

**STATE OF OREGON
MEMORANDUM OF UNDERSTANDING**

**BETWEEN
Oregon Health Authority
And
Department of Human Services**

**Information Sharing
Network and Information Systems Access**

I. PARTIES

This Memorandum of Understanding (“MOU”) constitutes an interagency agreement between the Oregon Health Authority (“OHA”) and the Department of Human Services (“DHS”), collectively called the “Agencies”.

II. PURPOSES

The purpose of this MOU is to set forth the respective commitments of the Agencies concerning network and information systems access, and information sharing between the Agencies. As a result of HB 2009 (2009), 2009 Or Laws Chapter 595, DHS and OHA were created as separate agencies but they continue to use the same network and information systems, and apply the same information sharing practices to administer their programs and responsibilities.

The administration of the network and information systems is managed by the OHA Office of Information Systems. The Office of Information Systems, including the Information Security and Privacy Office, is a shared service between DHS and OHA, as provided for in the separate Memorandum of Understanding and Delegation of Duties Regarding Shared Services between OHA and DHS (Agreement # 11-0001). This MOU shall be interpreted and applied consistently with that Memorandum of Understanding and Delegation of Duties Regarding Shared Services.

III. AUTHORITIES

Some of the authorities that apply to the DHS and OHA use of information and use of data and information systems include the following examples (a non-exclusive list).

- A. The OHA is the state Medicaid and Children’s Health Insurance Program agency, ORS 413.032, and thus responsible for the administration of these programs. The Medicaid agency is required to have certain data use agreements with Source Entities, including but not limited to the Social Security Administration and the Internal Revenue Service, for use in confirming eligibility for

medical assistance. In addition, under federal Medicaid law, the state is required to provide safeguards which restrict the use or disclosure of information concerning applicants and recipients to purposes directly connected with the administration of the public assistance laws. *See generally* 42 CFR 431. Likewise, DHS is responsible for administering various aspects of the medical assistance programs. ORS 411.320 authorizes DHS to use and disclose information about applicants for and recipients of public assistance for purposes of the administration of the public assistance laws in Oregon or as necessary to assist public assistance recipients in accessing and receiving other governmental or private nonprofit services.

- B. OHA is a covered entity, adopting a hybrid entity status, for purposes of the Health Insurance Portability and Accountability Act and the privacy rules enacted pursuant thereto. DHS and the non-health care components of OHA are business associates of OHA's health care components, authorized to use and disclose protected health information in accordance with a business associate memorandum of understanding. (Exhibit B) In addition, DHS and OHA perform other activities in accordance with federal and state law and the Privacy Rules, including but not limited to, child and adult protective services, DHS as the legal custodian of children in its care, for health oversight, in connection with law enforcement, to avert a serious threat to health or safety, and as a government program providing public benefits where the information is maintained in a single or combined data system accessible to all such government programs.
- C. HB 2009 Section 20 authorizes DHS and OHA to delegate to each other such duties, functions or powers that the authority or the department deems necessary for the efficient and effective operation of their respective functions. DHS and OHA have adopted privacy rules that encompass authorized uses and disclosures of confidential information.
- D. To the extent that the creation of the OHA and the assignment of information or those data systems and networks to OHA involves the rights and obligations of DHS legally incurred under contracts, leases and business transactions executed, entered into or begun before June 26, 2009, those rights and obligations with respect to the duties transferred to OHA by Section 19 of HB 2009, are transferred to OHA. For purposes of succession to those rights and obligations, the OHA is a continuation of DHS and not a new authority, in the manner provided in Section 24 of HB 2009. For those contracts, leases and business transactions executed, entered into or begun after June 26, 2009, DHS and OHA operate under delegations of authority pursuant to Section 20 of HB 2009.

III. DURATION, MODIFICATION AND TERMINATION

- A. **Effective Date and Duration:** The terms of this Agreement shall apply to the period of time beginning July 1, 2011, and ending on or before June 31, 2013, subject to automatic renewal in two-year terms. Automatic renewal will continue unless one Agency notifies the other Agency in writing of its intent not to renew, as provided in Paragraph C below.
- B. **Modification:** Either Agency may request changes to this MOU. Any amendments to this MOU must be in writing and signed by both parties 30 days prior to the effective date of the amendment or modification, except to the extent that the effective date of the actions that form

the basis for the amendment is otherwise established as prior to the date of the Amendment by federal or state law. In the event either Agency wishes to modify or discontinue the provision of any of the provisions of this MOU which might have a fiscal impact on one or the other party, the party desiring the change or modification will, to the extent practical, permit that change to occur at the end of the next calendar quarter, unless the date of the change is subject to a negotiated schedule.

