District of Columbia
Department of Behavioral Health
PRIVACY MANUAL

The Department of Behavioral Health (DBH) Privacy Manual outlines the DBH Network providers' obligations to protect the privacy of individually identifiable health information created, received or maintained as health care providers. The DBH Privacy Manual was developed to protect the interests of DBH consumers[1], and to fulfill its legal obligations under the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") and its implementing regulations at 45 Code of Federal Regulations Parts 160 and 164 ("Privacy Rules"); the D.C. Mental Health Information Act (MHIA) of 1978, as amended; the Data-Sharing and Information Coordination Amendment Act of 2010; and 42 CFR, Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records. These rules are applicable to both electronic and paper protected health information (PHI).

As a workforce member, you are obligated to follow the DBH Privacy Manual. Failure to comply with this Manual will subject DBH employees to discipline in accordance with Chapter 16 of the District Personnel Manual and applicable collective bargaining agreements. All workforce members (including DBH employees) are subject to civil and criminal penalties for violating HIPAA, the MHIA, the Data Sharing and Information Coordination Amendment Act of 2010, and 42 CFR, Part 2.

If DBH employees have questions about any use or disclosure of individually identifiable health information or about their obligations under the DBH Privacy Manual, HIPAA, MHIA, the Data Sharing and Information Coordination Amendment Act of 2010, or 42 CFR, Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records, consult the DBH Privacy Officer at 202-671-4088 or the Saint Elizabeths Hospital Assistant Privacy Officer at 202-299-5280. In addition, DBH employees can also contact the District-wide Privacy and Security Official at 202-442-9373 before they act.

Workforce members who are not DBH employees, should contact their agency Privacy Officer if they have any questions.

Privacy Manual updates will be announced by DBH. Providers are responsible for updating their manual and checking the DBH website for posted changes. When revisions are extensive, the entire manual will be revised and reissued by DBH electronically.

Sabriana Howard-Clark, DBH Privacy Officer — 12/4/13 (Date)

Matthew Caspari, DBH General Counsel — 1/10/14 (Date)

Stephen T. Baron, Director, DBH — 1/13/14 (Date)

[1] Unless specifically stated otherwise, for the purposes of this manual, consumer includes individuals receiving mental health treatment and/or substance abuse services.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

I. USE AND DISCLOSURE POLICIES AND PROCEDURES

1. Fundamental Policies on Use and Disclosure of Protected Health Information (PHI)[2].

DBH Network[3] providers are obligated to protect the privacy of a consumer's PHI. These policies and procedures are applicable to both electronic and paper PHI.

Unless specifically stated otherwise, consumer includes individuals receiving mental health treatment and/or substance abuse services.

No PHI may be disclosed unless the disclosure is in compliance with the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA); the D.C. Mental Health Information Act (MHIA) of 1978, as amended; the Data-Sharing and Information Coordination Amendment Act of 2010; 42 CFR, Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records; and this Manual.

PHI may only be disclosed by workforce members[4] who are authorized to release PHI due to their job position and responsibilities.

Upon first service encounter/intake with a consumer, Network providers will give the consumer written notice of the uses and disclosures of protected health information (PHI) within the Network (Form 1, Joint Notice of Privacy Practices).

Network providers must then ask the consumer to sign an acknowledgement of receipt of Form 1, DBH Joint Notice of Privacy Practices. Copies of each will be given to the consumer, and the original acknowledgement of receipt of Form 1 will be filed in the consumer's clinical record (See Section 7 of this manual regarding the Joint Notice of Privacy Practices).

Protected health information shall not be disclosed outside the DBH Network, absent written consent from a consumer, except as indicated in Section 3, Circumstances that Do Not Require Written Authorization to Disclose PHI.

Use and disclosure of alcohol/drug treatment and prevention records must comply with 42 CFR Part 2. See Section 4.

---

[2] PHI – Protected health information – any written, recorded, electronic (ePHI), or oral information which either (1) identifies or could be used to identify, a consumer; or (2) relates to the physical or mental health or condition of a consumer, provision of health care to a consumer, or payment for health care provided to a consumer. PHI does not include information in the records listed in subsection (2) 45 C.F.R. § 160.103.

[3] DBH Network – an organized health care arrangement consisting of DBH and participating providers (Network providers).

[4] Workforce members – every employee in the DBH Network. Workforce members include public and private employees and contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

1a) Treatment, Payment, Health Care Operations Within the DBH Network

Network providers may use and disclose PHI within the Network for the purposes of treatment, payment, and healthcare operations, but only to the minimum extent necessary. This does not apply to alcohol/drug treatment and prevention information, which requires written consent to share with another Network provider. See Section 4.

Procedure.

(1) Before making any disclosure within the Network, workforce members must confirm that:

- The intended recipient of the PHI is a participating provider in the Network, and
- The PHI to be disclosed is for treatment, payment, or health care operations of the Network.

(2) Obtain request for disclosure in writing.

See Section 2, Authorization for Use and Disclosure, for information regarding specific written authorization (DBH HIPAA Form 3).

See Part II, Section 5 for disclosure procedures.

1b) Treatment, Payment, Health Care Operations Outside the DBH Network.

Network providers may disclose PHI outside the Network only if:

(1) the consumer has executed a HIPAA/MHIA/42 CFR Part 2 compliant written authorization (e.g., DBH HIPAA Form 3) specific to the intended use or disclosure (See Section 2 on authorization for use or disclosure); or

(2) one of the conditions described in Section 3 or 4 for regarding circumstances that do not require written authorization to disclose PHI applies.

See Part II, Section 5 for disclosure procedures.

1c) Employees May Disclose PHI to Other Employees Within the Same Distinct Program to the minimum extent necessary to facilitate the delivery of services to the consumer.

1d) Consumer or Personal Representative.

For consumers in active treatment, a consumer's own PHI may be disclosed to the consumer or his/her personal representative once the treating health care professional approves disclosure. The minimum necessary requirement does not apply to consumers and their personal representatives.

See Section 2 for information regarding authorization. See also Section 8a of this manual on the consumer's right to inspect and copy his or her own PHI.

1e) Incidental Use and Disclosure.

Examples of incidental use and disclosure include phone conversations related to PHI being inadvertently overheard within the Network, information being sent to the wrong person by mistake within the Network, etc.

Workforce members should employ common sense and good judgment when using or disclosing PHI in conversation, by mail, electronic transmission or any other means, and when recording and storing PHI in any medium, to avoid any incidental use or disclosure of the PHI in connection with an otherwise permitted or required use or disclosure.

Incidental disclosures do not constitute an unauthorized disclosure (breach) as described in 1f below, unless they are believed to pose a significant risk of financial, reputational, or other harm to the affected consumer.

1f) Unauthorized Disclosure (Breach).

A breach is, generally, an impermissible use or disclosure of PHI that compromises the security or privacy of the PHI and poses a significant risk of financial, reputational, or other harm to the affected consumer.

Exceptions to the definition of breach:

(1) The covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

(2) There is an unintentional good faith acquisition, access, or use of PHI by a workforce member acting under the authority of a covered entity or business associate.

(3) An inadvertent disclosure of PHI was made by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate.

- In (2) and (3) above, the information cannot be further used or disclosed in a manner not permitted by HIPAA.

Procedure. If there is an unauthorized disclosure,

(1) Workforce members must:

(a) Notify their supervisor, who will contact the Privacy Officer/designee to determine level of risk. Agencies should presume incidents are reportable breaches unless there is a low probability that the PHI has been compromised after risk assessment.[5]

[5] Compromised means that PHI is inappropriately viewed, re-identified, re-disclosed or otherwise misused.

(b) Report any unauthorized release of a consumer's PHI as a major unusual incident (MUI) in accordance with DBH Policy on Reporting Major Unusual Incidents (MUIs) and Unusual Incidents (UIs).

(c) Document the event on Form 6, Disclosure Log, and forward to their agency Privacy Officer or designee no later than within 24 hours.

(2) The Privacy Officer or designee will send written notification of unauthorized disclosure to the affected consumer and/or inadvertent recipient as applicable (DBH HIPAA Form Letters 6.1 or 6.2).

(3) Network provider agency Privacy Officers must report any unauthorized disclosure immediately, but no longer than within five (5) business days, to the DBH Privacy Officer. The DBH Privacy Officer will inform the District–wide Privacy and Security Official. See Section 18 for penalties for breach violations.

(4) The Privacy Officer/designee or District-wide Privacy and Security Official and the agency will determine necessary actions to mitigate harm to the affected individual when consequential events occur.

(5) Unauthorized disclosures that affect 500 consumers or more must be reported by the agency to the Department of Health and Human Services (HHS).

(6) If a consumer contacts the Privacy Officer with concerns, the Privacy Officer or designee will notify the consumer or personal representative of the right to file a grievance or to pursue as a HIPAA complaint.

Unauthorized disclosures may result in disciplinary action.

Incidental disclosures as described in 1e) above, do not constitute an unauthorized disclosure.

2. Authorization for Use or Disclosure.

2a. Authorization

The signature and date of the consenting party must be on all authorizations in order for the authorization to be valid.

Network providers shall use DBH HIPAA Form 3, Authorization to Use or Disclose Protected Health Information, including mental health information, and alcohol/drug treatment and prevention information, for required written authorizations outside the Network, except for disclosures that do not require written authorization addressed in Section 3, and for authorization for research (see Section 16). Use and disclosure of alcohol/drug treatment and prevention information is more stringent. HIPAA Form 3 is required in order to share alcohol/drug treatment and prevention information within and outside the Network, except for disclosures that do not require written authorization addressed in Section 4.

The identity and authority of a person requesting or authorizing PHI must be verified and documented on the authorization/consent form. If an authorization form other than HIPAA Form 3 is received, ensure that the authorization form includes the MHIA and HIPAA required elements for a valid release of information as described in Appendix A, Standard Agency Protocols for Routine or Recurring Disclosures, and if applicable, the required elements from 42 CFR, Part 2, for alcohol/drug treatment and prevention information (See Section 4 of this manual), or consult the Privacy Officer/designee to ensure the authorization is compliant with HIPAA, MHIA, and if applicable, 42 CFR, Part 2.

DBH HIPAA Form 3 is available in English, Spanish, and Amharic. Consumers who speak primarily Spanish or Amharic should be given the appropriate translated version of HIPAA Form 3. The consumer must sign the English version to ensure the recipient will be able to follow the consumer's authorized use(s) and disclosure(s).

Consumers 18 years of age or over have the power to authorize use or disclosure of PHI, unless a guardian has been appointed, in which case only the guardian has authority to authorize use or disclosure. See Section 2a(3) below for consumers who are minors.

See Section 8 Access, and Section 10 Disclosure Accounting, for information about consumer's rights to access and disclosure accounting of PHI.

Give the consumer (or the consumer's personal representative) a copy of the signed authorization form, file the original form in the consumer's clinical record, include a copy with information to be disclosed, and provide a copy to the Privacy Officer/designee.

2a(1) Obtaining Authorization.

Whenever a workforce member seeks, or a consumer directs, use or disclosure of his/her PHI for which authorization is required as stated in Section 2a above, the workforce member must:

- Provide DBH HIPAA Form 3, Authorization to Use or Disclose Protected Health Information, including mental health information and alcohol/drug

treatment and prevention information, to the consumer or personal representative.

The consumer shall provide a valid government issued picture identification or the workforce member must verify the consumer's identity by a government official or DBH provider's oral representation.

If a personal representative is requesting information, supporting documentation is required as follows:

for a guardian – guardianship order and valid government issued picture ID.

for a representative – a power of attorney for medical decisions or notarized document granting permission by the consumer is required in addition to a valid government issued picture identification.

for a deceased consumer – court order appointing personal representative in addition to a valid government issued picture identification.

- Fill in, or have the consumer (or the consumer's personal representative) completely fill in, the authorization form.
- Have the consumer (or the consumer's personal representative) read, sign, and date the completed authorization form. An authorization that is incomplete, that you know contains false information, or that is not signed and dated is invalid.
- If the authorization form is signed by the consumer's personal representative, be sure that it shows the personal representative's name and the relationship that gives the personal representative authority to act on the consumer's behalf.
- Give the consumer (or the consumer's personal representative) a copy of the signed authorization form, file the form in the consumer's clinical record, include a copy with information to be disclosed, and provide a copy to the Privacy Officer/designee.
- Comply strictly with the terms of the authorization on use and disclosure of the PHI.

2a(2) Authorization by Personal Representatives.

For purposes of authorizing use or disclosure of, or access to, protected health information (PHI), a personal representative is a person specifically authorized by an adult consumer in writing, or by a court, as the legal representative of the consumer, or a person authorized by law to make health care decisions on behalf of the consumer.

(1) Network providers may use and disclose to a personal representative the PHI that is relevant to the scope of the representation.

(2) Network providers will furnish a personal representative the same access to and disclosure accounting for a consumer's PHI that must be provided the

consumer, provided the access or disclosure accounting involves PHI relevant to the scope of the representation.

Workforce members must consult the Privacy Officer or designee if there is any question regarding required disclosure to a personal representative.

2a(2)i. Abusive Personal Representative.

Workforce members should contact the Privacy Officer/designee or the Office of General Counsel if they have a reasonable belief that:

- the personal representative has subjected or may subject the consumer to abuse, neglect or domestic violence, and that acknowledging the personal representative could endanger the consumer; or
- in authorizing disclosure of, or requesting access to, the consumer's PHI, the personal representative is not acting in the consumer's best interest.

Workforce members must document the reasons for their suspicions in the consumer's clinical record.

Consult and follow instructions from the Privacy Officer/designee or Office of General Counsel before you disclose a consumer's PHI to a personal representative you suspect may be abusive.

See Section 3b, Required by Law, for information about reporting child and adult abusive relationships to appropriate government authority.

2a(3) Authorization for Minors.

(1) **General rule:** For minors under the age of 14, use, disclosure, or access may be authorized only by the parent or legal guardian. For minors at least age 14 but under age 18, use, disclosure, or access must be authorized by both the parent or legal guardian and the minor.

(2) **Exceptions:**

(a) A minor may authorize use of, disclosure of, or access to his or her own PHI when the minor is receiving treatment without the consent of the parent or legal guardian in accordance with D.C. Code 7-1231.14. Workforce members should direct any questions to the Privacy Officer/designee or the Office of General Counsel.

(b) an emancipated minor may authorize use of, disclosure of, or access to his or her own PHI, but must provide a copy of his/her emancipation court order.

2a(4) Personal Representatives of Deceased Consumers and Persons involved in Decedent's Care or Payment.

(1) **Rights of Executors.** Network providers will furnish an executor, administrator or other person authorized by a court, to act for the deceased consumer or the deceased consumer's estate, the same rights with respect to the

deceased consumer's PHI that must be accorded living consumers, provided the PHI is relevant to the scope of the representation.

(2) Unless contrary to a consumer's expressed preferences, Network providers may disclose to a family member, other relative, or a close personal friend of the consumer, or any other person identified by the consumer, the PHI directly relevant to such person's involvement with the consumer's care or payment related to the consumer's health care.

(3) Health care information is no longer considered PHI 50 years after death.

Workforce members should consult the Privacy Officer or designee or the Office of General Counsel if there is any question regarding the right of an executor, administrator, or other person authorized to act for a deceased consumer or the estate.

2a(5) Authorizations Received From Third Parties. If a workforce member receives an authorization from someone other than the consumer or the consumer's personal representative, take the actions below:

(1) If the authorization is on a DBH HIPAA Form 3, review Form 3 to ensure it is complete, contains no false information, and is signed and dated by the consumer or consumer's personal representative.

- If the authorization form is signed by the consumer's personal representative, *be sure that it shows the personal representative's name and the relationship that gives the personal representative authority to act on the consumer's behalf, and supporting documentation is attached.*
- If you have any questions consult the Privacy Officer or designee or the Office of General Counsel.

(2) If the authorization form is not DBH HIPAA Form 3, ensure that the authorization form includes the MHIA and HIPAA required elements for a valid release of information as described in Appendix A, and if applicable, the required elements from 42 CFR, Part 2, for alcohol/drug treatment and prevention information (See Section 4 of this manual), or consult the Privacy Officer/designee to ensure the authorization complies with HIPAA, MHIA, and if applicable, 42 CFR, Part 2. Electronic signatures may be acceptable if the sending entity is in compliance with the Electronic Signatures in Global and National Commerce Act ("E-SIGN").

Minimum Necessary. You are not required to limit the PHI used or disclosed to the minimum necessary, though you are confined to using and disclosing only the PHI identified by the authorization (See Section 5a, Minimum Necessary Determination).

2b) Psychotherapy Notes and Information Received in Confidence.

Psychotherapy notes and personal notes regarding mental health information shall not be kept as part of the consumer's clinical record, but shall be maintained, if at all, by the mental health professional who created the notes.

(1) ***Psychotherapy Notes*** are notes made by a mental health professional documenting or analyzing the contents of conversations during an individual, joint, group, or family therapy or counseling session and maintained in a location separate from the consumer's clinical record. Psychotherapy notes excludes medication prescriptions and monitoring, counseling sessions start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

(2) ***Personal Notes*** are notes of or about information received in confidence regarding a consumer which is limited to:

(a) mental health information disclosed to the mental health professional in confidence by other persons on condition that such information not be disclosed to the consumer or other persons; and

(b) the mental health professional's speculations.

