MASSACHUSETTS DEPARTMENT OF PUBLIC HEALTH

MA-ATR PARTICIPATING PROVIDER

CONFIDENTIALITY AGREEMENT

I. GENERAL PROVISIONS

Section 1. Provider and the Commonwealth of Massachusetts, Department of Public Health, Bureau of Substance Abuse Services ("MDPH/BSAS") executed a MA-ATR Participating Provider Agreement ("Provider Agreement") authorizing Provider to participate in the Massachusetts Access to Recovery ("MA-ATR") program funded by a grant awarded to MDPH/BSAS by the federal Substance Abuse and Mental Health Services Administration ("SAMHSA"). This Confidentiality Agreement ("Confidentiality Agreement") is incorporated by reference into the Provider Agreement.

Section 2. The terms and conditions of this Confidentiality Agreement are intended to protect the privacy and security of all confidential information that Provider may manage, receive and/or create in the performance of its duties and responsibilities under the Provider Agreement, and to ensure that Provider complies with the federal Confidentiality of Alcohol and Drug Abuse Patient Records law and regulations (42 CFR Part 2), the Fair Information Practices Act ("FIPA") (M.G.L. c. 66A), and the Massachusetts Security Breach Law (M.G.L. c. 93H) as well as all other applicable state or federal laws governing the privacy or security of any data managed, received and/or created by Provider under the Provider Agreement.

II. DEFINITIONS FOR USE IN THIS AGREEMENT

All terms used, but not otherwise defined herein, shall be construed in a manner consistent with 42 CFR Part 2, FIPA, the Security Breach Law, and as well as any other applicable state or federal laws governing the privacy or security of any data managed, received and/or created by Provider under the Provider Agreement.

"Breach" means the unauthorized use or disclosure of Confidential Information.

"Confidential Information" (CI) includes:

- Personal Data (M.G.L. c. 66A)
- Patient Identifying Information (42 CFR §2.11)
- Personal Information (MGL c. 93H)
- Other information that MDPH/BSAS determines requires protection from unauthorized access and about which Provider is notified.

Hereinafter, this Confidentiality Agreement shall use "CI" to refer to all Confidential Information, unless only a subset is appropriate.

"MA-ATR Client" means an individual referred for services or receiving services in the MA-ATR program.

"Disclose" means transfer, disseminate, release, or communicate by other means information to any outside person or entity.

"Data Subject" means an individual to whom Confidential Information refers.

"Electronic Media" means:

- *Electronic storage media* including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
- *Transmission media* used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Faxes sent directly from one fax machine to another, person-to-person telephone calls, video teleconferencing, and messages left on voice-mail are not considered transmission media. However, any faxes sent from a computer, including those made by a fax-back system, are considered transmission media.

"Holder" (referenced herein as Provider) has the meaning set forth in M.G.L. c. 66A, section 1 and means any person or entity that contracts or has an arrangement with an agency (MDPH/BSAS) whereby it holds Personal Data including Patient Identifying Information created or held under the contract.

"Patient Identifying Information (PII)" has the meaning set forth in 42 CFR §2.11 and includes the name, address, social security number, fingerprints, photograph, or similar information by which the identity of a patient can be determined with reasonable accuracy and speed either directly or by reference to other public available information. The term does not include a number assigned to a patient by a program, if that number does not consist of, or contain numbers (such as a social security, or driver's license number) which could be used to identify a patient with reasonable accuracy and speed from sources external to the program.

"*Personal Information" (PI)* has the meaning set forth in M.G.L. c. 93H, §1 and includes a person's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such person: (a) social security number, (b) driver's license number, or credit or debit card, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal Information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

"Personal Data" (PD) has the meaning set forth in M.G.L. c. 66A and includes any information in any medium concerning an individual, which because of name, identifying number, mark or description can be associated with a particular individual,

provided that the information is not contained in a public record and shall not include intelligence information, evaluative information or criminal offender record information as defined in M.G.L. c. 6, §167.