- C. Termination:** The Agencies may terminate this MOU by mutual agreement at any time, with the termination effective on a mutually agreed upon date. Either Agency may unilaterally terminate this MOU by giving written notice to the other Agency in advance of the effective date of such termination, provided that no such termination notice shall relieve any Party of any ongoing obligation incurred under this MOU prior to such termination date. Such advance notice of termination is deemed necessary by the Parties in order to allow for the reconfiguration of services and their delivery, as well as budget and expenditure authority.

IV. INFORMATION SHARING, NETWORK AND DATA SYSTEMS ACCESS BETWEEN DHS and OHA

DHS and OHA share information because their systems are integrated into a common system or as different systems that contain information that is used and disclosed between the Agencies (shared systems), and in conjunction with the Agencies' responsibilities to operate and administer programs that serve the same or similar clients or populations. In addition, Service Level Agreements within DHS and OHA describe the information and systems management, as well as the reimbursement and cost allocation methodologies as between the Agencies.

The Agencies will use the information or data received or maintained in shared systems for the purpose of administering their programs in accordance with the legal and security requirements applicable to those programs. This MOU does not expand upon or create additional legal authority, but acknowledges that the Agencies will continue to share information and use information in the shared systems in accordance within applicable law and agreements with Source Entities that govern the use of the information.

V. OHA and DHS BUSINESS ASSOCIATE AGREEMENT

For purposes of the HIPAA Privacy and Security regulations, 45 C.F.R Parts 160 and 162, the Oregon Health Authority is a covered entity, adopting a hybrid entity status. The Department of Human Services and the non-health care components of OHA are business associates of the OHA. A Business Associate MOU between DHS and OHA is attached hereto and incorporated herein. Compliance issues related to HIPAA Privacy Rules should be directed to the Information Security and Privacy Office.

VI. DATA USE AGREEMENTS WITH SOURCE ENTITIES

The Agencies have data use agreements with other entities that provide data to DHS or OHA under specific terms and conditions (“Source Entities”). The following list provides examples, but is not intended to be an exclusive list.

- A. U.S. Social Security Administration
- B. U.S. Internal Revenue Service
- C. Oregon State Police
- D. Oregon Employment Department

Each Agency acknowledges that it must comply with all applicable terms and conditions to obtain and maintain access to information or data provided through Source Entities in accordance with separate data use or information exchange agreements with the Source Entity.

VII. OHA or DHS DATA USE AGREEMENTS WITH OTHER ENTITIES

This MOU acknowledges that the Agencies may enter into contracts or other agreements, including but not limited to data use agreements, with state agencies, local governments, tribes, contractors, nonprofit agencies. All DHS or OHA data use agreements or other contracts or agreements with other agencies, local governments, tribes, contractors, or nonprofit agencies that include provision for the use or disclosure of confidential information or access to networks or information systems must be permitted by applicable law, and include provisions that address the Access Roles and Responsibilities (Exhibit A) and, if applicable, the Business Associate MOU (Exhibit B).

VIII. DOCUMENTS

This MOU consists of this document and includes the following listed exhibits which are incorporated into this MOU:

- 1. Exhibit A: Access Roles and Responsibilities
- 2. Exhibit B: Business Associate MOU

This MOU is directly related to and should be interpreted and applied in a manner consistent with the Memorandum of Understanding and Delegation of Authority between the Department of Human Services and the Oregon Health Authority.

IX. AGREEMENT CONTACTS

DHS: Chief Operating Officer

OHA: Chief Operating Officer

Information Security and Privacy Office

X. SIGNATURES

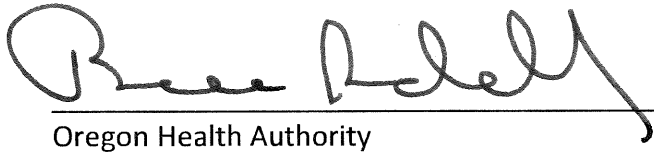
The parties to this Memorandum of Understanding represent that they are authorized to enter into this Memorandum of Understanding on behalf of the DHS and the OHA, respectively.