No one can have access to psychotherapy process notes or personal notes regarding mental health information received in confidence except the mental health professional may disclose them as needed if the consumer sues the mental health professional for malpractice or wrongful disclosure.

2c) Authorization for Research.

Workforce members should refer all questions and requests for use and disclosures of PHI related to research to their Privacy Officer or designee (also see Section 16-Research).

2d) Authorization Expiration or Revocation.

Expiration. The consumer may authorize disclosure for any period of time up to three-hundred and sixty-five (365) days, except in cases where the consumer authorized the disclosure in order to obtain life insurance or non-cancellable or guaranteed renewable health insurance, in which case the authorization can be up to two (2) years from the date of the policy.

Revocation. A consumer may revoke authorization at any time. The effective date of the revocation is the date the provider who was authorized to release the information receives the written revocation. The revocation must be in writing.

Procedure.

If a consumer (or the consumer's personal representative) who has given authorization indicates a desire to revoke it, the workforce member must document the revocation as follows:

- Verify identify of consumer (and the identity and authority of a personal representative) revoking authorization (see Section 6, Identity and Authority Verification).
- Have the consumer (or the consumer's personal representative) fill in the date and sign the revocation section on the original authorization, HIPAA Form 3.

- If the consumer brings in a separate written and signed revocation, document the date received on the original HIPAA Form 3 and attach the revocation.
- Give the consumer (or the personal representative) a copy.
- Re-file the original HIPAA Form 3, with the revocation section filled out, in the consumer's clinical record.
- Give a copy to the privacy officer/designee.
- The Privacy Officer shall notify the business associate(s) of any revocation by the individual to the use or disclosure of their PHI, to the extent that the revocation may affect the use or disclosure of PHI by the business associate.

3. Circumstances That Do Not Require Written Authorization to Disclose PHI.

The circumstances under which protected health information (PHI) may be used or disclosed without authorization for public health, public interest, public benefit, and law enforcement activities are very narrow, specific circumstances as described in the subsections below. Refer to Section 4 for specific requirements for use and disclosure of alcohol/drug treatment and prevention records by certified alcohol/drug treatment and prevention providers.

Procedure.

(1) Workforce members must consult the Privacy Officer or designee before disclosing PHI in response to any request, demand or legal process to use or disclose PHI that is not accompanied by the written authorization of the consumer or the consumer's personal representative, except in emergency situations that meet the description in subsections 3a, 3b(1)(a), and 3b(1)(c).

(2) **Minimum Necessary.** Determine the minimum necessary PHI (see Section 5a of this manual) to use or disclose in all of the circumstances described in this Section except when required by law (subsection 3b).

(3) **Use Form 6** – Disclosure Log, to log each disclosure outlined in this Section **except** in emergency situations and for disclosures to law enforcement officials when required by law. See Section 10 for guidance on disclosure accounting. Ensure the original Form 6 is filed in the consumer's clinical record, and provide a copy to the Privacy Officer or designee.

3a) Public Health and Safety Threats. (D.C. Official Code 7-1203.03)

The minimum necessary PHI may be disclosed on an emergency basis to one or more of the following if a mental health professional reasonably believes that the disclosure is necessary to initiate emergency psychiatric hospitalization of the consumer pursuant to D.C. Code § 21-521 or to otherwise protect the consumer or another person from a substantial risk of imminent and serious physical injury:

(1) a consumer's spouse, parent, legal guardian;

(2) a duly accredited officer or agent of the District of Columbia in charge of public health;

(3) the Department of Behavorial Health;

(4) an individual or entity that is licensed or certified by, or has entered into an agreement with, DBH to provide behavioral health services or supports;

(5) the District of Columbia Pretrial Services Agency;

(6) the Court Services and Offender Supervision Agency;

(7) a court exercising jurisdiction over the consumer as a result of a pending criminal proceeding;

(8) emergency medical personnel (e.g., EMTs and emergency room doctors);

(9) an officer authorized to make arrests in the District of Columbia; or

(10) an intended victim.

Any disclosure of mental health information under this section shall be limited to the minimum necessary to initiate or seek emergency hospitalization of the consumer under D.C. Code 21-521 or to otherwise protect the consumer or another individual from a substantial risk of imminent and serious physical injury.

3b) Required by Law.

(1) PHI may be disclosed to the extent required by law to meet the compulsory reporting provisions of District or federal law that attempt to promote human health and safety. The following situations are examples of compulsory reporting laws:

(a) **Child Abuse:** If you are CFSA employee, agent or contractor, or a physician, psychologist, medical examiner, dentist, chiropractor, registered nurse, licensed practical nurse, person involved in the care and treatment of consumers, law-enforcement officer, humane officer of any agency charged with the enforcement of animal cruelty laws, school official, teacher, athletic coach, Department of Parks and Recreation employee, public housing resident manger, social service worker, day care worker, human trafficking counselor, domestic violence counselor, or mental health professional, you are required by law to report or have a report made immediately if you know or have reasonable cause to suspect that a child known to you in your official capacity has been, or is in immediate danger of being, mentally or physically abused or neglected. If you have reasonable cause to suspect child abuse or neglect, you must immediately notify your supervisor. This notification does not relieve you of your individual duty under the law to ensure that a report is made immediately to the Child and Family Services Agency's 24-hour reporting line at 202 671-SAFE (7233). (D.C. Official Code §4-1321.02) Also see DBH Policy 630.2, Reporting Abuse or Neglect of Children.

(b) **Child Fatalities:** Pursuant to D.C. Official Code §4-1371.12, every physician, psychologist, medical examiner, dentist, chiropractor, qualified mental retardation professional, registered nurse, licensed practical nurse, person involved in the care and treatment of patients, health professional licensed pursuant to Chapter 12 of Title 3, law-enforcement officer, school official, teacher, social service worker, day care worker, mental health professional, funeral director, undertaker, and embalmer are also required by law to report to the Registrar of Vital Records as soon as practicable, but in any event within five business days, the death of a child who died in the District of Columbia, or a ward of the District of Columbia who died outside of the District.

We must also provide the Child Fatality Review Committee with immediate access to any and all records they request regarding a deceased child.

(c) **Adult Abuse:** The law requires that conservators, court-appointed mental retardation advocate, guardian, health-care administrator, licensed health professional, police officer, humane officer of any agency charged with the enforcement of animal cruelty laws, bank manager, financial manager, or social worker immediately report to Adult Protective Services (202-541-3950) if, in their official capacity, they have substantial cause to believe that an adult is in need of protective services due to abuse or neglect or exploitation by another. (D.C. Official Code §7-1903(a)(1)). Also see DBH Policy 630.3 Reporting Elder and Vulnerable Adult Abuse and Neglect.

(2) **Health and human services information:** In accordance with the D.C. Data Sharing and Information Coordination Amendment Act of 2010, Network providers may use and disclose health and human services information to a network provider or certain D.C. Health and Human Service Agencies or their service provider[6] without consent for the following purposes:

(a) To establish eligibility for or determine the amount and type of: treatment, services, benefits, support, or assistance;

(b) To coordinate: treatment, benefits, services, support or assistance;

(c) To conduct oversight activities for: management, financial and other audits, program evaluations, planning, investigations, examinations, inspections, quality reviews, licensure, disciplinary actions; or civil, administrative, or criminal proceedings or actions; or

(d) To conduct research related to treatment, benefits, services, supports, and assistance, provided that: the information is not disclosed in a manner permitting identity to be reasonably inferred, and the agency receiving information will be treated via HIPAA.

To comply with HIPAA, Network providers may share with those D.C. Health and Human Services Agencies, and their respective service providers, that are covered entities under HIPAA, including the Department of Human Services, Child and Family Services Agency, Department of Health, and the Department of Health Care Finance.

All requests for information must be in writing and describe the purpose for the information and establish/verify a connection to the consumer. As with any disclosure in the absence of a release, the scope of the disclosure must be limited to the minimum extent necessary to accomplish the purpose of the disclosure. Network providers must respond to requests within 48 hours, not unreasonably deny a request, and within 5 business days of the date of the request, supply the requested information to the extent such request was approved. Finally, nothing in this section authorizes the disclosure of psychotherapy notes without a signed release.

Examples of establishing eligibility for services and coordination of treatment:

Consumer A receives services from DBH and CFSA. CFSA requests that DBH participate in a treatment planning conference to coordinate Consumer's A treatment and services. Consumer A has not signed an authorization for release of information. Under the Mental Health Information Act, D.C. Official Code 7-1203.02(3), DBH is authorized to disclose Consumer A's PHI to CFSA during the treatment planning conference to the extent necessary to effectively coordinate treatment. The PHI disclosures must be limited to the minimum amount necessary to coordinate treatment and the disclosures must be documented in Consumer A's records.

[6] Service provider – means an entity that provides health or human services to District residents pursuant to a contract, grant, or other similar agreement with an agency.

Consumer B receives services from DBH. Consumer B applies for public benefits through DHS. As part of the application process, DHS requests information from DBH concerning the Consumer's enrollment status and current treatment plan. Consumer B has not signed an authorization for release of information. After evaluating the particular request, DBH determined that the information requested by DHS was too broad and went beyond the minimum necessary to establish Consumer B's eligibility for the particular public benefit that Consumer B applied for. As a result, DBH verified that Consumer B was a DBH Consumer but did not disclose the current treatment plan in the absence of an authorization.

Consumer C receives services from DBH. After receiving complaints from Consumer C's neighbors, MPD calls the DBH Access Helpline to request information on whether Consumer C is a DBH consumer and, if, so, the name of Consumer C's provider. MPD is not a health and human services agency. In the absence of an emergency, DBH is not authorized to disclose.

3c) Health Oversight Activities. PHI may be disclosed to District agencies or their service providers that provide health and human services to District residents pursuant to a contract or agreement with a District agency for the purposes of health oversight activities.

PHI may be disclosed to qualified personnel to carry out management audits, financial audits, quality improvement activities, or program evaluation, complaint investigations or compliance enforcement or review of a mental health professional or mental health facility, provided that such personnel have demonstrated and provided assurances, in writing, of their ability to comply with all applicable federal and District privacy laws, including the requirement that they avoid revealing, directly or indirectly, the identity of any consumer whose information they receive.

Contact the Privacy Officer/designee or Office of General Counsel to ensure personnel are qualified and entitled to information prior to any disclosure being made. The Privacy Officer or designee will certify that assurances are adequate.

3d) Judicial and Administrative Proceedings.

(1) The minimum necessary PHI may be disclosed (1) by a mental health professional in order to initiate or seek civil commitment proceedings; and (2) in a civil or administrative proceeding in which the consumer, the consumer's representative, or in the case of a deceased person, any one claiming or defending through the consumer who makes the consumer's mental condition an element of the claim or defense.

In addition, PHI may be disclosed in response to a judicial or administrative order, provided we disclose only the expressly ordered information, and it may be disclosed in response to a subpoena or other process, but only if either the consumer has executed an authorization or a judge has authorized the disclosure in writing. See also DBH Policy on Subpoenas for DBH Employees and Mental Health Information.

(2) Disclosures in Court Actions. In addition to mental health information that is disclosed when a defendant's competence or mental health is at issue or when otherwise authorized by law, in a criminal proceeding, the court may order the disclosure or re-disclosure of a defendant or offender's mental health information when and only to the extent necessary to monitor the defendant or offender's compliance with a condition of pretrial release, probation, parole, supervised release, or diversion agreement that the defendant or offender obtain or comply with mental health treatment ordered by a court or the U.S. Parole Commission.

(3) In litigation for the collection of fees, no PHI other than administrative information shall be disclosed, except to the extent necessary (a) to respond to a motion of the consumer or the consumer's representative for greater specificity; or (b) to dispute a defense or counterclaim. "Administrative information" consists of the consumer's name, age, sex, address, identifying number or numbers, dates and character of sessions [individual or group], and fees.

(4) Any disclosure or re-disclosure of mental health information ordered under this section shall be limited to the minimum necessary to monitor the consumer's compliance and the court's order shall specify the information that may be disclosed or re-disclosed.

Refer any request for court related disclosures to the Privacy Officer or designee or the Office of General Counsel.

3e) Law Enforcement. Disclosures to correctional institutions or law enforcement officials when a person is in custody.

(1) A mental health professional or mental health facility may disclose to a correctional institution or a law enforcement official having lawful custody of a consumer, mental health information about the consumer to facilitate the delivery of mental health services and mental health supports to the consumer.

(2) Any disclosure of mental health information under this section shall be limited to the minimum necessary to facilitate the delivery of mental health services and mental health supports.

3f) Research. Refer questions and requests for use and disclosure of PHI related to research to the Privacy Officer or designee or the Office of General Counsel. Also see Section 16, Research.

3g) Protection and Advocacy Organization ("ULS"). We are required by federal law to grant access in most instances to records requested by the designated organization responsible for protection and advocacy ("P&A") in the District of Columbia for persons with mental illness (currently University Legal Services, or "ULS"). ULS is authorized to investigate allegations of abuse and neglect and pursue legal remedies on behalf of individual consumers. In certain narrow circumstances, ULS is entitled to have access to a consumer's records even if they do not have written authorization from the consumer or the consumer's personal representative. If you receive a request for disclosure of PHI from a representative of ULS, or any other organization representing itself as the P&A organization, and the requestor does not present an authorization signed by the consumer or the consumer's personal

representative in accordance with Section 2, consult the Privacy Officer or the Office of General Counsel before disclosing or granting access to the protected information.

4. Use and Disclosure of Alcohol/Drug Treatment and Prevention Records by DBH Certified Alcohol/Drug Treatment and Prevention Providers

4a. **Records related to an individual's treatment for substance abuse are strictly confidential.** That confidentiality is protected by federal law and regulations as well as District of Columbia law and regulations.

Disclosure of information that identifies an individual (directly or indirectly) as having a current or past drug or alcohol problem (or participating in a drug/alcohol treatment and prevention program) is generally prohibited (including to other providers within the Network) unless the individual consents in writing or other exceptions in 42 CFR Part 2 apply.

4b. **Records of the identity, diagnosis, prognosis, or treatment of any consumer[7] may be disclosed only under the following conditions:**

1. With written authorization from the:

   - Consumer or, for minors, his or her parent or legal guardian;
   - For consumers adjudicated incompetent, the person authorized under District law to act on his or her behalf;
   - For deceased consumers, the consumer's executor, administrator or personal representative.

2. Without patient authorization only under the following circumstances:

   Emergency situations:
   - To report suspected child abuse or neglect. (42 CFR §2.12(c)(6))
   - In a medical emergency when there is a threat to health of individual that requires immediate medical attention. *Once disclosed due to medical emergency, information loses its protection and may be redisclosed as permitted by HIPAA.* (42 CFR §2.51)(a)
   - To report a crime or threat of a crime occurring on the provider's premises or directed against the provider's staff. (42 CFR §2.12(c)(5))

   Other Exceptions:
   - For health oversight activities such as evaluating programs and audits.
   - In response to a court order in accordance with 42 CFR Part 2. Prior to disclosure, DBH employees will consult with the DBH Office of General Counsel to ensure the court order is in accordance with 42 CFR Part 2 as applicable. Network providers should consult with legal counsel as appropriate. A subpoena alone is not sufficient for disclosure. A subpoena must be accompanied by written consent (DBH HIPAA Form 3 or a written consent that contains comparable required elements for a valid release of information).
   - For research purposes, such as research related to the development of better treatments, provided the research study meets certain privacy requirements.
   - Pursuant to a qualified service organization or business associate agreement.

[7] The term consumer includes individuals receiving mental health treatment and/or substance abuse services.

Procedure.

(1) Workforce members must consult the Privacy Officer or designee before disclosing PHI in response to any request, demand or legal process to use or disclose PHI that is not accompanied by the written authorization of the consumer or the consumer's personal representative, except in emergency situations.

(2) **Minimum Necessary.** Determine the minimum necessary PHI (see Section 5a of this manual) to use or disclose in all of the circumstances described in this Section.

(3) **Use Form 6** – Disclosure Log, to log each disclosure outlined in this Section except in emergency situations. See Section 10 for guidance on disclosure accounting. Ensure the original Form 6 is filed in the consumer's clinical record, and provide a copy to the Privacy Officer or designee.

4c. Individuals requesting a DBH certified alcohol/drug treatment and prevention provider to disclose alcohol/drug treatment and prevention information must submit a completed DBH HIPAA Form 3, Authorization to Use or Disclose PHI. If a different written consent form is submitted, it must contain comparable required elements for a valid release of information, or request that the individual fill out the DBH HIPAA Form 3, to ensure all required elements are included.

Required elements for release of information from 42 CFR Part 2 must be in writing and include:

- Name/general designation of program making disclosure,
- Name of individual/entity receiving disclosure,
- Name of consumer who is subject of disclosure,
- Purpose/need for disclosure,
- Description of how much and what kind of info will be disclosed,
- Consumer's right to revoke consent, and any exceptions,
- Date/event/condition on which consent expires,
- Consumer's signature,
- Date signed, and
- HIPAA: Program's ability to condition treatment, payment, enrollment, or eligibility on the consent.

