the Secretary, in a time and manner designated by Health Care Provider or designated by the Secretary, for purposes of the Secretary determining Health Care Provider's compliance with the Privacy Standards. The provisions of this section of the Addendum shall survive the termination of this Agreement.

3.11 **Notice of Request for PHI.** Business Associate agrees to notify Health Care Provider within 2 business days of receipt of any request, subpoena or other legal process to obtain PHI or an accounting of PHI. Health Care Provider in its discretion shall determine whether Business Associate may disclose PHI pursuant to such request, subpoena, or other legal process. Business Associate agrees to cooperate fully with Health Care Provider in any legal challenge initiated by Health Care Provider in response to such request subpoena, or other legal process. The provisions of this section shall survive the termination of this Agreement.

[Optional: Include the following section only if you intend Business Associate to be able to use PHI in its own management or administration functions.]

3.12 **Proper Management and Administration of Business Associate.**

3.12.1 **Permissible Uses.** Except as otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

3.12.2 **Permissible Disclosures**. Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are required by law, or that 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 the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

[Optional: Include the following section only if you Intend Business Associate to perform Data Aggregation functions.]

3.13 **Data Aggregation**. Except as other limited in this Agreement, Business Associate may use PHI to provide Data Aggregation services to Health Care Provider as permitted by 42 CF.R. **§** 164504(e)(2)(i)(B).

(Optional: Include the following section only if Business Associate will receive PHI in Designated Record Sets.]

3.14 **Access to Records In a Designated Record Set**. At the request of Health Care Provider and in the time and manner designated by Health Care Provider, Business Associate agrees to provide access to PHI in a Designated Record Set to Health Care Provider (and its employees and agents) or, as directed by Health Care

Provider to an individual in order to meet the requirements under 45 C.F.R. § 164.524.

(**Optional: Include the following section only if Business Associate will receive PHI in Designated Record Sets.]**

3.15 **Amendment of Records in a Designated Record Set.** At the request of Health Care Provider and in the time and manner designated by Health Care Provider, Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Health Care Provider (or its employees or agents) directs or agrees to pursuant to 45 C.F.R. § 164.526.

IV. Termination.

4.1 **Termination Upon Breach**. Any other provision of this Agreement notwithstanding, this Agreement may be terminated by Health Care Provider upon 5 business days written notice to Business Associate in the event that the Business Associate breaches any provision (including any covenant, representation, warranty, or condition) contained in Article III of this Addendum or any other such provision of this Addendum that relates to PHI and such breach is not cured within the 5 day notice period; provided, however, that in the event that termination of this Agreement is not feasible in Health Care Provider's sole discretion, Health Care Provider shall report the breach to the Secretary, notwithstanding any other provision of this Agreement to the contrary.

4.2. **Return or Destruction of PHI upon Termination**.

4.2.1 **General Provisions**. Upon termination of this Agreement, Business Associate shall either return or destroy, at the option of Health Care Provider, all PHI received from the Health Care Provider, or created or received by Business Associate on behalf of the Health Care Provider and which Business Associate still maintains in any form. Business Associate shall not retain any copies of such PHI.

4.2.2. **Alternative Arrangement**. Notwithstanding the foregoing, to the extent that the Health Care Provider agrees that it is not feasible to return or destroy such PHI, Business Associate shall provide Health Care Provider with a written acknowledgement and notification of the conditions that make return or destruction infeasible. Business Associate hereby agrees to (a) extend the protections of this Agreement to such PHI only for those purposes that make the return or destruction infeasible, (b) limit further uses and disclosures of such PHI to such purposes, and (c) extend any term or provision of this Agreement relating to PHI so that such term or condition shall survive termination of this Addendum. Thereafter, such PHI shall be used or disclosed solely for such purpose or purposes, which prevented the return or destruction of such PHI.

4.2.3 **Applicability of Provisions**. The provisions of this section of the Addendum shall apply, to the same extent that it applies to Business Associate, to PHI that is in the possession of agents of Business Associate.