Department of Human Services

7.15.11

Date



Oregon Health Authority

7.15.11

Date

EXHIBIT A
ACCESS ROLES AND RESPONSIBILITIES

DHS and OHA agree that their contracts or other agreements, including but not limited to data use agreements, with state agencies, local governments, tribes, contractors, and nonprofit agencies that provide for the use of Information Assets or for access to Network and Information Systems shall include requirements to preserve the confidentiality and security of the information and systems.

Provisions in the contracts or other agreements, including but not limited to data use agreements, with state agencies, local governments, tribes, contractors, nonprofit agencies shall include the following terms and conditions, and may include additional requirements pertinent to the program and any limitations on access and disclosure required by DHS or OHA. Consequently, the provisions below are written as terms and conditions that could be incorporated into such agreements.

I. DEFINITIONS

- **“Access”** means access to any combination of Client Records, Information Assets, and Network and Information Systems.
- **“Grantor”** means DHS or OHA or “Agency”, whichever is responsible for providing access to Information Assets or Network and Information Systems, to the Receiver.
- **“Receiver”** means the entity or individual that is receiving the access or information from the Grantor pursuant to a written agreement.
- **“Client Record(s)”** means any client, applicant, or participant information regardless of the media or source, provided by the Grantor to the Receiver.
- **“User”** means any individual authorized to Access Network and Information Systems and who has an assigned unique log-on identifier.
- **“Individual User Profile (IUP)”** refers to a DHS or OHA form used to authorize a User, identify their job assignment and the required access to Network and Information System(s). It generates a unique alpha/numeric code used to access the Network and Information Systems.
- **“Network and Information System(s)”** is the computer infrastructure which provides personal communications; Client Records; regional, wide area, and local networks; and the internetworking of various types of networks.
- **“Information Asset(s)”** refers to all information provided through the Grantor, regardless of the source, which requires measures for security and privacy.
- **“Incident”** is a threat or event that compromises, damages, or causes a loss of confidential or protected information (e.g., unauthorized disclosure of information, failure to protect user ID’s, theft of computer equipment or Client Records, etc.)
- **“Source Entity”** means the entity from which the Grantor received access to or use of information or data where that access or use is limited by the terms and conditions agreed to by the Grantor in a written data use or information exchange agreement with the Source Entity.

II. CONFIDENTIALITY OF CLIENT INFORMATION

- A.** All information as to personal facts and circumstances obtained by the Receiver on a client shall be treated as privileged communications, shall be held confidential, and shall not be divulged without the written consent of the client, his or her attorney, the responsible parent of a minor child, or his or her guardian except as required by other terms of this contract or agreement. Nothing prohibits the disclosure of information in summaries, statistical, or other form, which does not identify particular individuals.
- B.** The use or disclosure of information concerning clients shall be limited to persons directly connected with the administration of the contract or agreement. Confidentiality policies shall be applied to all requests from outside sources.
- C.** Grantor, Receiver, User, and any subcontractor will share information as necessary to effectively serve OHA or DHS clients, whichever is applicable under the contract or agreement.

III. INFORMATION PRIVACY/SECURITY/ACCESS

If the Work performed under a contract or agreement requires Receiver or its subcontractor(s) to have access to or use of any Grantor computer system or other Grantor Information Asset for which Grantor (DHS or OHA) imposes security requirements, and Grantor grants Receiver or its subcontractor(s) access to such Grantor Information Assets or Network and Information Systems, Receiver shall comply and require all subcontractor(s) to which such access has been granted to comply with OAR 407-014-0300 through OAR 407-014-0320, as such rules may be revised from time to time. For purposes of this section, "Information Asset" and "Network and Information System" have the meaning set forth in OAR 407-014-0305, as such rule may be revised from time to time

IV. ACCESS CONTROL

If required for access, the Grantor agrees to promptly review requests, including forms such as the IUP, and will:

- Notify the Receiver of the approval or denial of its request for each User for whom Access has been requested;
- Provide any unique log-on identifier required for approved Access;
- Ensure that updates to approved inquiry processes and instructions are provided to Receiver.

Receiver agrees to complete any forms (such as the IUP) for each person for whom Access is requested. The original shall be kept in a secure location. The form shall be provided to the Agency upon request.

No User shall access data for any purpose other than those specifically authorized under this MOU.