4d. When responding to a request for PHI, the agency privacy officer/designee must verify the identity and authority of the requesting individual. Documents appropriate to verify identity include:

- Personal identification (government issued photo ID) *Attach a copy.*
- Government official or Department of Behavioral Health provider's oral representation. *State what you were told and why your reliance on it was reasonable in the circumstances.*
- If form is mailed in, the signature on the form must be notarized or the person who is providing consent must have his/her signature notarized or attach a copy of his/her government issued ID.

4e. The requesting individual must also present evidence of an appropriate relationship with the consumer with respect to healthcare. Documents appropriate to verify authority include:

- Identification as parent, guardian, or acting in loco parentis with respect to minors,
- Executor or administrator with respect to a deceased individual or estate,
- Power of attorney or other legal authority to act on behalf of an individual with respect to health care, or
- Other evidence of an appropriate relationship.

4f. Redisclosure. Any person who receives alcohol/drug treatment and prevention information from a certified alcohol/drug treatment and prevention provider, shall not redisclose the alcohol and drug treatment and prevention information unless by written consent or as otherwise authorized by 42 CFR Part 2.

4g. Any disclosure of alcohol/drug treatment and prevention information must be accompanied by the following written statement:

> "This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR 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 CFR 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 patient. (42 CFR § 2.32)"

4h. Unless superseded by 42 CFR Part 2, DBH certified Alcohol/Drug Treatment and Prevention Providers shall follow other DBH privacy processes as described in the DBH Privacy Manual except for Section 3.

II. STANDARD PROCEDURES

5. Disclosure Procedures.

5a) Minimum Necessary Determination.

As a workforce member, you will access and use only the minimum necessary protected health information (PHI) reasonably needed to perform your duties for the Network. You must not attempt to access or use more than the minimum necessary PHI needed to perform your duties.

If you cannot apply the criteria in Section 1, 2, or 3 below, you must apply the criteria in Section 4 below to determine whether the disclosure or request is for the minimum necessary PHI to accomplish the purpose. If you have questions, consult the Privacy Officer or designee.

(1) Minimum Necessary Not Applicable When:

- The recipient of the requested PHI is either the consumer who is the subject of the information or the consumer's personal representative.
- The consumer or the consumer's personal representative authorized the disclosure pursuant to Section 2, Authorization for Use or Disclosure.
- The disclosure is required by the Department of Health and Human Services (HHS), District of Columbia Office of Inspector General (OIG) or the Department of Behavioral Health (DBH) for complaint investigation or compliance enforcement or review.
- The disclosure is required by law.
- The disclosure is required for compliance with the HIPAA Administrative Simplification Rules.
- The disclosure involves de-identified information.

(2) Reliance on Requestor.

Workforce members can rely on the request to be for the minimum necessary because the request is from one of the following and such reliance is reasonable under the circumstances:

- A covered entity or a business associate of a covered entity.
- A professional who is a member of our workforce or is our business associate providing professional services to us, and who represents that the requested information is the minimum necessary.
- A public official who represents that the requested information is the minimum necessary.

- A researcher who presents appropriate documentation or representation for the research.

(3) Routine or Recurring Disclosures or Requests.

The disclosure or request is routine or recurring.

(4) Standard Criteria for Individual Determination.

The disclosure or request must meet our criteria for minimum necessary as determined by following the actions below:

- Ascertain the purpose of the disclosure or request.
- Identify the particular PHI to be disclosed or requested.
- Determine whether the particular PHI is a reasonably related to the purpose for the disclosure or request.
- Determine what PHI can reasonably be expected to satisfy the purpose of the disclosure or request. Disclose no more than the minimum necessary PHI as applicable.
- Determine whether the purpose of the disclosure or request can be accomplished with de-identified health information. If it can, then we may disclose or request only de-identified health information.

5b) **Routine or Recurring Disclosures and Requests.**

Follow the DBH standard protocols in Appendix A. Network Providers may use Appendix A as a guide and adjust as needed to address specific routine or recurring protocols specific to their organization.

5c) **Non–Routine and Non–Recurring Disclosures or Requests.** Do not disclose or request PHI for a non–routine and non–recurring purpose until you review the situation on an individual basis against our standard criteria to ensure that only the minimum necessary PHI for the purpose is disclosed or requested. Refer to Section 5a (4) above, Standard Criteria for Individual Determination. If you question whether a particular disclosure or request should be subject to an individual review (rather than treated as routine or recurring) or how to conduct the individual review based on our criteria, consult your Privacy Officer or designee.

5d) **Entire Clinical Record.** When an entire clinical record is to be used, disclosed or requested, you must:

(1) Determine on an individual basis whether the situation justifies using, disclosing or requesting an entire clinical record as the minimum necessary PHI for the purpose. Do not redisclose PHI unless specifically stated on the authorization.

(2) Whenever the entire clinical record is requested by individuals outside the Network, the Privacy Officer/medical records officer must approve the release of the entire record.

5e) **Redisclosure**. You cannot redisclose PHI without written authorization, except as required by law. Also see Appendix A.

5f) **Right to Disclosure Accounting.** See Section 10 for disclosure accounting and disclosure log requirements.

6. Identity and Authority Verification.

You must verify the identity and authority of any person or entity who is requesting or authorizing disclosure of protected health information (PHI) before you disclose PHI. Use HIPAA Form 3, "Verification of Identity of Consumer or Personal Representative Providing Consent" section to document the verification.

You must also verify the identity and authority of the person who is receiving the PHI before releasing any information.

Procedure.

Verification of Identity and Authority.

(1) For written authorization, obtain appropriate identification and, if the person is not the consumer who is the subject of the PHI sought, evidence of authority. See section 2a(1) above, Obtaining Authorization, for examples of identification and authority.

(2) For emergency situations, workforce members must take reasonable steps to identify and record identification and organization of person requesting information.

If you question whether you have obtained sufficient verification, consult your Privacy Officer or designee before you make any disclosure.

III. CONSUMERS' INFORMATION RIGHTS

7. Joint Notice of Privacy Practices.

Within the DC Behavioral Health Network, participating providers will maintain a Joint Notice of Privacy Practices, FORM 1, to give consumers written notice of the uses and disclosures of protected health information (PHI) that the Network may make, and of the consumers' rights and the Network's legal duties with respect to PHI. The Network will always use and disclose PHI consistent with our Notice. We will furnish our Notice to any person who requests one.

Only the Joint Notice of Privacy Practices that has been approved by the DBH Privacy Officer may be distributed to Network providers. The DBH Privacy Officer will ensure the Notice and any revisions to it are consistent with DBH policy, District policy, MHIA, HIPAA, 42 CFR Part 2, and any other applicable local and federal laws.

Procedure.

(1) **Distribution of the Network's Joint Notice of Privacy Practices.** The Department of Behavioral Health (DBH) will ensure that the Notice is electronically available on the DBH website as part of the DBH Privacy Manual (1000.3).

Participating Network providers will disseminate the Joint Notice of Privacy Practices to each new consumer during enrollment.

The Notice must also be posted in a clear and prominent place at each of the service delivery sites so that consumers seeking service may reasonably be expected to be able to read the Notice.

Network providers will notify consumers that the terms of the Notice have been changed by posting it at service delivery sites. DBH will also post the changed Notice on the DBH website.

A paper copy of the Notice must be provided to the consumer, upon request.

(2) **Acknowledgment for the Joint Notice of Privacy Practices.** Providers must obtain the consumer's signature on the acknowledgement of receipt page of the Joint Notice of Privacy Practices DBH HIPAA Form 1. The acknowledgement of receipt page of the Notice shall be filed in the consumer's clinical record.

If the consumer fails or refuses to sign the Notice we will document our effort to obtain it on the acknowledgement of receipt page of the Notice and file it in the consumer's clinical record.

Consumers who do not write can be directed to sign using an X with a witness to verify and note they observed this activity by the consumer. For consumers who do not read, the Notice can be read to them.

8. Access.

8a) Right to Inspect and Copy.

(1) We will respond to all requests for access to protected health information (PHI) within thirty (30) days of receipt of the written request, including providing the requesting party either with photocopies or the opportunity to inspect and photocopy the requested information as long as we or our business associates maintain it in designated record sets (See subsection 8d below on designated record sets).

(2) If the consumer is in active treatment, the treating health care professional at the Network provider will be contacted before responding to the request to access PHI. The licensed health care professional, responsible for the diagnosis or treatment of the consumer, shall have the opportunity to discuss the PHI with the consumer at the time of such inspection, if applicable.

Procedure.

(1) **Access Request.** As soon as a request for access to PHI is received, the workforce member will complete, or have the consumer complete, FORM 7– Access Request, and transmit FORM 7 to the Privacy Officer or designee by the next business day.

(2) **Access Response.** The Privacy Officer will coordinate with the Network provider as required. Based on the recommendation of a licensed health care professional whether to grant or deny a consumer access to PHI, the Privacy Officer or designee will process each access request as follows:

- Coordinate and track the processing of the access request on Form 7a, Access Processing Form;
- Inform the consumer whether access is granted or denied in writing (with a statement of the reasons for denial, and the procedures for complaining to us and to Department of Health and Human Services about a denial); and
- If access is granted, inform the consumer of any applicable fees to ensure that the consumer still wants access, copies, or mailing;

  Access Fees. We may charge a reasonable, cost–based fee for copying and mailing of the requested PHI, see Appendix B, DBH Clinical Record Request Fee Schedule. We may not charge for providing access to or retrieving the requested PHI, and a consumer is entitled to one (1) free accounting disclosure in any 12 month period. The Privacy Officer or designee will determine applicable charges and inform the consumer in advance so that the consumer may elect to withdraw or modify the request to reduce or avoid the fee. See the schedule of fees in Appendix B at the back of this manual. Access fees will not apply to indigent (unable to pay) consumers.

- Notify affected business associates in writing to retrieve records; and
- Have the completed FORM 7 and applicable notification letters (DBH HIPAA Letters 7.1, Grant of Access to Records, 7.1a, Direction to Retrieve

Records, or 7.2, Denial of Access to Records) included in the consumer's clinical record.

(3) **Access Granted.** We will permit a consumer who has been granted access the opportunity to inspect and obtain a copy of his or her PHI at a time and place, or by mail, as may be mutually agreed by the consumer and the Privacy Officer or designee. We will provide the consumer a summary or explanation of the requested PHI, upon the consumer's request.

If instructed by the Privacy Officer or designee to supervise a grant of access, you will furnish the requested PHI in the form or format that the consumer requests. If the PHI is not readily producible and maintained electronically, provide a readable electronic copy. Consult with the Privacy Officer or designee if it appears that the form or format the consumer requested is not feasible. If the Privacy Officer or designee informs you that there is a fee, you must collect the fee before providing the access service to which the fee applies. All collected fees must be submitted to the responsible cashier's office in accordance with internal guidelines established by their organization (see Appendix B, Schedule of Fees).

- In the event that the consumer or consumer representative questions the accuracy or completeness of the consumer's record of behavioral health information, he/she may submit a DBH-HIPAA Form 9, Amendment Request, to the health care provider to amend the record. See Section 9, Right to Amend.

8b) Protected Health Information We May Withhold.

If a licensed health care professional denies access pursuant to one of the following reasons, the licensed health care professional must document the reasons for the denial in the consumer's clinical record and provide documentation for the reasons for denial to the Privacy Officer or designee.

(1) **Denial of Access without Right of Review.**

- Access is not allowed to the following information:
  - Psychotherapy notes;
  - Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
  - PHI maintained by a covered entity subject to the Clinical Laboratory Amendments Act of 1988, 42 USC §263a, or 42 USC §493.3(a)(2).

- Access may be denied if:
  - Granting access to information received in confidence would be reasonably likely to reveal the source of the information (see Section 2b of this manual).
  - The health care provider is a correctional institution or acting under the direction of a correctional institution and obtaining a copy would jeopardize the health, safety, security, custody or

rehabilitation of the individual, other inmates, or other persons at the correctional facility.

- The individual is participating in a course of research that includes treatment, provided that the individual agreed to the denial of access when agreeing to participation in the research, and was informed that the right to access would be reinstated upon completion of the research.

(2) **Denial of Access to PHI.** A licensed health care professional may limit the disclosure of portions of a consumer's record of PHI to the consumer if:

- A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
- The PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
- The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

The licensed health care professional that denied access due to these safety concerns must document the denial in the clinical record.

(3) **When PHI access is denied,** the Privacy Officer or designee will:

(a) Inform the consumer of the denial in writing and of the right of review and the procedures for exercising that right. See DBH HIPAA Letter 7.2, Denial of Access to Records and Section 8c below.

(b) The health care provider may designate a reviewing licensed health care professional who is not directly involved in the denial, who shall be permitted to review the consumer's record of PHI as a result of the denial of access within a reasonable time and report to the Privacy Officer or designee whether the denial is justified.

8c) Review of Access Denial.

The reviewing licensed health care professional shall be in substantially the same or greater professional class as the licensed health care professional who initially recommended the limited disclosure.

(1) The reviewing licensed health care professional shall instruct the health care provider to permit the consumer to inspect and duplicate those portions of the consumer's record of PHI which, in his or her judgment, do not pose a substantial risk of imminent psychological impairment to the consumer or pose a substantial risk of imminent and serious physical injury to the consumer or another person.

In the event that the reviewing licensed health care professional allows the consumer to inspect and duplicate additional portions of the consumer's record of PHI, the licensed health care professional primarily responsible for the diagnosis or treatment of the consumer shall be notified by the Privacy Officer and shall have the opportunity to discuss the information with the consumer at the time of transmittal, examination or duplication of information.

8d) Identification of Designated Record Sets.

Each Network Provider must identify in writing each designated record set it maintains or that is maintained on their behalf by their business associates, and the titles of persons or offices responsible for receiving and processing access requests.

Designated Record Set means a group of records maintained by or for DBH, other Network providers, and business associates that is: the medical and billing records relating to a consumer maintained by or for a health care provider; the enrollment, payment, claims adjudication, and case or medical management systems maintained by or for a health plan, or; used, in whole or part, by or for a covered entity to make decisions about consumers.

Procedure:

Each department must document on FORM 8-Designated Personnel and Record Sets the persons or job categories responsible for receiving and processing access requests in the agency, and the designated record sets maintained by the agency or for the agencies by business associates.

Send the completed FORM 8 to the medical records manager with a copy to the DBH Privacy Officer to maintain in the Privacy Officer file.

Promptly update FORM 8 upon any change in designated personnel or record sets.

9 Amendment.

9a) Right to Amend.

A consumer may request to amend his or her PHI for as long as it is maintained in designated record sets. An amendment request may be denied only as specified in subsection 9b below.

In the event that the consumer or consumer representative questions the accuracy or completeness of the consumer's record of protected health information, he/she may submit a DBH-HIPAA Form 9, Amendment Request, to amend the record.

Procedure.

(1) **Amendment Requests.**

A response to the consumer regarding the consumer's request to amend must be provided to the consumer within sixty (60) days of its receipt. Consequently, the workforce member who received the amendment request must transmit the amendment request to the agency Privacy Officer or designee by the next business day.

The workforce member must complete, or have the consumer complete, Form 9, Amendment Request, and promptly transmit the form to the agency Privacy Officer or designee.

(2) **Amendment Response.** The Privacy Officer will coordinate with the Network provider as required. Based on the recommendation of the responsible health care professional to grant or deny a consumer's amendment request, the Privacy Officer or designee will process each amendment request as follows:

- Coordinate and track the processing of the amendment request on Form 9a, Amendment Request Processing Form.
- Respond in writing to a consumer's request to amend within sixty (60) days. The initial response may be written notice that a thirty (30) day extension of the sixty (60) day response period will be taken for reasons stated in the notice including the date that we will provide our response. Inform the consumer in writing whether the amendment will be granted or denied.
- If amendment is granted:

  Prepare Amendment Letter 9.1, Grant of Amendment to Records, and provide to the consumer.

  Amend the consumer's clinical record in accordance with the proposed amendment; or include the proposed amendment as part of the consumer's clinical record.

  Inform the organization head or designee, and business associates with affected designated record sets on Letter 9.1a, Notification to Amend Records, that they are required to amend the record within five (5) business days. Furnish the amendatory material to append or link to the affected records so that thereafter each disclosure is only of the properly amended records.

Have the completed Form 9 Amendment Request and copies of amendment letters (9.1 Grant of Amendment to Records and 9.1a Notification to Amend Records) filed in the consumer's clinical record.

Maintain Form 9a, Amendment Request Processing Form with your Privacy Officer records.

Forms and sample letters are located at the back of this manual.

- If amendment is denied:

  Prepare Letter 9.2, Denial of Amendment to Records, and provide to the consumer.

  Inform heads of agencies and business associates with affected designated record sets, on Letter 9.2a, Notification of Record Amendment Denial, and furnish the required materials to append or link to the affected records so that they can be included with future disclosures of those records.