"Use" means the sharing, employment, application, utilization, examination, or analysis of information.

"MA-ATR Provider" or "Provider" means individuals, entities or organizations that has been authorized by MDPH/BSAS and with whom a Provider Agreement has been executed to provide vouchered services for clients in the MA-ATR program.

"Security Incident(s)" means any event or vulnerability caused by an internal and/or external source(s) that poses or could pose a threat to the confidentiality, integrity, or availability of Confidential Information. This includes an accidental or intentional interference with operations in an information system.

"Security Information" means non-public systems information, processes, and procedures used to protect Confidential Information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Security Information includes, without limitation, network diagrams, system schematic drawings, security policies and procedures, user account information and passwords, threat or vulnerability assessments, or any other records relating to the security of the Department's or BMC's information systems.

"WITS Voucher Management System (WITS VMS)" means the Web Infrastructure for Treatment Services ("WITS") electronic Voucher Management System ("VMS") utilized to implement MA-ATR. WITS VMS is an electronic, web-based data collection and voucher management tool.

III. OBLIGATIONS OF PROVIDER

Section 1. Purpose for Provider to Manage, Receive and/or Create Data. Provider has been authorized by MDPH/BSAS to participate in MA-ATR. Under the terms of its Provider Agreement, Provider has agreed, in accordance with all MA-ATR program requirements: (1) to furnish specified services at a defined reimbursement rate to MA-ATR Clients who may be referred to Provider; (2) to utilize WITS VMS, an electronic, internet-based system, to submit vouchers and maintain specified MA-ATR client, provider, and billing data; and (3) to maintain adequate backup documentation to demonstrate service provision by Provider to all MA-ATR clients. In the course of performing these and other duties as specified in the Provider Agreement, Provider and its employees, agents and subcontractors, if any, may manage, create, and/or receive confidential information related to MA-ATR clients.

Section 2. Restrictions on Access to Data. Provider is responsible for ensuring compliance by Provider's employees, agents and subcontractors with the guidelines or restrictions for access to CI in any medium included in this Confidentiality Agreement and in accordance with all MA-ATR program requirements. This includes but is not limited to required Confidentiality and WITS VMS training, and execution of a confidentiality pledge prior to accessing CI.

Permission to access to WITS VMS must be requested by Provider and authorized by MA-ATR, as set forth in the Provider Manual. Provider further acknowledges that it will limit access to WITS VMS to those individuals who are authorized to access WITS VMS by MA-ATR, and only to roles for which those individuals are authorized. Provider must immediately notify MA-ATR in writing when access is terminated for any staff person, for whatever reason. Provider acknowledges that it will strictly limit access to CI to those individuals who need access to CI for purposes of performing those services specified in the Provider Agreement.

Upon request, Provider and AHP shall provide MDPH/BSAS with a report listing all of Provider's authorized WITS VMS users, including their roles and authorized views/rights.

Section 3. Compliance with State and Federal Law. The Provider acknowledges that in the performance of the Provider Agreement, it may manage, receive and/or create Data including CI on behalf MDPH/BSAS. The Provider acknowledges that CI about MA-ATR clients is subject to the federal Confidentiality of Alcohol and Drug Abuse Patient Records law (42 CFR Part 2), and that PROVIDER is a Holder of CI within the meaning of FIPA, and will comply with the requirements of those laws, as well as all other applicable state or federal laws governing the privacy or security of any Data managed, received and/or created under the Provider Agreement.

Section 4. Ownership of Data. The Provider shall at all times recognize the MDPH/BSAS as sole owner of all Data including CI contained in the WITS/VMS system. As owner of the Data, the MDPH/BSAS shall at all times have complete control over the access, use, disclosure and disposition of the Data, including, as described in the Provider Agreement and this Confidentiality Agreement, use of the Data to perform the Provider Agreement, and for research and publication purposes. The Provider shall provide the MDPH/BSAS with access to or copies of any CI that it maintains pursuant to the Provider Agreement.