Except as otherwise specified or approved by the Grantor neither the Receiver nor its Users shall modify, alter, delete, or destroy any Information Assets.

The Receiver shall immediately notify the Grantor when the Receiver, or its Users, no longer require Access whether due to changes in their individual duties or due to changes in the Receiver's programs covered under this Agreement. Receiver is responsible for assuring that Users for whom it has requested Access have a need to Access the information, and to assure that Access is removed from persons who no longer have a need for Access.

V. SECURITY

The Receiver shall have established privacy and security measures in place that meet or exceed the standards set in laws, rules, and regulations, and that are applicable to Users regarding the safeguarding, security and privacy of Client Records, all Information Assets, regardless of the media, and all Network and Information Systems.

The Receiver shall prevent any unauthorized access to the Agency's Network and Information Systems by its Users. The Receiver shall ensure the level of security and privacy protection required in accordance with this Agreement is documented in a security risk management plan. The Receiver shall make its security risk management plan available to the Grantor for review upon request.

The Receiver shall maintain security of equipment and ensure the proper handling, storage and disposal of all Information Assets accessed, obtained, or reproduced through this Agreement to prevent inadvertent destruction or loss, ensure proper disposal when the authorized use of that information ends, consistent with the record retention requirements otherwise applicable to this Agreement.

VI. USER DISCLOSURE OF INFORMATION

Wrongful use or disclosure of Information Assets by the Receiver or its Users may cause the immediate revocation of the access granted through the contract or agreement, in the sole discretion of the Grantor, or the Grantor may specify a reasonable opportunity for the Receiver to cure the unauthorized use or disclosure and end the violation, and terminate access if the Receiver does not do so within the time specified by the Grantor. Legal actions also may be taken for violations of applicable regulations and laws.

The Receiver shall immediately report any Incidents involving Access addressed in this Agreement to the Grantor. The Receiver shall comply, and shall cause its subcontractors to comply, with any requirements for identifying and addressing a privacy or security Incident. This requirement applies regardless of whether the Incident was accidental or otherwise.

The Receiver and its Users shall comply with all federal and state laws, rules, and regulations applicable to the privacy, confidentiality, or security of Access, including HIPAA. The Receiver shall have established privacy and security measures in place that meet or exceed the standards set in OAR 407-014-0300 through OAR 407-014-0320.

The use and disclosure of any Access is strictly limited to the minimum information necessary to perform the required services.

VII. SUBCONTRACTS

Receivers shall ensure all Users including subcontractors are held to the same requirements as the Receiver regarding Access, where a subcontractor requires Access in order for Receiver to perform its obligations under the contract or agreement with DHS or OHA. The Receiver is responsible for ensuring that Access is removed from subcontractors who no longer have a need for Access.

VIII. COSTS

Costs related to the acquisition of all equipment, software, data lines or connections necessary to provide Access are the sole responsibility of the Recipient, unless otherwise agreed to by written contract or agreement.

Exhibit B
BUSINESS ASSOCIATE MOU
OHA and DHS

PURPOSE

This Business Associate Memorandum of Understanding (BA MOU) is between the Oregon Health Authority (Authority or OHA) and the Department of Human Services (Department or DHS) for purposes of the HIPAA Privacy and Security regulations, 45 C.F.R Parts 160 and 162.

DEFINITIONS

“Business Associate” in this context shall mean DHS or the non-health care component of the OHA when acting as a business associate of the Authority and shall have the same meaning as the term “Business Associate” in 45 C.F.R.160.103.

“Covered Entity” means the designated health care component of the Oregon Health Authority (OHA), as “Covered Entity” is defined in 45 C.F.R.160.103.

“Protected Health Information” (PHI) and “Electronic Protected Health Information” (E PHI) shall have the same meaning as the terms “protected health information” and “electronic protected health information” in 42 C.F.R. 160.103..

“Agency” means OHA acting as a Covered Entity as to a particular activity or function.

Other terms. Other capitalized terms shall have the meaning ascribed to them elsewhere in this BA MOU, or, if no such definition is specified herein, shall have the same meaning as those terms in 45 C.F.R. 160.103 and 164.501. Any reference to the Part, Subpart or Section in the Code of Federal Regulations (“C.F.R.”) shall include any regulation issued hereunder regardless of the date of issue..