  Have the completed FORM 9 and copies of notification letters (Letter 9.2 and 9.2a) filed in the consumer's clinical record.

  Maintain Form 9a, Amendment Request Processing Form with your Privacy Officer records.

  Forms and letters are located at the back of this manual.

9b) Basis for Denying Amendment Request.

We may decline to amend PHI if:

- We did not create the information (unless the consumer provides a reasonable basis to believe the originator is no longer available to act on the request).
- The information to be amended is not part of a designated record set maintained by us or by a business associate on our behalf.
- The information is accurate and complete.
- The information to be amended may be withheld from the right of access. See Section 8(b), Protected Health Information We May Withhold.

9c) Amending on Another Covered Entity's Notice.

Network Providers will amend PHI in our designated record sets upon receipt of notice from a covered entity that the PHI has been amended.

Procedure.

Workforce members must promptly inform the Privacy Officer or designee upon receipt of a notice from a covered entity that PHI has been amended, and send the notice to the Privacy Officer or designee. The Privacy Officer or designee will:

- Determine if we hold the affected PHI in our designated record sets or in designated record sets held on our behalf by business associates, and
- Notify and instruct the heads of agencies and our business associates with affected designated record sets (in writing) to amend the affected records within five (5) business days, so that thereafter each disclosure is only of the properly amended records.

10. Disclosure Accounting.

10a) Right to Disclosure Accounting.

Upon a consumer's request, Network providers will provide an accounting of each disclosure that is made of the consumer's PHI for up to six (6) years prior to the request.

Essentially, Network providers are obligated to account for disclosures we make without the consumer's authorization (See Section 3 and 4) unless they are exempt from accounting as described below, or that violate HIPAA, and unauthorized disclosures (breach) as described in Section 1f.

Network providers do not have to account for disclosures that are exempt from accounting as follows:

- Anything disclosed prior to six (6) years from the date of the request for disclosure.
- Disclosures made within the Network for treatment, payment, or health care operations (see Section 1a of this manual).
- Disclosures made to the consumer or the consumer's personal representative.
- Disclosures made pursuant to authorization.
- Disclosures made as part of a limited data set.
- Disclosures of de-identified PHI.
- Disclosures to business associates.
- Disclosures that are for national security or intelligence purposes.
- Disclosures made to correctional institutions or other law enforcement officials having lawful custody over an individual.
- Disclosures made on an emergency basis pursuant to D.C. Official Code 7-1203.03 (also see Section 3a of this manual), and pursuant to 42 CFR §2.51(a), 42 CFR §2.12(c)(6), and 42 CFR §2.12(c)(5), (also see Section 4 of this manual).

Procedure.

(1) Network providers are obligated to respond to the consumer's request for a disclosure accounting within sixty (60) days of its receipt. Workforce members must:

- Complete, or have the consumer complete, FORM 10, Request for Accounting of Disclosures of PHI.
- Promptly transmit FORM 10 to the Privacy Officer or designee by the next business day.

(2) **Accounting Fees**. Network providers may not charge for a consumer's first accounting in any 12 month period. Network providers may charge a reasonable, cost–based fee for other accountings within that same 12-month period. Refer to the standard schedule of fees in Appendix B at the back of this manual.

(3) **Accounting Response**. The Privacy Officer or designee will process a consumer's request for disclosure accounting as follows:

- Determine if there are fees for the consumer's accounting request. If there are, notify the consumer in advance of the fee so that the consumer may elect to withdraw or modify the accounting request to reduce or avoid the fee.
- Coordinate and track the processing of the accounting request on FORM 10a, Disclosure Accounting Processing Form. Direct any necessary agencies and business associates in writing to furnish the disclosure data needed to comply with the accounting request within five (5) business days on DBH HIPAA Letter 10.1.
- Respond in writing to the consumer's accounting request on DBH-HIPAA Letter 10.2 within sixty (60) days. (The initial response may be written notice that a thirty (30) day extension of the sixty (60) day response period will be taken for reasons stated in the notice including the date that we will provide our response.) Inform the consumer, in writing, that the disclosure accounting is available or to transmit the disclosure accounting to the consumer.
- Have the completed FORM 10 and copies of applicable notification letters (e.g., DBH HIPAA Letter 10.1 and 10.2) filed in the consumer's clinical record.
- The Privacy Officer will maintain FORM 10a, Disclosure Accounting Processing Form, with Privacy Officer records.
- Sample notification letters are located at the back of this manual.

10b) Accounting Information.

Network providers must track and record, and require our business associates to track and record accountable disclosures, and make the tracking information available to the Privacy Officer or designee on request, so that they comply with requirement to make disclosure accounting to consumers on request. If there is a question whether a particular disclosure needs to be recorded, consult the Privacy Officer or designee.

Procedure.

(1) **Use Form 6** – Disclosure Log, to document each accountable disclosure.

(2) The completed Form 6 must be filed in the consumer's clinical record. A copy must be filed in the Privacy Officer or designee file, and maintained for at least six (6) years to support disclosures.

10c) Accounting Content for Disclosure. The following information for each accountable disclosure of PHI (including disclosures to or by our business associates) must be recorded and maintained for at least six (6) years to support our disclosure accounting obligations.

- The disclosure date;

- The name and, if known, address of each person or entity that received the disclosure;
- A description of the PHI disclosed; and
- A statement of the purpose of the disclosure, or a copy of any written request for the disclosure from HHS or another government agency or organization to which the PHI was disclosed under one of the subsections in Section 3.

10d) **Accounting Content for Repetitive Disclosures.** For multiple disclosures for a single compliance review or complaint investigation, or to another government agency or organization to which we disclosed PHI pursuant to a single provision in Section 3, we need provide the consumer only:

- The frequency, or number of the repetitive disclosures during the accounting period; and
- The date of the last disclosure during the accounting period.

11. Restriction Requests.

11a) Requests.

(1) A consumer may request that a Network provider restrict certain uses or disclosures of his or her protected health information (PHI) for treatment, payment, health care operations, and/or in situations when disclosure requires giving the consumer an opportunity to agree or object. Network providers do not have to agree to a consumer's restriction, but if they do, they must follow the restriction.

(2) Network providers must agree to a restriction of PHI if the consumer (or a person on the consumer's behalf) pays for item or service in full out of pocket.

(3) In general, a Network provider will support consumer choice unless it is clinically contraindicated as determined by the clinical team. The Network provider will comply, and notify their business associates to comply with any such agreement it makes, except in a medical/psychiatric emergency.

Procedure.

(1) **Requests.**

If a consumer makes a request to restrict disclosure of his or her PHI, responsible clinical staff should:

- Complete FORM 11–Restriction Request, and have the consumer sign the form.
- Consult with clinical team to ensure that request is not clinically contraindicated.
- Check the consumer's clinical record to see if there is an advance directive regarding restriction of information (see DBH Policy 515.1, Advance Directives).
- Revise the consumer's advance directive (if appropriate) with the consumer.
- Transmit FORM 11 to the agency Privacy Officer or designee by the next business day.

(2) **Response.** Based on the conclusion of the clinical team, the Privacy Officer or designee will process each restriction request as follows:

- Coordinate and track the processing of the restriction request on FORM 11a, Restriction Request Processing Form.
- Notify the consumer, in writing, that we agree to or we deny the restriction, on DBH-HIPAA Letter 11.1, Agreement to Restriction Request; or DBH-HIPAA Letter 11.2, Denial of Restriction Request.
- If we agree to the restriction, notify affected agencies and business associates, in writing, of their obligation to comply with the restriction, on DBH-HIPAA Letter 11.1a, Notification of Restriction of PHI (to business associates).
- Have the completed FORM 11 and appropriate notification letters included in the consumer's clinical record (11.1, Agreement to

Restriction Request; 11.1a, Notification of Restriction of PHI to Business Associates; or 11.2, Denial of Restriction).

- Sample restriction form and notification letters mentioned above are located at the back of this manual.

11b) Medical/Psychiatric Emergency Exception.

Restricted PHI may be used or disclosed to a health care provider, if the information is needed in a medical/psychiatric emergency for treatment of the consumer who is the subject of our restriction agreement. Restricted PHI may also be disclosed to a person authorized to write an FD-12 if the mental health professional reasonably believes that such disclosure is necessary to initiate or seek emergency hospitalization.

Procedure.

When requested to disclose restricted PHI for treatment in a medical/psychiatric emergency, workforce members must:

- Exercise professional judgment to determine that a medical/psychiatric emergency exists that justifies using or disclosing the restricted PHI.
- Ask the recipient of PHI to not further use or disclose the restricted PHI.
- Document the basis for your determination in the clinical record (whether it resulted in using, disclosing or withholding the restricted PHI), and notify the Privacy Officer or designee in writing.

11c) Unenforceable Restrictions.

We will neither agree to, nor comply with, a restriction request for disclosures that does not require written authorization (See Section 3 and 4).

Procedure.

(1) If you receive a restriction request that is unenforceable, notify the Privacy Officer or designee who will inform the consumer in writing that the restriction agreement cannot prevent uses or disclosures.

(2) You must promptly notify the Privacy Officer or designee if you receive a request for restricted PHI from HHS or another government agency or organization. Follow the direction of the Privacy Officer or designee regarding the response to such request.

11d) Restriction Termination.

Based on a consumer's request, or the clinician's determination that the restriction is clinically contraindicated, we may terminate the restrictions for disclosure of PHI.

Procedure.

In order to terminate a restriction agreement, responsible clinical staff must complete FORM 11b, Termination of Restriction, have consumer sign as appropriate, and submit the form to the Privacy Officer or designee by the next business day. The Privacy Officer or designee will do the following:

- Notify the consumer, in writing, that we are terminating the restriction agreement as requested, on DBH-HIPAA Letter 11.3, Notice of Termination of Restriction Agreement (to consumer).
- Inform the agency head, or designee, of affected agencies and business associates, in writing, of the termination of the restriction agreement on DBH-HIPAA Letter 11.3a, Notice of Termination of Restriction (to business associates).
- Have the completed FORM 11b, Termination of Restriction, and applicable notification letters (DBH HIPAA-Letter 11.3 and 11.3a) included in the consumer's clinical record.
- Sample termination of restriction form and notification letters mentioned above are located at the back of this manual.

Responsible clinical staff. As a result of a restriction termination, responsible clinical staff will follow DBH Policy 515.1, Advance Directives, and have consumer's preferences updated on the appropriate form and filed in the clinical record.

12. Confidential Communication.

A consumer may request confidential communications (that is, the use of alternative means or alternative locations to communicate protected health information (PHI) to the consumer), if the request is reasonable and in writing.

Procedure.

(1) **Requests.**

(a) If a workforce member receives a consumer's request to use alternative means or locations when communicating PHI to the consumer, complete or have the consumer complete FORM 12-Confidential Communication Request, then promptly transmit FORM 12 to the Privacy Officer or designee by the next business day.

(b) Consult with the Privacy Officer or designee before making a communication of PHI, if there is any question whether that communication should be treated as a confidential communication.

(c) You are not allowed to require a consumer to explain the basis for requesting confidential communications, nor may you question the validity of the consumer's representation that confidential communication is needed because of danger to the consumer.

(2) **Response.** Only the Privacy Officer or designee may approve a request for confidential communication of PHI. The Privacy Officer or designee will process each confidential communication request as follows:

(a) Coordinate and track the processing of the confidential communication request on Form 12a, Confidential Communication Request Processing Form.

(b) Respond to the consumer by means and location appropriate to the confidential communication request. The Privacy Officer or designee will inform the consumer whether we will accommodate the confidential communication request on DBH-HIPAA Letter 12.1, Accommodation of Confidential Communication Request.

(c) If we accommodate the confidential communication request, notify affected agencies and business associates in writing of their obligation to comply with the confidential communication request on DBH-HIPAA Letter 12.1a, Notification of Confidential Communication Requirement (to business associates).

(d) If the consumer's request does not contain all of the information requested on the form, inform the consumer on DBH HIPAA Letter 12.2, Denial of Confidential Communication Request, that we will not accommodate the confidential communication request without additional, specified information. The response must use the means or location appropriate to the confidential communication request.

(e) Have the completed FORM 12 and applicable notification letters mentioned above included in the consumer's clinical record.

Sample notification form and letters mentioned above are located at the back of this manual.

IV. RELATIONSHIP POLICIES AND PROCEDURES

SECTION 13 RESERVED

14. Business Associates.

Business Associate (BA) means a person or entity who, on behalf of DBH or a Network provider (covered entity), and other than in the capacity of a workforce member: creates, receives, maintains or transmits PHI, or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services which involves the disclosure of individually identifiable PHI from the covered entity, or from another business associate of the covered entity, to the person or entity.

Business Associates shall ensure its employees, agents, subcontractors, representatives and members of its workforce are appropriately informed of the terms of the HIPAA compliance clause between the business associate and the covered entity.

14a) Uses and Disclosures with Business Associates.

Protected health information (PHI) may not be disclosed to a business associate, and a business associate may not be allowed to create or receive PHI on behalf of DBH or a Network provider unless the HIPAA Privacy Compliance Clause (see Appendix C) is a part of the agreement with the business associate.

The Contracting Officer is responsible for completing the contracting process and ensuring that any agreements that involve the use of PHI have the appropriate HIPAA Privacy Compliance Clause included in the agreement.

14b) Business Associate Compliance.

Business Associates and their subcontractors are officially liable for certain requirements of the HIPAA Privacy and Security Rules, whether a formal agreement exists or not. The Omnibus Rule now gives the Office of Civil Rights (OCR) the latitude to directly investigate business associates for breaches, and they will shortly be incorporated into the random audit program.

If a business associate has materially breached its agreement, the business associate will be required to promptly report the breach to the covered entity (DBH or the Network provider as applicable) and cure the breach. If the business associate fails to cure the breach, the agreement should be terminated. The breach should be reported to the agency and DBH Privacy Officer, DBH Office of Accountability, and if the breach affects 500 consumers or more, to the Department of Health and Human Services. Also see Section 1f, regarding unauthorized disclosures (breach).

The business associate must report to the covered entity (DBH or the Network provider), in writing, any use or disclosure of PHI not permitted or required by the HIPAA Privacy Compliance Clause (attached to business agreements) to the agency and DBH Privacy Officer immediately, but not longer than five (5) days, once the business associate becomes aware of or suspects such unauthorized use or disclosure. The business associate also has the option of reporting an unauthorized use or disclosure to the District-wide Privacy and Security Official.

In the event the business associate imposes sanctions against any member of its workforce, agents and subcontractors for violation of the provisions of HIPAA or other applicable federal or state privacy laws, the business associate shall inform

the agency and DBH Privacy Officer of the imposition of sanctions. The business associate also has the option of reporting the sanctions to the District-wide Privacy and Security Official.

Procedure.

Workforce members must immediately notify and cooperate with the DBH Privacy Officer, DBH Office of Accountability, and District-wide Privacy and Security Official, if they learn that a business associate may have breached or violated their agreement. The workforce member must follow the instructions of the DBH Privacy Officer, DBH Office of Accountability, and District-wide Privacy and Security Official, regarding investigation and resolution of the suspected breach or violation.

14c) Network Provider Agency as Business Associate.

If a Network provider agency serves as a business associate of another covered entity, the Network provider will enter into a business associate agreement with that covered entity.

The Network provider agency must ensure that the HIPAA Privacy Clause (see Appendix C) is a part of the agreement, and fully comply with the terms of each agreement it enters into as a business associate of a covered entity.

Procedure.

(1) The agency must obtain the approval of the agency Privacy Officer for any business associate agreement the agency may be asked to accept before it may undertake any business associate function or activity involving PHI, to ensure that the HIPAA Privacy Clause is a part of the agreement.

(2) The agency must immediately notify the agency and DBH Privacy Officer and cooperate with the privacy officers if the agency learns that it may have breached or violated a business associate agreement with a covered entity. The agency must follow the instructions of the agency and DBH Privacy Officer regarding investigation and resolution of the suspected breach or violation. Failure to comply with a business associate agreement obligations can expose the agency to sanctions under HIPAA and the MHIA.

14d) Documentation.

The agency Privacy Officer will maintain a list of organizations and persons with which the agency has a business associate agreement. The Privacy Officer will also retain all documentation the agency creates or receives regarding compliance of business associates or the agency's compliance as a business associate of covered entities, until six (6) years after the later of their creation or last effective date.

14e) Termination of Contract.

Except as provided in the paragraph below, upon termination of the contract, for any reason, the business associate shall return in a mutually agreed upon format or confidentially destroy all PHI received from the covered entity, or created or received by the business associate on behalf of the covered entity within five (5) business days of termination. This provision shall apply to PHI that is in the possession of all subcontractors, agents, or workforce members of the business associate. The business associate shall retain no copies of PHI in any form.

In the event that the business associate determines that returning or destroying the PHI is infeasible, the business associate shall provide to the covered entity notification of the conditions that make the return or confidential destruction infeasible.

Upon determination by the agency Privacy Officer that the return or confidential destruction of the PHI is infeasible, the business associate shall extend the protections of the HIPAA Compliance Clause of the business agreement to such PHI and limit further uses and disclosures of such PHI for so long as the business associate maintains such PHI.