Section 5. Agreements by Third Parties. Provider is prohibited from engaging a subcontractor or agent under the terms of the Provider Agreement, without prior consent of MDPH/BSAS. If MDPH/BSAS authorizes the Provider in advance to engage a subcontractor or an agent, and such subcontractor or agent receives CI from or creates or receives CI on behalf of Provider or MDPH/BSAS, the Provider shall obtain and maintain a written agreement with each such agent or subcontractor. The agreement shall provide that such agent or subcontractor agrees to be bound by the same restrictions, terms and conditions that apply to the subcontractor pursuant to this Confidentiality Agreement with respect to such CI including, but not limited to, implementing reasonable safeguards to protect the CI, as specified in this Confidentiality Agreement unless otherwise approved in writing by MDPH. All provisions of the Agreement apply to all such Data, whether in the possession of the Provider or any agent or subcontractor. The Provider is responsible for using all reasonable efforts to ensure each agent's and subcontractor's compliance with all applicable provisions of this Confidentiality Agreement. Upon request, the Provider shall provide the MDPH/BSAS with a copy of the written terms between the Provider and any subcontractor or agent.

Section 4. Security: Appropriate Safeguards. The Provider agrees to implement administrative, physical and technical safeguards that reasonably and appropriately

protect the confidentiality, integrity and availability of the Data including CI. For Data that is received, maintained or transmitted in electronic format, such safeguards shall be based on ISO 27001 and 27002, or other appropriate standard as approved by MDPH/BSAS, and must include specific standards for privacy and information security established by the MDPH/BSAS and the Commonwealth. Unless otherwise approved by MDPH/BSAS in writing, appropriate safeguards for all Data shall include, at a minimum:

For All Data, however maintained:

1. Establishing written policies regarding privacy and information security, including technological and operational procedures.
2. Providing appropriate privacy and information security training for each of its employees, agents, or subcontractors who will have access to Data, including training on the provisions of this Agreement and execution of a Confidentiality Pledge (attached)
3. Requiring each of its employees, agents, or subcontractors having any access to or use of CI to comply with applicable laws and regulations relating to confidentiality, privacy, and security of the CI.

For Data maintained in hardcopy format and subject to 42 CFR Part 2:

4. Records in hardcopy format that contain CI must be maintained in a secure room, locked file cabinet, safe or other similar container when not in use, as required by 42 CFR section 2.16.

For Data received, created, maintained or transmitted in electronic format:

5. Network security oversight including the ability to detect unauthorized malware or system activity either on an individual computer or system-wide. This includes antivirus and intrusion detection.
6. Ensuring that software patches are up to date.
7. Requiring individual user accounts which are password protected and can be audited.
8. Requiring passwords for accessing CI to be periodically changed and to consist of a minimum of eight (8) characters and contain at least one each: uppercase letter, lowercase letter, and numerical character.
9. Laptop security – When a laptop maintaining CI is not in use, the CI must be secured in an encrypted volume on the hard drive. (Example: PGP Whole Disk File and Disk Encryption). Laptops must not be left unattended when powered on or in sleep mode (i.e. they must be fully powered down) unless they are secured using lockable cables or in locked offices.
10. CI stored on portable electronic media (including USB thumb drives, CDs, external hard drives and other non-volatile media) must be maintained in an encrypted file using security functions which are FIPS approved and/or NIST recommended.
11. Data Backup – The Provider shall backup Data as is necessary to ensure the integrity and availability of all information required to perform Provider's obligations under the Provider Agreement. The Provider shall provide for the security of all backup tapes and storage media.
12. To the extent feasible a separate back-up tape should be utilized for CI received or created under the Provider Agreement. If the CI is stored on backup tapes which cannot be segregated from other data maintained by the Provider due to the choice of backup media and system, the Provider shall continue to ensure the privacy and security of the CI so long as the backup media is needed. All protections pertaining to any CI covered by the Agreement shall remain in force for so long as the Provider maintains such CI.