RECITALS

1. The Authority is a covered entity, as the state Medicaid and state CHIP agency, a covered health care provider, and a health care clearinghouse. The Authority has adopted a hybrid entity status, so the terms of this BA MOU describing the “Agency” apply to the functions of the Authority that are within its health care component.
2. Some non-health care components of the OHA may act as a Business Associate of the Authority in the provision of administrative services to the Authority’s health care components.
3. DHS as Business Associate of the Authority has statutorily established roles and responsibilities in the administration of programs related to children and families, seniors and people with disabilities; licensing or certifying individuals, homes, facilities, institutions and programs providing health and human services and long term care services; as well as administration of other public assistance programs. Among other things, DHS determines eligibility for the

Medicaid and CHIP program. To the maximum extent feasible, the Department administers a system of integrated eligibility and services for health and human services.

4. The purpose of this BA MOU is to assure compliance with HIPAA, and to assure cooperation and collaboration between OHA and Business Associate in performance of their respective duties. OHA and Business Associate recognize that there are many points of interconnection between their programs and the people who receive services through these programs. Consistent with the terms of this BA MOU, there are a variety of circumstances in which DHS or the non-health care component of the OHA is providing services as a business associate on behalf of the OHA.
5. OHA and DHS agree to abide by the confidentiality and information sharing requirements set forth in the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and its implementing Privacy Rule and Security Rules ("HIPAA Rules"), 45 C.F.R. Parts 160 and 164, as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 111-5 ("ARRA"), and in state and federal law to the extent not preempted by the HIPAA Rules.
6. The agencies will share all relevant information regarding health plan eligibility and services for individuals, on a continuing basis in shared data systems serving both the Authority and the Department.
7. OHA and DHS use and disclose PHI and EPHI in the performance of their obligations in accordance with applicable law and agreements.
8. HIPAA and the HIPAA Rules require that Agency, as a Covered Entity, obtain satisfactory assurances from its Business Associates that they will comply with the Business Associate requirements set forth in 45 C.F.R. 164.502(e) and 164.504(e) and as amended by the HITECH Act. Business Associate desires to provide such assurances with respect to the performance of its obligations under applicable law and agreements; and
9. Both Agency and Business Associate are committed to compliance with the standards set forth in the HIPAA Rules, and as they may be amended further from time to time, in the performance of their obligations under applicable law and agreements.

NOW, THEREFORE, in consideration of mutual and valuable consideration which the parties hereby acknowledge as received, the parties agree as follows:

MEMORANDUM OF UNDERSTANDING

The parties agree that the following terms and conditions shall apply to the performance of their obligations under applicable law and agreements.

- 1. SERVICES.** Business Associate provides certain categories of services for or on behalf of Agency, as described in the Addendum to this BA MOU, which may involve the use and disclosure of PHI and EPHI. Business Associate may make use of PHI and EPHI to perform those services consistent with this BA

MOU, the HIPAA Rules and other applicable federal or state laws or regulations. All other uses of PHI and EPHI are prohibited.

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE.

- (a) Business Associate agrees to not use or disclose PHI or EPHI other than as permitted or required by this BA MOU, or as permitted by the HIPAA Rules or as Required By Law.
- (b) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the PHI and EPHI other than as provided for by this BA MOU.
- (c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI or EPHI by Business Associate in violation of the requirements of this BA MOU.
- (d) Business Associate agrees to report to Agency, as promptly as possible, any use or disclosure of the PHI or EPHI not provided for by this BA MOU, of which it becomes aware.
- (e) Business Associate agrees to ensure that any agent that itself would be a Business Associate to whom it provides PHI or EPHI agrees to the same restrictions and conditions that apply through this BA MOU, to such Business Associate with respect to such information.
- (f) Business Associate agrees to provide access to PHI and EPHI to an Individual in order to meet the requirements under 45 C.F.R. 164.524.
- (g) Business Associate agrees to make any amendment(s) to PHI and EPHI pursuant to 45 C.F.R. 164.526 at the request of Agency or an Individual, and in the time and manner designated by Agency.
- (h) Business Associate agrees to make internal practices, books, and records, including policies and procedures and any PHI or EPHI, relating to the use and disclosure of PHI and EPHI received from, or created or received by Business Associate on behalf of Agency, available to Agency or to the Secretary, within the time and in the manner designated by Agency or the Secretary, for purposes of the Secretary determining compliance with the HIPAA Rules.
- (i) Business Associate agrees to respond to requests for disclosures of PHI and EPHI, and Business Associate agrees to document such disclosures to the extent such documentation is required to respond to a request by an Individual for an accounting of disclosures of PHI and EPHI in accordance with 45 C.F.R. 164.528.
- (j) Business Associate agrees to provide to Agency or an Individual, in time and manner to be designated by Agency, information collected in accordance with Section 2(i) of this BA MOU, to permit Agency to respond to a request by an Individual for an accounting of disclosures of PHI and EPHI in accordance with 45 C.F.R. 164.528.