The obligations outlined in the section of the business agreement, entitled: Obligations and Activities of Business Associate, will remain in force to the extent applicable.

V. OTHER TYPES OF DISCLOSURES

15a) Limited Data Set and Data Use Agreement.

Network providers are permitted to use and disclose protected health information (PHI) included in a limited data set without obtaining an authorization or documentation of a waiver or an alteration of authorization. Limited data sets may be used and disclosed if you have a data use agreement for health care operations, or for research, public health, public interest, or public benefit (see Section 3). Network providers may use and disclose a limited data set for research activities conducted by itself, another covered entity, or a researcher who is not a covered entity if the disclosing Network provider and the limited data set recipient enter into a data use agreement. Because limited data sets may contain identifiable information, they are still PHI and protected by HIPAA and the MHIA.

Limited Data Set – Refers to PHI that excludes 16 categories of direct identifiers and may be used or disclosed, for purposes of research, public health, or health care operations, without obtaining either an individual's authorization or a waiver or an alteration of authorization for its use and disclosure, with a data use agreement.

Data Use Agreement – An agreement into which the Network provider enters with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and how it will be protected.

A limited data set is described as health information that excludes certain, listed direct identifiers (see below) but that may include city; state; ZIP Code; elements of date; and other numbers, characteristics, or codes not listed as direct identifiers. The direct identifiers listed in HIPAA's limited data set provisions apply both to information about the individual and to information about the individual's relatives, employers, or household members. The following identifiers must be removed from health information if the data are to qualify as a limited data set:

1. Names.
2. Postal address information, other than town or city, state, and ZIP Code.
3. Telephone numbers.
4. Fax numbers.
5. Electronic mail addresses.
6. Social security numbers.
7. Medical record numbers.
8. Health plan beneficiary numbers.
9. Account numbers.
10. Certificate/license numbers.
11. Vehicle identifiers and serial numbers, including license plate numbers.
12. Device identifiers and serial numbers.
13. Web universal resource locators (URLs).
14. Internet protocol (IP) address numbers.
15. Biometric identifiers, including fingerprints and voiceprints.
16. Full-face photographic images and any comparable images.

A data use agreement is the means by which Network providers obtain satisfactory assurances that the recipient of the limited data set will use or disclose the PHI in the data set only for specified purposes. Even if the person requesting a limited data set from a Network provider is an employee or otherwise a member of the Network provider's workforce, a written data use agreement meeting HIPAA requirements must be in place between the Network provider and the limited data set recipient.

HIPAA requires that a data use agreement contain the following provisions:

(1) Specific permitted uses and disclosures of the limited data set by the recipient consistent with the purpose for which it was disclosed. A data use agreement cannot authorize the recipient to use or further disclose the information in a way that would violate HIPAA.

(2) Identify who is permitted to use or receive the limited data set.

(3) Stipulations that the recipient will:

- Not use or disclose the information other than permitted by the agreement or otherwise required by law.
- Use appropriate safeguards to prevent the use or disclosure of the information, except as provided for in the agreement, and require the recipient to report to the Network provider any uses or disclosures in violation of the agreement of which the recipient becomes aware.
- Hold any agent of the recipient (including subcontractors) to the standards, restrictions, and conditions stated in the data use agreement with respect to the information.
- Not identify the information or contact the individuals.

If a covered entity is the recipient of a limited data set and violates the data use agreement, it is deemed to have violated HIPAA. If the Network provider providing the limited data set knows of a pattern of activity or practice by the recipient that constitutes a material breach or violation of the data use agreement, the Network provider must take reasonable steps to correct the inappropriate activity or practice. If the steps are not successful, the Network provider must discontinue disclosure of PHI to the recipient and notify HHS.

There are specific PHI uses and disclosures that a Network provider is permitted to make for research without an authorization, a waiver or an alteration of authorization, or a data use agreement. These limited activities are the use or disclosure of PHI preparatory to research and the use or disclosure of PHI pertaining to decedents for research.

Any questions from DBH workforce members regarding limited data sets should be directed to the agency Privacy Officer or designee.

FORM 13-Data Use Agreement contains the mandatory terms that HIPAA requires to be in a data use agreement.

Procedure. Workforce members will submit the proposed data use agreement to the Privacy Officer or designee for approval. If approved, obtain the signature of the intended recipient on the data use agreement before disclosing the limited

data set. Send the original, signed data use agreement to the Privacy Officer or designee. Retain a copy for your agency's file.

Minimum Necessary. A limited data set may contain only the minimum necessary PHI for the purpose for which the limited data set is to be used or disclosed.

15b) De–Identified Health Information.

(1) De–Identified Health Information is PHI that has been stripped of all identifiers and cannot be used alone or in combination with any other information to identify the consumer.

De–identified health information may be disclosed without restriction. Network providers will treat as PHI any key or other means to re–identify health information that has been de-identified. Minimum necessary does not apply to de-identified PHI.

Network providers may also disclose PHI to a business associate to create de–identified health information (See Section 14 for information on business associates).

The following identifiers must be removed from health information if the data are to qualify as de-identified health information:

1. Names;

2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

   (a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

   (b) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

4. Telephone numbers;

5. Fax numbers;

6. Electronic mail addresses;

7. Social security numbers;

8. Medical record numbers;

9. Health plan beneficiary numbers;

10. Account numbers;

11. Certificate/license numbers;

12. Vehicle identifiers and serial numbers, including license plate numbers;

13. Device identifiers and serial numbers;

14. Web Universal Resource Locators (URLs);

15. Internet Protocol (IP) address numbers;

16. Biometric identifiers, including finger and voice prints;

17. Full face photographic images and any comparable images; and

18. Any other unique identifying number, characteristic, or code, except that DBH or a Network provider may assign a code or other means of record identification to allow information de-identified to be re-identified by DBH or a Network provider, provided that:

(a) Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(b) Security. DBH or a Network provider does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

Procedure.

(1) All identifiers of the consumer and the consumer's relatives, household members, and employers, associated with the health information must be removed. We must have no actual knowledge that the information remaining after stripping these identifiers could be used, alone or in combination with other information to identify the consumer.

(2) Health information may be de–identified under the supervision and subject to the documented approval of the Privacy Officer or designee.

(3) The Privacy Officer or designee must verify that health information is de-identified before you may use or disclose it without restriction.

(2) Re–Identification Codes.

Any code or means employed to permit re–identification of de–identified health information will not be derived from or relate to any consumer whose information has been de–identified, be capable of translation to identify a consumer, or be used or disclosed for any purpose other than re–identification of de–identified health information.

Procedure. The Privacy Officer or designee must approve the selection of re-identification codes for de-identified health information. You will

consider re-identification codes to be PHI and apply the privacy protections of the DBH Privacy Manual to them.

16. Research - a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to increase knowledge.

16a) Permitted Use and Disclosure for Research Purposes. A covered entity may use or disclose protected health information (PHI) for research, regardless of the source of funding of the research, provided that:

(1) The covered entity obtains approval for the use or disclosure of PHI by either: an Institutional Review Board (IRB) or a Privacy Board.

(a) An IRB must be established in accordance with federal regulations as cited in 45 C.F.R. § 164.52 (i)(1)(i)(A).

(b) A Privacy Board must: (1) have members with varying backgrounds and appropriate professional competency to review the effect of the research protocol on the individual's privacy rights and related interests; (2) include at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with either; and (3) ensure that members do not review projects if there is a conflict of interest.

(2) Reviews Preparatory to Research (for IRB and Privacy Board). The covered entity obtains from the researcher representations that:

(a) Use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research,

(b) No PHI is to be removed from the covered entity by the researcher, and

(c) The PHI is necessary for the research purposes.

(3) Research of Decedent's Information. The covered entity obtains from the researcher:

(a) Representation that the use or disclosure sought is solely for research on the PHI of decedents,

(b) Documentation of the death of such individuals, if requested, and

(c) Representation that the PHI is necessary for the research purposes.

(4) Authorizations.

(a) As applicable, covered entities may combine "conditioned" and "unconditioned" authorizations. Authorizations must differentiate between conditioned and unconditioned portions. Unconditioned authorizations must be opt in, e.g., __ check box or ___ second signature line.

(b) Authorization may govern future research and must reasonably put individual on notice of potential future research.

16b) Documentation of Approval of the Use or Disclosure of PHI. If approved, the IRB or Privacy Board must document the following:

(1) Identification and Date of Action. A statement identifying the IRB or Privacy Board and the date of approval.

(2) Approval Criteria. A statement that the IRB or Privacy Board has determined that the use or disclosure of PHI satisfies the following criteria:

(a) The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on, at least, the following:

- An adequate plan to protect the identifiers from improper use and disclosure;
- An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
- Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted by this section.

(b) The research could not practicably be conducted without access to and use of the PHI.

(3) PHI Needed. A brief description of the PHI for which use or access has been determined to be necessary by the IRB or Privacy Board.

(4) Review and Approval Procedures. A statement that the use or disclosure of PHI has been reviewed and approved under either normal or expedited review procedures, as follows:

(a) An IRB must follow the requirements of the federal regulations.

(b) A Privacy Board must review the proposed research at convened meetings at which a majority of the Privacy Board members are present, including at least one member who satisfies the criteria for non affiliation as stated in 16a(1) of this section, and the use or disclosure must be approved by the majority of the Privacy Board members present at the meeting, unless the Privacy Board elects to use an expedited review procedure as stated below.

(c) A Privacy Board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the PHI for which use or disclosure is being sought. If the Privacy Board elects to use an expedited review procedure, the review and approval of the use or disclosure of PHI may be carried out by the chair of the Privacy Board, or by one or more members of the Privacy Board as designated by the chair.

(d) The approval must be signed by the chair or designee of the IRB or Privacy Board.

VI. CONSUMER COMPLAINTS AND VIOLATIONS

17. Complaints and HHS Enforcement.

17a) Complaints.

The agency Privacy Officer or designee will investigate and appropriately respond to each written complaint received regarding privacy policies or compliance with the DBH Privacy Manual, HIPAA, the MHIA, Data Sharing and Information Coordination Amendment Act, or 42 CFR Part 2, within ten (10) business days of receipt.

Complaint, for the purposes of this policy, means any concern communicated by a person questioning the privacy policies or compliance with privacy policies, including but not limited to: any act or failure to act relating to a consumer's rights to access to his/her health information, to maintain the privacy of his/her health information, to request restrictions on uses or disclosures of his/her PHI, to request confidential communications regarding his/her PHI, to request amendment of his/her PHI, or to receive an accounting of disclosures of his/her PHI. If a complaint as described in this paragraph is initiated as a grievance, the Office of Consumer and Family Affairs (OCFA) must notify the agency Privacy Officer to ensure compliance with HIPAA regarding complaints.

Procedure.

(1) **Complaint Receipt.**

- Workforce members will advise the consumer or personal representative of the right to file a grievance or to pursue as HIPAA privacy complaint as outlined below.
- If the consumer wants to pursue as a grievance, refer the consumer to the grievance coordinator at the provider level.

  (Consumers may also file a grievance with the DBH where appropriate.)
- If the consumer wants to pursue as a HIPAA privacy complaint, complete, or have the complainant complete FORM 14–Complaint Form; and promptly transmit FORM 14 to the Privacy Officer or designee.

(2) **Complaint Response.** The Privacy Officer or designee will respond to the complaint on the organization's behalf and will process the complaint within ten (10) business days of receipt by the agency as follows:

- Notify OCFA of the complaint,
- Investigate the complaint,
- Document the investigation, findings, and conclusions on Form 14a, Complaint Investigation and Processing Form, and retain with the Privacy Officer files with a copy to OCFA.
- Institute corrective action if warranted,
- Notify the complainant of the resolution of the complaint in writing on Complaint Response Letter 14.1, and

- Have the completed FORM 14 and Complaint Response Letter 14.1, filed in the consumer's clinical record, provide a copy to OCFA, and retain a copy for the Privacy Officer or designee file.

Sample form and notification letter is included in the back of this manual.

17b) Department of Health and Human Services (HHS) Enforcement and Compliance Cooperation.

Network providers will cooperate with any compliance review or complaint investigation by HHS, while preserving the rights of their organization.

Procedure.

(1) **The Privacy Officer or designee will:**

- Coordinate response to any HHS compliance review, complaint investigation or other inquiry, to ensure that all applicable obligations of your organization are fulfilled and all applicable rights and privileges of your organization are preserved and protected.
- Arrange for HHS to have access to your facilities, books, records, accounts, and other non-privileged information sources, during normal business hours.

(2) **Agencies**.

- If a workforce member receives any inquiry, immediately notify the agency Privacy Officer of any inquiry from HHS or any other government official. The agency Privacy Officer will inform the DBH Privacy Officer, who will inform the District-wide Privacy and Security Official.
- Workforce members must await instruction from the agency Privacy Officer before responding to these inquiries or providing any documents or other information on behalf of your organization.
- Verify the identity and authority of a HHS representative prior to disclosure.
- Do not obstruct or interfere with any lawful process, warrant, order or subpoena that may be presented. If the officials insist they have the right of immediate search and seizure of your organization's records, equipment or other matters specified in the process presented, do not obstruct or interfere with them. Instead, use your best efforts to contact the Privacy Officer or agency legal counsel, and observe and document everything that the officials search, seize, say, and do.

(3) **Minimum Necessary.** Workforce members are not required to limit PHI to the minimum necessary.

(4) **Disclosure Log. Use Form 6**-Disclosure Log, to document disclosure.

18 PENALTIES FOR BREACH VIOLATIONS

District of Columbia and federal laws require that PHI be appropriately safeguarded from unauthorized access. Any unauthorized or inappropriate use of PHI owned and/or maintained by the District of Columbia in all formats and electronic systems, by the user or by another who has inappropriately been permitted or enabled access to the system by the user, may subject the user to criminal and civil sanctions pursuant to federal and state law as well as disciplinary action up to and including removal.

18a) MHIA Penalties

- Criminal Violations: (misdemeanor)
  1. Willful: up to $1,000 fine; up to 60 days in jail.
  2. Knowingly, under false pretenses or through deception: up to $5,000 fine; up to 90 days in jail.
- Civil Violations:
  1. Negligent: damages and costs.
  2. Willfully or intentionally: damages not less than $1,000 and costs.

18b) HIPAA Penalties

- Criminal Violations:
  1. Up to $50,000 and 1 year in prison.
  2. Up to $100,000 and 5 years in prison if committed under "false pretenses".
  3. Up to $250,000 and 10 years in prison if intent is commercial advantage, personal gain, or malicious harm.
- Civil Violations:

Violation Category	Each Violation	All Identical Violations Per Calendar Year
Did Not Know	$ 100 - $ 50,000	$ 1,500,000
Had Reasonable Cause to know	$1,000 - $ 50,000	$ 1,500,000
Willful Neglect - corrected in 30 days	$10,000 - $ 50,000	$ 1,500,000
Willful Neglect - not corrected	$ 50,000	$ 1,500,000

18c) Data Sharing Act Penalties

- Criminal Violations (misdemeanor):
  1. Knowingly: up to $2,500 fine, imprisoned not more than 60 days, or both.
  2. Knowingly through deception or theft: up to $5,000 fine, imprisoned not more than 180 days, or both.

- Civil Violations:
  1. Negligent: $500 for each violation.
  2. Willful: $1,000 for each violation.

18d) 42 CFR Part 2 Penalties (for alcohol/drug treatment and prevention information)

- Criminal Violations:
  Fine up to $500 for 1st offense and up to $5,000 for each subsequent offense.

Procedure.

(1) DBH and its participating Network providers shall use DBH-HIPAA Form 15, Confidentiality and Security of PHI for notification and documentation purposes.

(2) Employees must sign the form to acknowledge that they have been informed of the inappropriate uses, restrictions and penalties for MHIA, HIPAA, Data Sharing Act, and 42 CFR Part 2 violations. New DBH employees must sign the form during new employee orientation.

(3) Participating Network providers must develop internal procedures to ensure employees are aware of the penalties and sign DBH HIPAA Form 15.

(4) Workforce members must immediately notify their supervisor and Privacy Officer of any unauthorized use or disclosure of PHI by employees.

(5) Network provider Privacy Officers must report any unauthorized disclosure immediately, but no longer than with 5 business days, to the DBH Privacy Officer. The DBH Privacy Officer will inform the District–wide Privacy and Security Official.

(6) Unauthorized disclosures that affect 500 consumers or more must be reported by the agency to the Department of Health and Human Services (HHS). Also see Section 1f of the manual regarding unauthorized disclosure (breach).

VII. SECURITY POLICIES AND PROCEDURES

These security policies and procedures in some instances speak specifically to DBH responsibilities and to DBH equipment. However, all Network providers shall adopt and follow these security policies to the fullest extent that they are applicable, or they shall adopt and follow comparable security policies and procedures that capture the intent and security measures addressed in these policies.