13. Media Sanitization - Unless otherwise authorized under the terms of the Provider Agreement or other written agreement, all instances of any CI stored on electronic storage media, including thumb drives, controlled by the Provider, must be destroyed upon termination of the Agreement. CI must be destroyed so that it cannot be recovered from the electronic storage media. Acceptable methods include the use of file wiping software such as DBAN (for hard disk drives) or SDELETE (for individual files), and the degaussing and shredding of backup tapes. Electronic storage media such as floppy disks, CDs, and DVDs used to store data must be made unusable by physical destruction such as shredding.

Section 5. Non-Secure Transmissions Prohibited. The Provider agrees that it will not transmit CI over any unsecured network or over any wireless communication device.

- Transmissions of CI over the Internet are limited to secure transmission protocols approved in writing by the MDPH/BSAS.
- All CI hosted by the Provider or by the Provider's subcontractor or agent, and accessible remotely, including via the Internet, must be secured through the use of managed firewalls and other perimeter access technologies. (Example: Virtual Private Networks (VPN)). Any other method of remote access to CI must be approved in writing by the MDPH/BSAS. MDPH/BSAS has approved access to CI via WITS VMS.
- Use of WITS VMS with a secure internet connection is a secure transmission protocol approved by MDPH/BSAS.

Section 6. Reporting of Disclosures or Security Incidents. The Provider agrees that it will notify AHP no later than one (1) business day following discovery or notice of:

- any use or disclosure of CI not allowed by the Provider Agreement,
- any Security Incident involving or potentially involving Data.

The notification may be made orally. A written report shall then be filed with AHP within ten (10) calendar days of the notification.

The written report must include:

1. A complete description of the circumstances of the incident;
2. The name(s) of the person(s) assigned to review and investigate the incident;
3. A description of any CI used or disclosed during the incident;
4. The names of persons and organizations involved in the incident;
5. The actions the Provider has undertaken or will undertake to mitigate any harmful effect of the incident; and
6. A corrective action plan that includes steps the Provider has undertaken or will take to prevent future similar incidents from occurring.

Provider shall report all disclosures or security incidents to AHP:

Rebecca Starr
MA-ATR
Advocates for Human Potential
490-B Boston Post Road
Sudbury, MA 01776
Phone: 978-261-1424
Fax: 978-261-1467
E-mail: rstarr@ahp.net

Section 7. Mitigation. The Provider shall mitigate, to the extent practicable, any harmful effect that is known to the Provider of its use or disclosure of CI in violation of the Provider Agreement or any Security Incident. The Provider shall in consultation with the MDPH/BSAS and AHP take measures that the MDPH/BSAS deems appropriate to recover the CI and prevent a future breach of the confidentiality and/or security of the CI. The Provider shall report to the MDPH/BSAS Privacy Officer and AHP the results of all mitigation actions taken.

The provisions of M.G.L. c. 93H or other legal authority may require notice to be provided to Data Subjects. Any notice required to be made as a result of an unauthorized use or disclosure of CI, a Security Incident for which Provider, its agents or employees is responsible or any breach that occurred through its information system(s) shall be made in a manner approved in advance by MDPH/BSAS. The Provider shall pay the full cost of any such notification, whether notice is given by MDPH/BSAS or the Provider.

Nothing in this Section shall be deemed to waive any of MDPH/BSAS' or AHP's legal rights or remedies that arise from the Provider's unauthorized use or disclosure of the CI or security breach.