(k) Business Associate agrees to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI that it creates, receives, maintains, or transmits on behalf of the Agency.

(l) In the event of Discovery of a Breach of Unsecured PHI, Business Associate shall:

- (i) Notify the Agency's Privacy Officer of such Breach. Notification shall include identification of each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been accessed, acquired or disclosed during such Breach;
- (ii) Confer with the Agency's Privacy Officer as to the preparation and issuance of an appropriate notice to each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been accessed, acquired or disclosed as a result of such Breach;
- (iii) Where the Breach involves more than 500 individuals, confer with the Agency's Privacy Officer as to the preparation and issuance of an appropriate notice to prominent media outlets within the State or as appropriate, local jurisdictions; and,
- (iv) Confer with the Agency's Privacy Officer as to the preparation and issuance of an appropriate notice to the Secretary of DHHS of Unsecured PHI that has been acquired or disclosed in a Breach. Business Associate understands that if the Breach was with respect to 500 or more individuals, such notice to the Secretary must be provided immediately, and therefore, time is of the essence in the obligation to confer with the Agency's Privacy Officer. If the Breach was with respect to less than 500 individuals, a log may be maintained of any such Breach and the log shall be provided to the Secretary annually documenting such Breaches occurring during the year involved.
- (v) Except as set forth in (vi) below, notifications required by this section are required to be made without unreasonable delay and in no case later than 60 calendar days after the Discovery of a Breach. Therefore, the notification of a Breach to the Agency's Privacy Officer shall be made as soon as possible and Business Associate shall confer with the Agency's Privacy Officer as soon as practicable thereafter, but in no event, shall notification to the Agency's Privacy Officer be later than 30 calendar days after the Discovery of a Breach. Any notice shall be provided in the manner required by the HITECH Act, sec 13402(e) and (f), Public Law 111-5, 45 C.F.R. 164.404 through 164.410 and as agreed upon by the Agency's Privacy Officer.
- (vi) Any notification required by this section may be delayed by a law enforcement official in accordance with the HITECH Act, sec 13402(g), Public Law 111-5.
- (vii) For purposes of this section, the terms "Unsecured PHI" and "Breach" shall have the meaning set forth in 45 C.F.R. 164.402. A Breach will be considered as "Discovered" in accordance with the HITECH Act, sec 13402(c), Public Law 111-5, 45 C.F.R. 164.404(a)(2).

(m) Business Associate shall comply with 45 C.F.R. 164.308, 164.310, 164.312 and 164.316 and all requirements of the HITECH Act, Public Law 111-5, that relate to security and that are made applicable to Covered Entities, as if Business Associate were a Covered Entity.

(n) Business Associate shall be responsible for any and all costs incurred in issuing any notices required by HITECH or other costs as a result of Business Associate's Breach of Unsecured PHI. If responsibility for the breach is shared between Agency and Business Associate, as between them, the two agencies will allocate costs proportionally.

3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE.

(a) General Use and Disclosure Provisions.

(1) Business Associate may use or disclose PHI and EPHI to perform functions, activities, or services for, or on behalf of, Agency as specified in this BA MOU, provided that such use or disclosure would not violate the HIPAA Rules if done by Agency or the minimum necessary policies and procedures of Agency.

(2) Agency has determined that disclosures to Business Associate are necessary and appropriate for Agency's Treatment, Payment and Health Care Operations and other purposes identified in the Addendum as allowed under the HIPAA Rules.

(3) All applicable federal and state confidentiality or privacy statutes or regulations, and related procedures, continue to apply to the uses and disclosures of information under this BA MOU, except to the extent preempted by the HIPAA Rules.

(b) Specific Use and Disclosure Provisions.

(1) Business Associate may use PHI and EPHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

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

(3) Business Associate may use PHI and EPHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. 164.502(j)(1).