It is DBH's policy to ensure confidentiality is maintained at all times. As workforce members there is an obligation to protect the privacy of individually identifiable protected health information (PHI) that we create, receive or maintain in our respective roles. Please keep this is mind when printing PHI, faxing, receiving PHI and/or leaving your computers unattended. Be sure to promptly retrieve documents from printers, faxes and close out any program that may expose PHI when you leave your work area.

The DBH Chief Information Officer/designee shall serve as the DBH Information Technology (IT) Security Officer for HIPPA compliance regarding all technology issues and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

1. FAX Policy
2. Computer Security
3. Portable Devices Policy
4. Protection and Physical Security of PHI and DBH Sensitive Information
5. Antivirus and Malicious Code Software and Other Requirements
6. DBH Network Security
7. Secure Print Option Policy

FAX Policy

Purpose.

To ensure that only authorized persons send and receive sensitive information and protected health information (PHI) by fax, and that appropriate protections are in place to prevent misuse.

Policy.

Who is Affected: All DBH employees, contractors, and consultants, and Network providers.

Affected Systems: All fax systems, including stand-alone fax machines, automatic faxing systems, and computer based faxing systems.

Location of fax machines: Fax machines should be located in secured areas where access is available only to authorized or supervised individuals.

Determine if the receiving fax machine where you are sending a fax to is located in a secure area before sending.

If the receiving fax machine is not located in a secure area, call the intended recipient and arrange for immediate pick-up of fax before sending.

Faxing precautions: PHI or sensitive information may be faxed only to verified fax numbers. Preprogramming into fax machines is the preferred method. Requests to send faxes to unknown fax numbers should be carefully verified (e.g., contacting the intended recipient in advance or other knowledgeable person) to ensure appropriate authorization. Fax numbers that are entered manually must be double-checked when the fax number is provided and checked again to be certain the correct fax number has been entered before the fax is sent.

All employees must ensure that documents are not left unattended in fax machines.

Fax Confidentiality Notice: All faxes containing PHI must include a confidentiality notice on the cover page advising an inadvertent recipient of the nature of the information and what to do. Sample Notice:

This transmission and any included attachments are intended only for the person or entity to which it is addressed for their official and confidential use. This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged or protected information under the Health Insurance Portability and Accountability Act (HIPAA), the D.C. Mental Health Information Act (MHIA), or 42 CFR, Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use, copying, or action taken in reliance on the contents of this communication is strictly prohibited. If you have received this communication in error, please notify the sender immediately and delete/destroy all copies of the original transmission. You cannot redisclose PHI without written authorization except as allowed by law.

If the transmission includes alcohol/drug treatment and prevention information, the following statement must also be included:

> "This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR 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 CFR 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 patient. (42 CFR § 2.32)"

Computer Security

Purpose.

Computers at DBH are used to acquire, access, process, and manipulate data, including DBH sensitive data and protected health information (PHI). Maintaining appropriate confidentiality of information is a Department requirement. Security procedures outlined in this policy must be followed to achieve this goal. Also see DBH Policy 811.1, Wireless Communication Devices and Other Portable Technology Equipment.

Policy.

Who is Affected: All DBH employees, contractors and consultants.

Affected Systems: All computers and/or portable devices owned or operated by DBH.

User ID/Passwords: Access privileges are determined based on the duties and responsibilities of each position. User-specific IDs and passwords for network and application access must be used. Sharing of IDs/passwords is prohibited. Violation of this procedure may result in suspension or termination of network access and privileges. Users are responsible for activity accomplished under their login ID and password.

Screensavers: Use of a screensaver or blank screen which locks the computer after a brief period of inactivity is mandatory. Screensavers must be configured to require a password to return to applications or desktop. From a security perspective, this not only protects PHI but it also reduces the likelihood of your workstations being compromised if you happen to walk away and inadvertently forget to lock the workstation.

All DBH computers shall have a locking screensaver that is automatically activated any time a computer remains idle for ten (10) minutes. Idle means no activity via keyboard or mouse. Once the screensaver is activated, the user must enter their password to use the computer.

Files Downloads: Only business related files may be saved on computer systems without approval by Information Services. Also see DBH policy on internet access. Care is to be taken when downloading files from email attachments, portable devices, and/or Internet sites. Scanning of downloads for viruses and malicious code may not capture every type of potential problem. Users should be very wary of downloading information from unfamiliar sites.

Email concerns: The DBH's electronic-mail system is intended for business purposes. Personal use is permissible only within reasonable limits. See DBH policy on email for further details. DBH policy requires care when dealing with sensitive information or PHI to ensure it is properly addressed. Be cautious opening email from unknown parties or with "teaser" lines that are intended to fool users into installing virus or malicious code. Attachments are especially dangerous if they are executable files.

Social engineering: It is illegal to give out or share PHI with individuals who have no need or no authority for the information or whose identity has not been confirmed. Participation in surveys regarding information security, computer users, network infrastructure, or any Information Technology (IT) topic should be declined or referred to the DBH IT Security Officer/designee at DBHIT.Security@dc.gov for participation approval.

File storage on local disks: DBH confidential and PHI may NOT be stored on non DBH disk drives. This information should preferably be stored on secure network drives so that it can be properly secured and backed up.

File storage on network drives: Data owners (persons who created or originated the document or file) are responsible for working with Information Services to ensure users rights to network storage locations are set up and maintained properly. Data owners are responsible for permitting access to their files.

File storage on flash drives or other media: DBH sensitive and PHI may only be stored as described in DBH Policy 811.1, Wireless Communication Devices and Other Portable Technology Equipment.

Disposal of storage media: In order to maintain confidentiality of information, all users are responsible for ensuring storage media are properly destroyed when no longer used. Disposing of intact media in waste containers is NOT adequate. Contact IT ServUs Help Desk for proper disposal techniques for the following:

- Hard Disks
- Magnetic tape
- Memory modules
- Diskettes and CDs
- Optical media (e.g., CDs, DVDs, and Blue Ray)
- Memory cards
- USB drives
- Tablets
- Any other storage media.

Computer power on passwords: It is DBH policy that power-on passwords (*requires a password to continue boot-up of the computer or* device) are not permitted on network computers.

File passwords: Password protection available in applications such as Microsoft Word, Microsoft Excel, and Microsoft Access provides minimal security. Contact Information Services for security evaluation and/or risk assessment to determine an adequate method for securing PHI or DBH confidential files.

Modems: Use of modems on network systems has many security ramifications. Written approval from Information Services is required prior to modem installation.

Remote control software: Use of remote control software on computers and portable devices is prohibited without the express written approval of Information Services. If approval is given, Information Services procedures for configuring the security aspects of the remote control software must be followed.

Portable Devices Policy

The criteria for issuance, use, and maintenance of wireless communication devices and other portable technology equipment is outlined in DBH Policy 811.1, Wireless Communication Devices and Other Portable Technology Equipment. This policy is available on the DBH website.

Protection and Physical Security of PHI and DBH Sensitive Information

Purpose.

To ensure that only authorized individuals have access to DBH sensitive and Protected Health Information (PHI) stored or located outside of information systems and computers.

Policy.

Who is Affected: All DBH employees, contractors, and consultants, and Network providers.

Clinical records. The clinical records of consumers are always defined as PHI. Procedures for use and disclosure are outlined in DBH privacy policies and procedures and in local provider policies. Clinical record storage areas must be tightly controlled locations, provide for signing out of records, and restrict access to the areas. Clinical records or portions of those records used in clinical areas must be kept in secure areas when not actually in use. Vigilance in observing that unauthorized individuals do not access clinical records is required on the part of all staff.

Other Protected Health Information. Information outside of clinical records that contains individually identifiable data is PHI. This information may be contained in reports, documents, letters, notes, forms, applications, and verbal communication. All PHI, regardless of location, must be treated as confidential and is to be stored, accessed, and transported in a secure manner. Several requirements must be met:

a. Information is available to authorized individuals.
b. Locked or secure storage areas must be used.
c. Documents with PHI must not be posted in public areas.

Storage and Use of PHI in work areas. Work areas, including offices, cubicles, shared activity areas, and nursing stations must maintain the confidentiality of PHI. All PHI must be out of view of any casual observer or visitor. PHI must be stored in locked files or desks, or maintained in a tightly controlled access environment.

Oral Communication. Communication of PHI via conversation, whether in-person or via electronic communication methods (wired telephone, portable telephone, paging systems, voice mail, telephone answering systems) must use reasonable safeguards to maintain confidentiality. Conversation between clinical staff involving PHI should be discrete and audible only to the involved parties. Paging systems should not communicate PHI under any circumstances. Voice mail messages should minimize disclosure of PHI by requesting a return call to a specific number to a specific person without providing detailed PHI. Messages left on answering systems should provide minimal information, usually requesting a return call.

Printing. Reports and documents containing confidential or PHI must be printed where only authorized individuals can access them or by using the secure print options feature on DBH copiers. Printouts must be picked up promptly.

Disposal. Proper safeguards and procedures must be followed when disposing of PHI and DBH sensitive information after the required record retention time frame has expired. Shredding of PHI and DBH sensitive information must be handled in a secure and appropriate manner.

Transport of PHI and DBH Sensitive information. Appropriate procedures and precautions must be used when transferring confidential information and PHI. At a minimum, sealing of envelopes, boxes, or pouches is required, and they should be marked CONFIDENTIAL.

Identification Badges. PHI or DBH sensitive information should not be handled or given to any individual without proper identification and authorization. All DBH employees must wear their ID badge at all times when accessing or coming into contact with PHI.

Antivirus and Malicious Code Software And Other Requirements

Purpose.

To prevent occurrences of computer viruses and malicious code incidents. Computer viruses and malicious code incidents pose a serious threat to information security, including availability of network services. Potential effects include: corruption of data; destruction of data; transfer or compromise of confidential or sensitive information; computer operating system problems; increased expenses to repair or correct computer problems; lost productivity; and increased help desk calls. For this reason, efforts to control computer viruses are important at DBH.

Definitions.

1. **Malicious Code**, such as viruses and worms, attack a system in one of two ways, either internally or externally. Traditionally, the virus has been an internal threat, while the worm, to a large extent, has been a threat from an external source.

2. **Computer Viruses** have the following necessary characteristics: replication; requires a host program as a carrier; activated by external action; and replication limited to (virtual) system. In essence, a computer program which has been infected by a virus has been converted into a Trojan horse. The program is expected to perform a useful function, but has the unintended side effect of viral code execution. Upon execution, the virus attempts to replicate and "attach" itself to another program. It is the unexpected and generally uncontrollable replication that makes viruses so dangerous.

Policy.

1. **Computer Hardware:** All computers including portable devices are required to have antivirus\malicious code software installed when connected to the DBH Network (This includes personally owned equipment.). DBH provides the software where deemed appropriate.

2. **Configuration of Antivirus Software:** Procedures for installation and configuration of antivirus software, as determined by Information Services and the DBH IT Security Officer must be adhered to. Only DBH approved antivirus software may be installed on DBH equipment.

3. **Scanning Features:** All CDs and other media must be scanned by all users prior to use in a computer or portable device. All computers should be scanned at least weekly for viruses and malicious code. Depending on risk analysis for individual systems, executable files (files that run a program), documents, and other types of files should be considered for scanning before each use.

4. **Reporting Viruses and Malicious Code:** All users should report unusual computer functioning and application problems to the DBH IT Security Officer at DBHIT.Security@dc.gov. These problems may indicate the presence of viruses or malicious code.

5. **Virus Alert:** Users who are notified about computer viruses or malicious code via email, various news sources, or via other sources should absolutely NOT forward these messages to other users as the email may suggest. Contact Information Services for instructions. In most cases, such emails are actually virus hoaxes relating to non-existent problems. However, virus hoaxes can cause considerable loss in productivity and damage. Information Services will verify and determine the appropriate course of action.

6. **Virus Signature Updates:** Office of the Chief Technology Officer (OCTO) provides DBH automatic updates to virus signatures and patterns. DBH will distribute and update within the network infrastructure as frequently as possible, at a minimum once per week. In the event of the discovery of significant virus or malicious code threats, updates shall be deployed immediately.

7. **Monitoring:** Information Services is responsible for tracking and monitoring occurrences of viruses and malicious code incidents. The Chief Information Officer and DBH IT Security Officer must be informed by designated DBH staff of major incidents, and may be involved in subsequent investigations.

8. **Servers:** Antivirus and malicious code software shall be installed on all servers by Information Services. Configuration, updates, and scanning frequency are determined by Information Services and the DBH IT Security Officer.

DBH Network Security

Purpose.

The security of the DBH network is the foundation for security of electronic information. In order to ensure confidentiality, integrity, and availability of protected health information (PHI) and DBH sensitive information, this policy establishes a set of basic rules for network use that must be followed by all employees, consultants, contractors, and others with access to the DBH Network.

Policy.

1. **Connection of Devices:** Information Services must review and approve all requests to connect computers, printers, and portable devices of any type to the DBH Network. End-users are not permitted to connect devices to the Network without prior written approval from Information Services.

2. **Moving Network Devices:** No devices connected to the DBH Network may be relocated and reconnected to the DBH Network without approval from Information Services. Contact the IT ServUs Help Desk for assistance.

3. **Connection Control:** Information Services is responsible for ensuring that only authorized connections are active.

4. **Modems:** Modem use is not permitted on any device in the DBH Network infrastructure without written approval from Information Services.

5. **Monitoring:** Software that monitors any network activity must have written approval from Information Services and the DBH IT Security Officer before installation.

6. **Wireless Connections:** Access points for wireless devices must be approved in writing by Information Services and the DBH IT Security Officer.

Secure Print Option Policy

Purpose.

To ensure that safeguards are available to protect sensitive information sent to certain centrally located network copiers.

Policy.

Who is Affected: All DBH employees, contractors, and consultants.

Affected Systems: All DBH network Xerox copiers owned or operated by DBH.

Location of Printers: All DBH network Xerox copiers are located throughout DBH.

Procedures.

All DBH network Xerox copiers have secure print.

Secure print enables you to print sensitive documents to the Xerox copiers.

This optional feature only releases the document to be printed when you are physically standing at the copier and ready to pick up the document by entering your own secure password.

To activate secure print feature on your computer, go to print, properties, choose secure print from the job type pull down menu, put in your passcode, and print. The job will be held at the printer until you enter the same passcode to release it.

At the printer, choose the job status button, select your job in the print queue and choose release, enter your passcode and your job will print.

VIII. DEFINITIONS

Administrative information means a consumer's name, age, sex, address, identifying number or numbers, dates and character of sessions (individual or group), and fees.

Agency includes all of DBH and other organizations in the Network.

Authorization means a written form signed by a consumer that authorizes the use or disclosure of the consumer's protected health information (1) by Network providers for purposes other than treatment, payment, or health care operations; or (2) by persons or entities other than Network providers for any purpose.

Business associate means a person or entity who, on behalf of a covered entity or of an organized health care arrangement, but other than in the capacity of a member of the workforce of such covered entity or arrangement:

> (A) Creates, receives, maintains or transmits PHI, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
>
> (B) Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, 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.

Behavioral health services means stand-alone and co-occurring, integrated treatment services for substance abuse and mental health disorders that are designed to promote a person's behavioral health.

Consumer, for the purposes of this manual, means a person who seeks or receives behavioral health services funded or regulated by DBH.

Covered entity means: (1) a health plan; (2) a health care clearinghouse; or (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by these policies and procedures. DBH and participating Network providers who transmit health information electronically are covered entities. Covered entity shall also include the designated health care components of the District government's hybrid entity or a District agency following HIPAA best practices.

Data collector means a person, other than the consumer, health care professional and health care facility who regularly engages, in whole or in part, in the practice of assembling or evaluating consumer protected health information.

Data Use Agreement is an agreement into which the covered entity enters with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and how it will be protected.

De-identified Information is protected health information that has been stripped of all identifiers and cannot be used alone or in combination with any other information to identify the consumer.

Department of Behavioral Health ("DBH") is the District government agency responsible for developing, supporting and overseeing a comprehensive, community-based system of services and supports for residents with mental health and/or substance use disorders that are accessible, accountable, culturally competent, and choice driven.

Designated record set means:

(1) A group of records maintained by or for a covered entity that is:

(i) The clinical records and billing records about consumers 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 consumers.

(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.

Disclosure means the release of, transfer of, provision of access to, or divulging or communicating in any other manner of information outside the entity holding the information.

HHS stands for the United States Department of Health and Human Services.

Health care means care, services, or supplies related to the health of a consumer including mental health and/or substance abuse services and supports. *Health care* includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of a consumer or that affects the structure or function of the body; and

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

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care operations includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities, in accordance with 45 C.F.R. §164.501.

Health care provider means a provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health oversight agency means an agency that is authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg- 91(a)(2)).

The Health Information Technology for Economic and Clinical Health Act (HITECH) provides enforcement, accountability, penalty and persecution-related guidelines for those involved in sharing or accessing PHI, including electronic PHI (ePHI).

Information Received in Confidence is information received from other persons on condition that such information not be disclosed to the consumer or other persons.

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Limited Data Set refers to PHI that excludes 16 categories of direct identifiers and may be used or disclosed, for purposes of research, public health, or health care operations, without obtaining either an individual's authorization or a waiver or an alteration of authorization for its use and disclosure, with a data use agreement.