4.2.4 **Health Care Provider's Right to Cure**. At the expense of Business Associate, Health Care Provider shall have the right to cure any breach of Business Associate's obligations under this Addendum. Health Care Provider shall give

Business Associate notice of its election to cure any such breach and Business Associate shall cooperate fully in the efforts by the Health Care Provider to cure Business Associate's breach. All requests for payment for such services of the Health Care Provider shall be paid within 30 days of Business Associate's receipt of the request for payment.

4.2.5 **Survival.** The provisions of this Article IV of the Addendum shall survive the termination of this Agreement.

V. Miscellaneous.

5.1 **Indemnification.** Business Associate hereby agrees to indemnify and hold Health Care Provider and its employees and agents harmless from and against any and all loss, liability, or damages, including reasonable attorneys' fees, arising out of or in any manner occasioned by a breach of any provision of this Addendum by Business Associate, or its employees or agents, without regard to any limitation or exclusion of damages provision otherwise set forth in this Agreement.

5.2 **Insurance.** Business Associate shall obtain and maintain, at its sole expense during the term of this Agreement, liability insurance on an occurrence basis with responsible insurance companies covering claims based on a violation of any of the Standards or any applicable state law or regulation concerning the privacy of patient information and claims based on its obligations pursuant to Section 5.1 of this Addendum in amount not less than **[Insert minimum amount of required coverage; for high risk business associates — suggest $1,000,000 per claim] [Optional, suggest inserting for high or medium risk business associates:**
Such insurance policy shall name Health Care Provider as an additional named insured and shall provide for 30 days prior written notice to Health Care Provider in the event of any decrease, cancellation, or non-renewal of such insurance.] A copy of such policy or a certificate evidencing the policy shall be provided to Health Care Provider upon written request.

5.3 **Injunction.** Business Associate hereby agrees that Health Care Provider will suffer irreparable damage if Business Associate breaches this Addendum and that such damages will be difficult to quantify. Business Associate hereby agrees that Health Care Provider may file an action for an injunction to enforce the terms of this Addendum against Business Associate, in addition to any other remedy Health Care provider may have.

5.4 **Authorization for Addendum**. Business Associate represents arid warrants that the execution and performance of this Addendum by Business Associate has been duly authorized by all necessary laws, resolutions and corporate action, and this Addendum constitutes the valid and enforceable obligations of the Business Associate in accordance with its terms.

5.5 **Legislative, Regulatory or Administrative Changes**. In the event of a change in federal, state or local law, any of which could, in Health Care Provider's reasonable judgment, materially and adversely affect the manner in which either party may perform services under this Addendum, the parties shall immediately amend this Addendum to comply with the law, regulation, or policy and approximate as closely as possible the arrangements set forth in this Addendum as it existed immediately prior to the change in law, regulation or policy.

5.6 **Interpretation.** Notwithstanding any other provision of this Agreement, any ambiguity in a provision of this Agreement that may require an interpretation of the Standards, shall be resolved to permit Health Care Provider to comply with the Standards including without limitation those standards relating to preemption of state laws.

In Witness Whereof, Health Care Provider and Business Associate have caused this instrument to be duly executed by their authorized representatives as of the Effective Date.

[Insert Full Legal Name of Health Care Provider]

_____

By: [Insert "President" or Title of Other Authorized Officer]

[Insert Full Legal Name of Business Associate]

_____

By: (Insert "President" or Title of Other Authorized Officer]

MENTAL HEALTH ASSOCIATION, INC.
995 Worthington Street
Springfield, MA 01109
(413) 734-5376
Fax: (413) 737-7949

ACKNOWLEDGEMENT OF REVIEW OF MHA PRIVACY POLICY AND PROCEDURES

I acknowledge that I have reviewed MHA's Privacy Policy and Procedures.

I understand that these are MHA's Privacy Policy and Procedures and that they are subject to change based on revisions to HIPAA Privacy laws and regulations.

I understand that my signature below indicates that I have reviewed and understand the above statements and have reviewed a copy of MHAs Privacy Policies and Procedures.

I understand that it is my responsibility to read and comply with these policies and procedures and any revisions to it.