(4) Business Associate may provide Data Aggregation services. Business Associate may use PHI and EPHI to provide the Data Aggregation services requested by Agency as permitted by 45 C.F.R. 164.504(e)(2)(i)(B). If Data Aggregation services are requested by Agency, Business Associate is authorized to aggregate Agency's PHI and EPHI with PHI or EPHI of other Covered Entities that the Business Associate has in its possession through its capacity as a Business Associate to such other

Covered Entities provided that the purpose of such aggregation is to provide Agency with data analysis relating to the Health Care Operations of Agency.

4. OBLIGATIONS OF AGENCY.

(a) Agency shall notify Business Associate of any limitation(s) in its notice of privacy practices of Agency in accordance with 45 C.F.R. 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI and EPHI. Agency may satisfy this obligation by providing Business Associate with Agency's most current Notice of Privacy Practices.

(b) Agency shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose PHI or EPHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI and EPHI.

(c) Agency shall notify Business Associate of any restriction to the use or disclosure of PHI or EPHI that Agency 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 or EPHI.

5. PERMISSIBLE REQUESTS BY AGENCY.

Agency shall not request Business Associate to use or disclose PHI or EPHI in any manner that would not be permissible under the HIPAA Rules if done by the Agency.

6. REMEDIES.

In addition to any other rights or remedies provided to either party in this BA MOU, upon Agency's or the Business Associate's knowledge of a pattern of activity or practice that may constitute a material breach by the other party of that party's obligations under this BA MOU, the party not in breach shall:

(1) Notify the other party of the breach and specify a reasonable opportunity in the Notice of Breach for the party in breach to cure the breach or end the violation; or

(2) If cure is not feasible, the party not in breach shall report the violation to the Secretary of Health and Human Services.

7. MISCELLANEOUS.

(a) Regulatory References. A reference in this BA MOU to a section in the Privacy Rule, Security Rule, or the HITECH Act means the section in effect as of the effective date of this BA MOU or as the Rules may be subsequently amended from time to time.

(b) Amendment; Waiver. The Parties agree to take such action as is necessary to amend this BA MOU from time to time as is necessary for Agency to comply with the requirements of HIPAA, the HIPAA Rules, and the HITECH Act. No provision hereof shall be deemed waived unless in writing, duly signed by authorized representatives of the parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any other right or remedy under this BA MOU.

(c) Survival. The respective rights and obligations of Business Associate under Section 6(c), this Section 7(c), and Section 7(e) of this BA MOU shall survive the termination of this BA MOU.

(d) Interpretation; Order of Precedence. Any ambiguity in this BA MOU shall be resolved to permit Agency to comply with the Privacy Rule, Security Rule and the HITECH Act; provided, however, that this BA MOU shall not supersede any other federal or state law or regulation governing the legal relationship of the parties, or the confidentiality of records or information, except to the extent that HIPAA preempts those laws or regulations. In the event of any conflict between the provisions of this BA MOU, and the HIPAA Rules, the HIPAA Rules shall control.

(e) No Third-Party Beneficiaries. Agency and Business Associate are the only parties to this BA MOU and are the only parties entitled to enforce its terms. Nothing in this BA MOU gives, is intended to give, or shall be construed to give or provide any benefit or right, whether directly, indirectly, or otherwise, to third persons unless such third persons are individually identified by name herein and expressly described as intended beneficiaries of the terms of this BA MOU.

(f) Successors and Assigns. The provisions of this BA MOU shall be binding upon and shall inure to the benefit of the parties hereto and their respective successors and permitted assigns, if any.

ADDENDUM TO BA MOU

This BA MOU encompasses a broad range of business associate relationships between Agency and Business Associate as established by statute, rule and agreements.

In addition to the work done by DHS as a “Business Associate” on behalf of OHA as the “Agency” under this BA MOU, DHS and OHA also perform other functions established by law.

This BA MOU does not limit the authorized uses and disclosures of PHI and EPHI consistent with federal and state laws. Examples of some of the types of authorized uses and disclosures of PHI and EPHI between OHA and DHS are listed below, and for purposes of this Exhibit B shall have the meaning as used in the HIPAA Rules.

1. Treatment
2. Payment
3. Health care operations
4. Eligibility determinations
5. Activities and functions as Required by Law
6. Public health functions
7. Abuse reporting and investigation
8. Health oversight
9. Judicial and administrative proceedings
10. Averting a serious threat to health or safety
11. Specialized government functions
12. Administration of public assistance programs