Mental health professional means any of the following persons engaged in the provision of professional services: (a) a person licensed to practice medicine; (b) a person licensed to practice psychology; (c) a licensed social worker; (d) a professional marriage, family, or child counselor; (e) a rape crisis or sexual abuse counselor who has undergone at least 40 hours of training and is under the supervision of a licensed social worker, nurse, psychiatrist, psychologist, or

psychotherapist; (f) a licensed nurse who is a professional psychiatric nurse; or (g) any person reasonably believed by the consumer to be one of the foregoing persons.

Mental health provider or "MH provider" means (a) any individual or entity, public or private, that is licensed or certified by DBH to provide mental health services or mental health supports; (b) any individual or entity, public or private, that has entered into an agreement with DBH to provide mental health services or mental health supports; and (c) DBH, including Saint Elizabeths Hospital and the Behavioral Health Authority.

Network Providers mean providers that are certified, licensed, or otherwise regulated by DBH and have entered into a contract or agreement with DBH to provide mental health services or supports or alcohol/drug treatment and prevention services.

Organized health care arrangement means an organized system of health care, such as the Network, in which the participating providers hold themselves out to the public as participating in a joint arrangement, and either (1) participate in joint activities that include utilization review, in which health care decisions by participating providers are reviewed by other participating providers or by a third party on their behalf; or (2) participate in quality assessment and improvement activities, in which mental health and/or alcohol/drug treatment and prevention services or supports provided by participating providers are assessed by other participating providers or by a third party on their behalf.

Participating provider means Network Provider.

Payment means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collections activities, medical necessity determinations and utilization review.

Protected health information (PHI) means any written, recorded, electronic (ePHI), or oral information which either (1) identifies, or could be used to identify, a consumer; or (2) relates to the physical or mental health or condition of a consumer, provision of health care to a consumer, or payment for health care provided to a consumer. PHI does not include information in the records listed in subsection (2) 45 C.F.R. §160.103.

Psychotherapy Process Notes are notes made by a mental health professional documenting or analyzing the contents of conversations during an individual, joint, group, or family therapy or counseling session and maintained in a location separate from the consumer's clinical record.

Quality Improvement Activities means the systematic, structured processes designed by the DBH/Network to continuously monitor, analyze, and improve its performance to improve the quality of services to its consumers.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Service Provider means an entity that provides health or human services to District residents pursuant to a contract, grant, or similar agreement with an agency.

Treatment means the provision, coordination, or management of health care and related services, consultation between providers relating to a consumer, or referral of a consumer to another provider for health care.

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

Workforce as used in these policies and procedures, means every employee in the DBH Network. It includes public and private employees and contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

IX. APPENDIX

APPENDIX A – Standard DBH Protocols for Routine or Recurring Disclosures

APPENDIX B – DBH Clinical Record Request Fee Schedule

APPENDIX C – District HIPAA Privacy Compliance Clause (for Business Agreements)

APPENDIX D – DBH-HIPAA Forms/Letters

STANDARD DBH PROTOCOLS FOR ROUTINE OR RECURRING DISCLOSURES

These protocols are applicable to the Department of Behavioral Health (DBH) for requests for disclosure of information from a consumer or personal representative. Network Provides may use these standard protocols as a guide and adjust as needed to address specific routine or recurring protocols specific to their organization.

Section 1. The processing of requests for information and records about a consumer's protected health information (PHI) (including mental health and alcohol/drug treatment and prevention information) is treated with confidentiality. Except as specifically authorized by the DC Mental Health Information Act, as amended (MHIA), the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA), the Data-Sharing and Information Coordination Amendment Act of 2010, and/or 42 CFR Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records, no PHI may be disclosed by or to any individual without the written consent of the consumer.

Written authorization for disclosure of PHI must comply with the requirements of the DBH HIPAA Privacy Manual. When an authorization form other than DMH HIPAA Form 3, Authorization to Use or Disclose Protected Health Information (PHI) (including mental health and alcohol/drug treatment and prevention information) is used, the form must contain all required elements in HIPAA, MHIA, and 42 CFR Part 2.

Contact the Privacy Officer or legal counsel if you have any questions on the process. See Section 2 below for required elements in MHIA and HIPAA for a valid release of information, and also see Section 2 of the DMH Privacy Manual for more information on the authorization for use and disclosure of PHI, and see Section 4 of the manual for use and disclosure of alcohol/drug treatment and prevention information.

Procedure:

1. Receive record request.
2. Provide a copy of each request/authorization to the consumer or the person authorizing the disclosure.
3. Log request into tracking system (important for accounting disclosure regulations under HIPAA; this is also imperative to monitoring the status of time-sensitive requests).
4. Validate request by identifying the consumer as a recipient of care at the facility and investigate the HIPAA compliance of the consumer's authorization to release records.
5. If the request is not notarized, witnessed, or accompanied with picture I.D., authenticate consumer's signature.
6. If the request does not contain the required core elements for a valid release of information (see Section 2 below), notify the requestor and provide a DBH HIPAA Form 3.
7. Match the record request with the consumer's clinical record (e.g., date of birth, sex, SS#).
8. Make initial assessment if record request can be processed. If the consumer is in active treatment, the treating health care professional must be contacted before responding to the request by the consumer for copies/access of their clinical record.
9. If the request cannot be processed, notify the requestor.
10. Locate exact information that has been requested and review and examine each page of the record for confidential and legally protected information.
11. Continue next level of evaluation of the request for special circumstances (e.g., subpoenas, deceased consumer, alcohol/drug treatment and prevention information), and determine if the information requested can be released.
12. If confidential or legally protected information cannot be released, notify the requestor.
13. If working with a paper chart, consolidate pages from the paper chart and designated pages within the electronic health record, and package with the request.
14. Verify consumer identification on every page of the record.
15. Review request and copy chosen pages from the clinical record to determine accuracy of the information.
16. You cannot redisclose PHI without written authorization except as allowed by law.
17. Verify due date for response to record request.

18. Monitor status and completion of pending requests and expedite time-sensitive items.
19. Update request status in the tracking system with the number of pages, content of what was released, recipient and date the records were prepared for release.
20. Create invoice for service, as applicable.
21. Set up accounts receivable file if no payment was received with request.
22. Record payments, if received.
23. Send documents as requested, and include a copy of the authorization and the Restricted Privacy Disclosure Notice (copy attached).
24. Include a copy of the authorization in the consumer's clinical record.
25. Close out request in tracking system when payment is received, track outstanding invoices, and perform collection efforts as needed.

Section 2. Required Elements in MHIA and HIPAA for a Valid Release of Information.

A valid authorization must be written in plain language and contain at least the following core elements:

1. Name of the person who is the subject of the disclosure.
2. Specify the nature of the information to be disclosed, the type of persons authorized to disclose such information, to whom the information may be disclosed and the specific purposes for which the information may be used both at the time of the disclosure and at any time in the future;
3. Advise the consumer of his/her right to inspect his/her record of PHI;
4. Contain the date upon which the authorization was signed and the date or an expiration event that relates to the consumer or the purpose of the use or disclosure, on which the authorization will expire, which shall be no longer than 365 days from the date of authorization;
5. Be signed by the person or persons authorizing the disclosure (If the authorization is signed by a personal representative of the consumer, a description of such representative's authority to act for the consumer must also be provided); and
6. State that the consent is subject to revocation, except where an authorization is executed in connection with a consumer's obtaining a life or non-cancellable or guaranteed renewable health insurance policy, in which case the authorization shall be specific as to its expiration date which shall not exceed 2 years from the date of the policy; or where an authorization is executed in connection with the consumer obtaining any other form of health insurance in which case the authorization shall be specific as to its expiration date, which shall not exceed 1 year from the date of the policy.

Required Statements. In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

- The ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization, by stating either: the covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization, or the consequences to the individual of a refusal to sign the authorization in accordance with HIPAA.
- The information cannot legally be redisclosed by the person or organization that received it without the consumer's authorization, except as allowed by law.

RESTRICTED PRIVACY DISCLOSURE NOTICE

TO:

FROM:

RE: (Consumer's Name) _____

Whenever copies of health records are released or other written disclosure is made, the disclosure must be accompanied by this standard cover sheet.

This transmission and any included attachments are intended only for the person or entity to which it is addressed for their official and confidential use. This communication, along with any attachments, is covered by federal and state law governing protected health information (PHI), and may contain confidential and legally privileged or protected information under the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA); the D.C. Mental Health Information Act of 1978, as amended (MHIA); and/or 42 CFR, Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use, copying, or action taken in reliance on the contents of this communication is strictly prohibited. If you have received this communication in error, please notify the sender immediately and delete/destroy all copies of the original transmission. You cannot redisclose PHI without written authorization except as allowed by law.

For Alcohol/Drug Records. If this transmission includes alcohol/drug treatment and prevention information:

This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR 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 CFR 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 patient. (42 CFR § 2.32)

Department of Behavioral Health
Clinical Record Request Fee Schedule

This fee schedule lists Department of Behavioral Health (DBH) charges for certifying, postage/certified mail, copying clinical records, charges for copying for Patient Advocacy for Individuals with Mental Illness (PAIMI), and disclosure accounting as shown below. This fee schedule is not applicable to FOIA requests.

Private providers can set their own fees; this schedule is provided to them for their information.

- **Certifying Clinical Record** — **$5.00**

- **Paper Form Record Copying***
  - **Pages 1-5** — **($1 per page for first 5 pages)**
  - **Pages 6+** — **$0.25/page**

- **Non-paper Form Record Copying** — **Reasonable charges apply**

- **Postage/Certified Mail** — **Actual cost**

- **Patient Advocacy for Individuals with Mental Illness (PAIMI)**
  - **Pages 1-15** — **No charge**
  - **Pages 16+** — **$0.25/page**

- **Disclosure Accounting Request*** — **$5.00/per request (presumptive rate, unless there are extraordinary circumstances)**

*A consumer is entitled to one free accounting disclosure and a copy of their record (up to 500 pages with no charge) in any 12 month period. If the consumer requests a second accounting disclosure within that same 12 month period, or more than 500 pages, the above fees apply.

These charges also apply to financial records.

Responsible DBH staff will apply the charges above to everyone requesting the copies/services noted except for those individuals/entities noted on the back of this form.

See the back of this form for important guidelines.

DBH Clinical Record Request Fee Schedule Guidelines

CEOs and DBH Privacy Officer/designee, are responsible for ensuring that:

(1) all fees are submitted in accordance with internal guidelines established by their organization;

(2) there are specific, written instructions to responsible staff in their organization on how they are to uniformly charge, collect, and handle fees; and

(3) policies and procedures are followed, including use of required forms, per DBH Privacy Manual.

Responsible DBH staff must use the attached checklist when a fee is not charged.

Exceptions to Charging Fees:

Please contact the DBH General Counsel's Office (202-673-2200) in connection with all formal discovery (subpoena or request for documents) in pending civil or criminal actions other than the following:

- **Court appointed attorneys** - under Chapter Five of Title 21 of the D.C. Code or D.C. Code §24- 501, shall not be charged for copies less than 500 pages per consumer, per case.
- **The Office of Attorney General and the U.S. Attorney's Office** shall not be charged for copies of records for consumers committed under D.C. Code §24- 501 to the extent the records relate to a pending release motion.
- **Third party payers** shall not be charged when DBH will derive direct financial benefit (e.g. Medicaid, private insurance).
- **Other healthcare providers/entities** that provide consumer treatment and care, or support services, and are requesting records to assist in providing treatment and care, or support services for the identified consumer shall not be charged.
- **District of Columbia agencies and judicial courts (pursuant to court orders)** shall not be charged.
- **Other organizations** shall not be charged if they demonstrate that District or federal laws (or the laws of the state in which they are incorporated or based) exempt them from such fees. If an organization states that it is exempt from fees, please ask them to provide a citation to the exempting law or regulation. If you have any remaining questions, contact the Privacy Officer.

Exceptions to Charging Fees for Release of Information Check List

The individual/entity was not charged any fees related to copies of consumer records because the individual/entity fits into one of the following categories:

☐ Consumer entitled to one free accounting disclosure and a copy of their record (up to 500 pages) in any 12 month period.
Indicate date provided: _____.

☐ Court appointed attorney representing an indigent consumer in a court case involving the hospitalization or commitment of the consumer (less than 500 pages per consumer per case).
Indicate date provided: _____.

☐ The attorneys for the government when those attorneys are requesting records of prisoners committed pending or following conviction to the extent the records relate to a pending release motion.

If you receive such a request for information in the context of formal discovery in a criminal or civil case (other than an instance specifically described above), please contact the DBH General Counsel's Office.

☐ Third party payers when the DBH will derive direct financial benefit. (e.g., Medicaid, private insurance).

☐ Other healthcare providers/entities that provide consumer treatment and care, or support services, and are requesting records to assist in providing treatment and care, or support services for the identified consumer.

☐ Other District of Columbia agencies and judicial courts (pursuant to court orders).

Any other organization that is exempted by applicable law from such fees. It is the responsibility of the exempt organization to identify the law that exempts the entity from the otherwise applicable fees.

File the checklist in the consumer's clinical record with the request if there is an exception to charging fees.

GOVERNMENT OF THE DISTRICT OF COLUMBIA

SECTION H. HIPAA PRIVACY COMPLIANCE

This HIPAA Compliance Clause is the standard language that must be included in contracts which involve access to the District's HIPAA protected data (protected health information) or creation of the same. When needed, agencies are encouraged to add business-specific language. This language should also be adapted and used where 1. an agency complies with the best practices of HIPAA, 2. where an agency facilitates access to HIPAA protected data, or 3. where agencies otherwise wish to protect similar data. Finally, where applicable, to ensure HIPAA compliance, this language must be adapted and incorporated or attached to miscellaneous agreements or arrangements such as Memoranda of Understanding, Memoranda of Agreement, Donation Agreements or small purchase arrangements.

For the purpose of this agreement [AGENCY], a covered component within the District of Columbia's Hybrid Entity will be referred to as a "Covered Entity" as that term is defined by the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") and associated regulations promulgated at 45 CFR Parts 160, 162 and 164 as amended (the "HIPAA Regulations") and [INSERT VENDOR INFORMATION], as a recipient of Protected Health Information or electronic Protected Health Information from [AGENCY], is a "Business Associate" as that term is defined by HIPAA.

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Regulations.

Definitions

a. *Business Associate* means a person or entity, who, on behalf of the District government or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of the District or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity for the District, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR § 164.501), management, administrative, accreditation, or financial services to or for the District, or to or for an organized health care arrangement in which the District participates, where the provision of the service involves the disclosure of protected health information from the District or arrangement, or from another business associate of the District or arrangement, to the person. A covered entity may be a business associate of another covered entity.

A Business Associate includes, (i) a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information; (ii) a person that offers a personal health record to one or more individuals on behalf of the District; (iii) a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

A *Business Associate* does not include: (i) a health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual; (ii) a plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of 45 CFR § 164.504(f) apply and are met; (iii) a government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law; iv) a covered entity participating in an organized health care arrangement that performs a function, activity or service included in the definition of a Business Associate above for or on behalf of such organized health care arrangement.

b. *Covered Entity* means a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by 45 C.F.R. Parts 160 and 164 of HIPAA. With respect to this HIPAA Compliance Clause, *Covered Entity* shall also include the designated health care components of the District government's hybrid entity or a District agency following HIPAA best practices.

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

d. *Designated Record Set* means a group of records maintained by or for the Covered Entity that are:

   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. Records used, in whole or in part, by or for the Covered Entity to make decisions about individuals.

e. *Health Care* means care services, or services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

   iv. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

   v. Sale or dispensing of a drug, device, equipment, or other item in accordance with the prescription.

f. *Health Care Components* means a component or a combination of components of a hybrid entity designated by a hybrid entity. *Health Care Components* must include non-covered functions that provide services to the covered functions for the purpose of

facilitating the sharing of Protected Health Information with such functions of the hybrid entity without business associate agreements or individual authorizations.

g. *Health Care Operations* shall have the same meaning as the term "health care operations" in 45 C.F.R. § 164.501.

h. *Hybrid Entity* means a single legal entity that is a covered entity and whose business activities include both covered and non-covered functions, and that designates health care components in accordance with 45 C.F.R. § 164.105(a)(2)(iii)(C). A *Hybrid Entity* is required to designate as a health care component, any other components of the entity that provide services to the covered functions for the purpose of facilitating the sharing of Protected Health Information with such functions of the hybrid entity without business associate agreements or individual authorizations. The District of Columbia is a Hybrid Covered Entity. Hybrid Entities are required to designate and include functions, services and activities within its own organization, which would meet the definition of Business Associate and irrespective of whether performed by employees of the Hybrid Entity, as part of its health care components for compliance with the Security Rule and privacy requirements under this Clause.

i. *Mental Health Information Act* is the law controlling any disclosure of mental health information in the District of Columbia (D.C. Official Code § 7-1201.01 et seq. 2009).

j. *Record* shall mean any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for the Covered Entity.