_____ _____
Employee's Printed Name Position

_____
Program

_____ _____
Employees Signature Date

Revised by MHA 07/15/09

Reason for Disclosure	Limits on the Disclosure	Who can make the decision?	Does the individual need to be notified?	Accounting for Disclosure Form needed?
Public Health uses including surveillance, investigations, and interventions.	Limited to the relevant PHI required by law	Director of Programs	No	Yes
Reporting child abuse to appropriate authority	Limited to the relevant PHI required by law	Staff person mandated to report	No	Yes
Report to the FDA if required by law to report adverse events or product defects	Limited to the relevant PHI required by law	Director of Programs	Yes	Yes
Notification required by law of the exposure of an individual to a communicable disease	Limited to the relevant PHI required by law	Director of Programs or Senior Manager at Site pursuant to a standing order	Yes	Yes
Notification to an employer of work related injuries or workplace surveillance	Limited to the PHI relevant to the workplace injury	Director of Programs or Senior Manager at Site pursuant to a standing order	Individual must be notified of this practice in Privacy Notice if organization intends to notify employers	Yes

Reason for Disclosure	Limits on the Disclosure	Who can make the decision?	Does the individual need to be notified?	Accounting for Disclosure Form needed?
Disclosures required by law to report victims of abuse, neglect or domestic violence (other than child abuse)	Limited to the relevant PHI required by law	Staff person required to report	Yes, unless, the disclosing staff person believes the individual would be placed at risk or harmed by the notification or the disclosure is to be made to a personal representative who the staff person believes is responsible for the abuse, neglect, or injury and that disclosure would not be in the individual's best interest.	Yes
Disclosures to authorized agencies or law enforcement where the report is not required by law to report victims of abuse, neglect or domestic violence, or other crimes where the staff person believes there is a serious threat to the individual or other potential victims.	PHI limited to the information relevant to the suspected abuse	Director of Programs	Yes, unless, the disclosing staff person believes the individual would be placed at risk or harmed by the notification or the disclosure is to be made to a personal representative who the staff person believes is responsible for the abuse, neglect or injury and that disclosure would not be in the individual's best interest.	Yes

Reason for Disclosure	Limits on the Disclosure	Who can make the decision?	Does the individual need to be notified?	Accounting for Disclosure Form needed?
Disclosures to report victims of abuse, neglect or domestic violence, or other crimes where the individual is incapacitated and the official receiving the information states that they do not intend to use the information against the individual and non-disclosure would adversely affect the enforcement effort.	PHI limited to the information relevant to the suspected abuse.	Treating professional or direct care provider in consultation with their supervisor	Yes, as soon as is practicable unless, the disclosing staff person believes the individual would be placed at risk or harmed by the notification or the disclosure is to be made to a personal representative who the staff person believes is responsible for the abuse, neglect, or injury and that disclosure would not be in the individual's best interest.	Yes
Disclosures to agencies charged with health oversight.	PHI should be relevant to the oversight of the healthcare program, to beneficiary eligibility, or to regulatory requirements to determine compliance with program standards	Director of Programs or other staff person designated by the Privacy Officer pursuant to a standing order for routine disclosures.	No	Yes

Reason for Disclosure	Limits on the Disclosure	Who can make the decision?	Does the individual need to be notified?	Accounting for Disclosure Form needed?
Disclosures pursuant to court orders, for subpoenas, or similar processes-see Subpoena Policy	PHI must be limited to the scope of the order.	Director of Programs must be consulted as soon as is practicable. The Director of Programs will consult with the agency's attorney who will advise on the response and disclosure, if made.	Yes	Yes
Disclosures of limited amounts of PHI to law enforcement to identify a suspect, fugitive, material witness or missing person.	Limited to identifying information only	Director of Programs	Yes	Yes
Disclosures of PHI to coroners or medical examiners for identification of deceased persons or to determine cause of death.	PHI released should be limited to the information relevant to the identification or determination of death, but can, where necessary, include the disclosure of psychotherapy notes	Director of Programs	No	Yes