Section 8. Notice of Request for Data. The Provider agrees to notify the MDPH/BSAS and AHP of (1) any request for CI that Provider is not authorized to respond to under the terms of the Provider Agreement and this Agreement, and (2) any legal request, court order, or subpoena for CI, prior to the return date or within two (2) days of the Provider's receipt, whichever is earlier, and to cooperate with MDPH/BSAS and AHP to resist any effort, including in judicial proceedings if necessary, to obtain access to information pertaining to clients, other than as expressly provided for in 42 CFR Part 2. To the extent that the MDPH/BSAS or AHP decides to assume responsibility for challenging the validity of such requests, the Provider agrees to cooperate fully with the MDPH/BSAS or AHP in such challenge.

Section 9. Access to Personal Data (PD).

A. The Provider shall provide the data subject with access directly to the subject's PD, subject to restrictions, if the individual makes the request directly to the Provider, as shall be necessary to meet its obligation under M.G.L. c. 66A and 42 CFR Section 2.23.

B. Such access or copies shall be provided to the MDPH/BSAS and AHP or individual within five (5) days of the request.

Section 10. Availability of PD for Amendment. The Provider shall allow an individual to make requests to amend his or her PD that the Provider maintains and for which the Provider is the source, subject to restrictions. The Provider shall also make any amendment(s) to PD that it received from or created or received on behalf of the MDPH/BSAS and AHP that the MDPH/BSAS or AHP directs, in order for the MDPH/BSAS and AHP to meet its obligations under M.G.L. c. 66A. All such amendments shall be made within ten (10) days of receipt of the request from the MDPH/BSAS or AHP.

Section 11. Accounting of Disclosures. The Provider shall document PD disclosures and required information related to such disclosures, as is necessary for the MDPH/BSAS or AHP to respond to an individual's request for accounting of disclosures in accordance with MDPH/BSAS' Confidentiality Policy and Procedures, Procedure # 12, available on the MDPH/BSAS website.

The Provider agrees to provide to the MDPH/BSAS and AHP or the individual, within ten (10) days of the request an accounting of disclosures of PD. At a minimum, the Provider will provide the following information: (i) the date of the disclosure, (ii) the name of the entity or person who received the PD, and if known, the address of such entity or person, (iii) a brief description of the PD disclosed, and (iv) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure.

Section 12. Access to Records. The Provider shall make available to the MDPH/BSAS and AHP its internal practices, books, and records including policies and procedures relating to the use, disclosure and security of the Data including CI received or created pursuant to the Provider Agreement. The MDPH/BSAS or AHP shall determine the time and manner for making such material available.

Section 13. Cooperation and Access to Premises. Upon request, the Provider shall furnish the MDPH/BSAS and AHP with a description of the steps it has taken to provide for the confidentiality, integrity and availability of the Data and to prevent use or disclosure of Data not authorized by the Provider Agreement. The Provider agrees to allow authorized representatives of the MDPH/BSAS and/or AHP access to premises where the Data is kept for the purpose of inspecting physical and information security arrangements. The Provider agrees to cooperate with MDPH/BSAS and/or AHP as necessary to permit MDPH/BSAS and AHP to meet its obligations under Executive Order 504 as well as all other applicable state or federal laws governing the privacy or security of any Data received or created under the Provider Agreement.

Section 14. Custodian. The Provider shall designate the Single Point of Contact to serve as the Custodian of the Data managed, received and/or created under the Provider Agreement. The Custodian shall oversee the Provider’s compliance with this Confidentiality Agreement. In the event, the Provider changes said designee, PROVIDER shall notify the MDPH/BSAS contact person in writing at least fourteen (14) calendar days before a change in the PROVIDER’s Single Point of Contact.

V. PERMITTED USES AND DISCLOSURES BY PROVIDER

Section 1. To Perform the Provider Agreement . The Provider agrees to use or disclose CI that it manages, receives and/or creates pursuant to the Provider Agreement only as specified in the Provider Agreement and this Agreement, to satisfy its obligations thereunder. This shall include providing the Department with full access to such CI for purposes of auditing the performance of the Provider under the Provider Agreement and as the Department determines is otherwise necessary. Provider shall immediately notify MDPH/BSAS and AHP of any request to access the CI that Provider is not authorized to respond to by the terms of this Agreement.

Section 2. Minimum Necessary. The Provider agrees to take reasonable steps to limit the amount of CI used and/or disclosed pursuant to Section 1 of this subsection to the minimum necessary to achieve the purpose of the use or disclosure.

Section 3. Publications and Research. Provider agrees that it may not publish any report or make any presentation based on the CI it receives or creates pursuant to the ATR Provider Agreement without the written approval of MDPH/BSAS. Further, Provider agrees that such CI may not be used for research purposes without the prior written approval of MDPH/BSAS. Any publication or research project approved by MDPH/BSAS may, at MPDH/BSAS's sole discretion, be subject to additional requirements or restrictions, including but not limited to submission for review by an MDPH Institutional Review Board and application of MDPH/BSAS standards for release of aggregate data.

VI. PLEDGE BY AUTHORIZED USERS. Unless otherwise approved in writing by MDPH/BSAS, all of Providers' employees, agents and subcontractors, if any, authorized to access the CI must sign a Confidentiality Pledge, a copy of which is attached to this agreement, prior to accessing CI. PROVIDER shall maintain the original signed Confidentiality Pledge(s) for a minimum of seven (7) years beginning on the first day after the final payment as specified in the Provider Agreement, and shall make all pledges available to MDPH/BSAS and/or AHP for inspection immediately upon request. PROVIDER shall provide a copy of each signed Pledge to MDPH/BSAS.

VII. DURATION AND TERMINATION

Section 1. Duration. The Confidentiality Agreement is coterminous with the underlying Provider Agreement and any renewal Agreement. If the Provider Agreement is amended, the Confidentiality Agreement shall be amended as needed.

Section 2. Termination Upon Breach of Provisions Applicable to CI The MDPH/BSAS may terminate the Provider Agreement immediately upon written notice, if the MDPH/BSAS determines that the Provider has materially breached any of its obligations regarding the privacy or security of CI. Prior to terminating the Provider Agreement, the MDPH/BSAS, in its sole discretion and according to standards approved by the MDPH/BSAS, may provide an opportunity for the Provider to cure the breach or end the violation. If such an opportunity is provided, but cure is not feasible, or the Provider fails to cure the breach or end the violations within a time period set by the MDPH/BSAS, the MDPH/BSAS may terminate the Provider Agreement immediately upon written notice.

Section 3. Effect of Termination or Completion.
Upon termination or completion of the Agreement, PROVIDER agrees that any records contained in WITS VMS related to PROVIDER's services to MA-ATR clients remain the property of MDPH/BSAS. PROVIDER agrees that it shall continue to ensure the privacy and security of any CI contained in any other records related to PROVIDER's services to MA-ATR clients so long as PROVIDER retains the CI. All protections pertaining to any CI covered by this Agreement shall remain in force for so long as the Provider maintains the CI.

VIII. MISCELLANEOUS PROVISIONS

Section 1. Remedies. Nothing in this Confidentiality Agreement shall be construed to waive or limit any of the MDPH/BSAS's legal rights or remedies that may arise from the Provider's unauthorized use or disclosure of CI or security breach. The MDPH/BSAS 's exercise or non-exercise of any authority under the Confidentiality Agreement including, for example, any rights of inspection or approval of privacy or security practices or approval of subcontractors, shall not relieve the Provider of any obligations as set forth herein nor be construed as a waiver of any of the Provider's obligations, or as an acceptance of any unsatisfactory practices, or privacy or security failures by the Provider.

Section 2. Interpretation. Any ambiguity in this Confidentiality Agreement shall be resolved to permit MDPH/BSAS to comply with MGL c. 66A and 42 CFR Part 2, and any other state or federal law pertaining to the privacy or security of the Data.