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

l. *Individually Identifiable Health Information* is information that is health information, including demographic information collected from an individual, and;

vi. Is created or received by a health care provider, health plan, employer, or health care clearinghouse;

vii. Relates to the past, present, or future physical or mental health or condition of an individual; or the past, present, or future payment for the provision of health care to an individual; and

viii. That identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

m. *National Provider Identifier (NPI) Rule:* "National Provider Identifier" shall mean the Standard Unique Health Identifier for Healthcare Providers; Final Rule at 45 C.F.R. Part 162.

n. *Privacy and Security Official.* The person or persons designated by the District of Columbia, a *Hybrid Entity*, who is/are responsible for developing, maintaining, implementing and enforcing the District-wide Privacy Policies and Procedures, and for overseeing full compliance with the Privacy and Security Rules, and other applicable federal and state privacy law.

o. *Privacy Officer.* "Privacy Officer" shall mean the person designated by the District's Privacy and Security Official or one of the District's covered components within its Hybrid Entity , who is responsible for overseeing compliance with the Covered Agency's Privacy Policies and Procedures, the HIPAA Privacy Regulations, HIPAA Security Regulations and other applicable federal and state privacy law(s). Also referred to as the agency Privacy Officer, the individual shall follow the guidance of the District's Privacy and Security Official, and shall be responsive to and report to the District's Privacy and Security Official on matters pertaining to HIPAA compliance.

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

q. *Protected Health Information.* "Protected Health Information" (PHI) or "Electronic Protected Health Information" (ePHI) means individually identifiable health information that is created or received by the Business *Associate from or on behalf of* the Covered Entity, or agency following HIPAA best practices, which is:

ix. Transmitted by, created or maintained in electronic media; or

x. Transmitted or maintained in any other form or medium;

Protected Health Information does not include information in the records listed in subsection (2) of the definition of Protected Health Information in 45 C.F.R. §160.103.

r. *Required By Law.* "Required By Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103, and shall include the MHIA and 42 CFR Part 2 as applicable.

s. *Secretary.* "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or his or her designee.

t. *Security Officer.* The person designated by the Security Official or one of the District of Columbia's designated health care components, who is responsible for overseeing compliance with the Covered Agency's Privacy Policies and Procedures, the Security Rules, and other applicable federal and state privacy law(s). The Covered Agency's security officer shall follow the guidance of the District's Security Official, as well as the Associate Security Official within the Office of the Chief Technology Officer, and shall be responsive to the same on matters pertaining to HIPAA compliance.

u. *Security Rule* "Security Rule" shall mean the Standards for Security of Individually Identifiable Health Information at 45 C.F.R. part 164.

v. *Workforce.* "Workforce" shall mean employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such entity, whether or not they are paid by the covered entity or business associate.

2. Obligations and Activities of Business Associate

a. The Business Associate agrees not to use or disclose Protected Health Information or electronic Protected Health Information (hereinafter "PHI" or Protected Health

Information") other than as permitted or required by this HIPAA Compliance Clause or as Required By Law.

b. The Business Associate agrees to use appropriate safeguards and comply with administrative, physical, and technical safeguards requirements in 45 C.F.R. §§ 164.308, 164.310, 164.312 and 164.316 as required by § 13401 of the Health Information Technology Economic and Clinical Health ACT (February 18, 2010) ("HITECH"), to maintain the security of the Protected Health Information and to prevent use or disclosure of such Protected Health Information other than as provided for by this Clause. Business Associate acknowledges that, pursuant to HITECH, it must comply with the Security Rule and privacy provisions detailed in this Clause. As such, Business Associate is under the jurisdiction of the United States Department of Health and Human Services and is directly liable for its own compliance. A summary of HIPAA Security Rule standards, found at Appendix A to Subpart C of 45 C.F.R. Part 164 is as follows:

Administrative Safeguards

Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)

Physical Safeguards

Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)

Technical Safeguards (see § 164.312)

Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

c. The Business Associate agrees to name a Privacy and/or Security Officer who is accountable for developing, maintaining, implementing, overseeing the compliance of and enforcing compliance with this Clause, the Security Rule and other applicable federal and state privacy laws within the Business Associate's business. The Business associate reports violations and conditions to the District-wide Privacy and Security Official and/or the Agency Privacy Officer of the covered component within the District's Hybrid Entity.

d. The Business Associate agrees to establish procedures for mitigating, and to mitigate to the extent practicable, any deleterious effects that is known to the Business Associate of a use or disclosure of Protected Health Information by the Business Associate in violation of the requirements of this Clause.

e. The Business Associate agrees to report to Covered Entity, in writing, any use or disclosure of the Protected Health Information not permitted or required by this HIPAA Compliance Clause or other incident or condition arising out the Security Rule, including breaches of unsecured protected health information as required at 45 CFR 164.410, to the District-wide Privacy and Security Official or agency Privacy Officer within five (5) days from the time the Business Associate becomes aware of such unauthorized use or disclosure. However, if the Business Associate is an agent of the District (i.e., performing delegated essential governmental functions), the Business Associate must report the incident or condition immediately. Upon the determination of an actual data breach, and in consultation with the District's Privacy and Security Official, the Business Associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the District.

f. The Business Associate agrees to ensure that any workforce member or any agent, including a subcontractor, agrees to the same restrictions and conditions that apply through this Clause with respect to Protected Health Information received from the Business Associate, Protected Health Information created by the Business Associate, or Protected Health Information received by the Business Associate on behalf of the Covered Entity.

g. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information.

h. Initially, within ten (10) days following the commencement of this Contract, or within ten (10) days of a new or updated agreement with a subcontractor, the Business Associate

agrees to provide the District a list of all subcontractors who meet the definition of a Business Associate. Additionally, Business Associate agrees to ensure its subcontractors understanding of liability and monitor, where applicable, compliance with the Security Rule and applicable privacy provisions in this Clause.

i. The Business Associate agrees to provide access within five business days, at the request of the Covered Entity or an Individual, **at a mutually agreed upon location, during normal business hours, and in a format** [as directed by the District Privacy Official or agency Privacy Officer, or as otherwise mandated by the Privacy Rule or applicable District of Columbia laws, rules and regulations, to Protected Health Information in a Designated Record Set, to the Covered Entity or an Individual, to facilitate the District's compliance with the requirements under 45 C.F.R. §164.524.

j. The Business Associate agrees to make any amendment(s) within five business days to the Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 **in a format** [*agency should insert appropriate terms for amendment if applicable*] or as directed by the District Privacy Official or agency Privacy Officer in order to facilitate the District's compliance with the requirements under 45 C.F.R. §164.526.

k. The Business Associate agrees to use the standard practices of the Covered Entity to verify the identification and authority of an Individual who requests the Protected Health Information in a Designated Record Set of a recipient of services from or through the Covered Entity. The Business Associate agrees to comply with the applicable portions of the [*Insert Applicable Agency Identity And Procedure Verification Policy*], attached hereto as Exhibit C and incorporated by reference.

l. The Business Associate agrees to record authorizations and log such disclosures of Protected Health Information and information related to such disclosures as would be required for the Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528 and applicable District of Columbia laws, rules and regulations.

m. The Business Associate agrees to provide to the Covered Entity or an Individual, within five (5) business days of a request **at a mutually agreed upon location, during normal business hours, and in a format designated** [*delete bolded material and insert agency appropriate terms if applicable*] by the District's Privacy and Security Official or agency Privacy Officer and the duly authorized Business Associate workforce member, information collected in accordance with Paragraph (i) of this Section above, to permit the Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528, and applicable District of Columbia laws, rules and regulations.

n. The Business Associate agrees to make internal practices, books, and records, including policies and procedures, and Protected Health Information, relating to the use and disclosure of Protected Health Information received from the Business Associate, or created, or received by the Business Associate on behalf of the Covered Entity, available to the Covered Entity, or to the Secretary, within five (5) business days of their request and **at a mutually agreed upon location, during normal business hours, and in a format designated** [*delete bolded material and insert negotiated terms if applicable*] by the District Privacy and Security Official or agency Privacy Officer and the duly

authorized Business Associate workforce member, or in a time and manner designated by the Secretary, for purposes of the Secretary in determining compliance of the Covered Entity with the Privacy Rule.

o. To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, the business associate agrees to comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s).

p. As deemed necessary by the District, the Business Associate agrees to the monitoring and auditing of items listed in paragraph 2 of this Clause, as well as data systems storing or transmitting protected health information, to verify compliance.

q. The Business Associate may aggregate Protected Health Information in its possession with the Protected Health Information of other Covered Entities that Business Associate has in its possession through its capacity as a Business Associate to other Covered Entities provided that the purpose of the aggregation is to provide the Covered Entity with data analyses to the Health Care Operations of the Covered Entity. Under no circumstances may the Business Associate disclose Protected Health Information of one Covered Entity to another Covered Entity absent the explicit written authorization and consent of the Privacy Officer or a duly authorized workforce member of the Covered Entity.

r. Business Associate may de-identify any and all Protected Health Information provided that the de-identification conforms to the requirements of 45 C.F.R. § 164.514(b) and any associated HHS guidance. Pursuant to 45 C.F.R. § 164.502(d)(2), de-identified information does not constitute Protected Health Information and is not subject to the terms of this HIPAA Compliance Clause.

3. Permitted Uses and Disclosures by the Business Associate

a. Except as otherwise limited in this HIPAA Compliance Clause, the Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, the Covered Entity as specified in the Contract, provided that such use or disclosure would not violate Subpart E of 45 CFR Part 164 if the same activity were performed by the Covered Entity or would not violate the minimum necessary policies and procedures of the Covered Entity.

b. Except as otherwise limited in this HIPAA Compliance Clause, the Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

c. Except as otherwise limited in this HIPAA Compliance Clause, the Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that the disclosures are Required By Law, or the 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 has knowledge that the confidentiality of the information has been breached.

d. Except as otherwise limited in this HIPAA Compliance Clause, the Business Associate may use Protected Health Information to provide Data Aggregation services to the Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

e. Business Associate may use Protected Health Information to report violations of the Law to the appropriate federal and District of Columbia authorities, consistent with 45 C.F.R. § 164.502(j)(1).

4. Additional Obligations of the Business Associate

a. Business Associate shall submit a written report to the Covered Entity that identifies the files and reports that constitute the Designated Record Set of the Covered Entity. Business Associate shall submit said written report to the Privacy Officer no later than thirty (30) days after the commencement of the HIPAA Compliance Clause. In the event that Business Associate utilizes new files or reports which constitute the Designated Record Set, Business Associate shall notify the Covered Entity of said event within thirty (30) days of the commencement of the file's or report's usage. The Designated Record Set file shall include, but not be limited to the identity of the following:

i. Name of the Business Associate of the Covered Entity;

ii. Title of the Report/File;

iii. Confirmation that the Report/File contains Protected Health Information (Yes or No);

iv. Description of the basic content of the Report/File;

v. Format of the Report/File (Electronic or Paper);

vi. Physical location of Report/File;

vii. Name and telephone number of current member(s) of the workforce of the Covered Entity or other District of Columbia Government agency responsible for receiving and processing requests for Protected Health Information; and

viii. Supporting documents if the recipient/personal representative has access to the Report/File.

b. Business Associate must provide assurances to the Covered Entity that it will continue to employ sufficient administrative, technical and physical safeguards, as described under the Security Rule, to protect and secure (the Covered Entity's) ePHI entrusted to it. These safeguards include:

i. The Business Associate agrees to administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that the Business Associate creates, receives, maintains or transmits on behalf of the covered entity.

ii. The Business Associate agrees to report to the covered entity any security incident of which it becomes aware, including any attempts to access ePHI, whether those attempts were successful or not.

iii. This Business Associate Agreement may be terminated if the covered entity determines that the business associate has materially breached the agreement.

iv. The Business Associate agrees to make all policies and procedures, and documents relating to security, available to the Secretary of HHS for the purposes of determining the covered entity's compliance with HIPAA.

v. This agreement continues in force for as long as the Business Associate retains any access to the Covered Entity's ePHI.

vi. With respect to the subset of PHI known as electronic PHI (ePHI) as defined by HIPAA Security Standards at 45 C.F.R. Parts 160 and 164, subparts A and C (the "Security Rule"), if in performing the Services, Business Associate, its employees, agents, subcontractors and any other individual permitted by Business Associate will have access to any computer system, network, file, data or software owned by or licensed to Provider that contains ePHI, or if Business Associate otherwise creates, maintains, or transmits ePHI on Provider's behalf, Business Associate shall take reasonable security measures necessary to protect the security of all such computer systems, networks, files, data and software. With respect to the security of ePHI, Business Associate shall: (A) 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 Provider; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; and (C) Report to the Provider any security incident of which it becomes aware.

vii. Business Associate agrees not to electronically transmit or permit access to PHI unless such transmission or access is authorized by this Addendum and the Agreement and further agrees that it shall only transmit or permit such access if such information is secured in a manner that is consistent with applicable law, including the Security Rule. For purposes of this Addendum, "encrypted" shall mean the reversible conversion of readable information into unreadable, protected form so that only a recipient who has the appropriate "key" can convert the information back into original readable form. If the Covered Entity stores, uses or maintains PHI in encrypted form, or in any other secured form acceptable under the security regulations, Covered Entity shall promptly, at request, provide with the key or keys to decrypt such information and will otherwise assure that such PHI is accessible upon reasonable request.

viii. In the event Business Associate performs functions or activities involving the use or disclosure of PHI on behalf of Covered Entity that involve the installation or maintenance of any software (as it functions alone or in combination with any hardware or other software), Business Associate shall ensure that all such software complies with all applicable standards and specifications required by the HIPAA Regulations and shall inform the Covered Entity of any software standards or specifications not compliant with the HIPAA Regulations.

c. At the request of the Covered Entity, the Business Associate agrees to amend this agreement to comply with all HIPAA mandates.

5. Sanctions

Business Associate agrees that its workforce members, agents and subcontractors who violate the provisions of HIPAA or other applicable federal or state privacy law will be subject to discipline in accordance with Business Associate's Personnel Policy and applicable collective bargaining agreements. Business Associate agrees to impose sanctions consistent with Business Associate's personnel policies and procedures and applicable collective bargaining agreements with respect to persons employed by it. Members of the Business Associate Workforce who are not employed by Business Associate are subject to the policies and applicable sanctions for violation of this Compliance Clause as set forth in business associate agreements. In the event Business Associate imposes sanctions against any member of its workforce, agents and subcontractors for violation of the provisions of HIPAA or other applicable federal or state privacy laws, the Business Associate shall inform the District Privacy Official or the agency Privacy Officer of the imposition of sanctions.

6. Obligations of the Covered Entity

a. The Covered Entity shall notify the Business Associate of any limitation(s) in its Notice of Privacy Practices of the Covered Entity in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect the use or disclosure of Protected Health Information by the Business Associate.

b. The Covered Entity shall notify the Business Associate of any changes in, or revocation of, permission by the Individual to the use or disclosure of Protected Health Information, to the extent that such changes may affect the use or disclosure of Protected Health Information by the Business Associate.

c. The Covered Entity shall notify the Business Associate of any restriction to the use or disclosure of Protected Health Information that the Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect the use or disclosure of Protected Health Information by the Business Associate.

7. Permissible Requests by Covered Entity

Covered Entity shall not request the Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule and Subpart E of 45 CFR Part 164 if done by the Covered Entity.

8. Representations and Warranties.

The Business Associate represents and warrants to the Covered Entity:

a. That it is duly organized, validly existing, and in good standing under the laws of the jurisdiction in which it is organized or licensed, it has the full power to enter into this HIPAA Compliance Clause and it, its employees, agents, subcontractors, representatives and members of its workforce are licensed and in good standing with the applicable agency, board, or governing body to perform its obligations hereunder, and that the performance by it of its obligations under this HIPAA Compliance Clause has been duly authorized by all necessary corporate or other actions and will not violate any provision of any license, corporate charter or bylaws;

b. That it, its employees, agents, subcontractors, representatives and members of its workforce are in good standing with the District of Columbia, that it, its employees, agents, subcontractors, representatives and members of its workforce will submit a letter of good standing from the District of Columbia, and that it, its employees, agents, subcontractors, representatives and members of its workforce have not been de-barred from being employed as a contractor by the federal government or District of Columbia;

c. That neither the execution of this HIPAA Compliance Clause, nor its performance hereunder, will directly or indirectly violate or interfere with the terms of another agreement to which it is a party, or give any governmental entity the right to suspend, terminate, or modify any of its governmental authorizations or assets required for its performance hereunder. The Business Associate represents and warrants to the Covered Entity that it will not enter into any agreement the execution or performance of which would violate or interfere with this HIPAA Compliance Clause;

d. That it is not currently the subject of a voluntary or involuntary petition in bankruptcy, does not currently contemplate filing any such voluntary petition, and is not aware of any claim for the filing of an involuntary petition;

e. That all of its employees, agents, subcontractors, representatives and members of its workforce, whose services may be used to fulfill obligations under this HIPAA Compliance Clause are or shall be appropriately informed of the terms of this HIPAA Compliance Clause and are under legal obligation to the Business Associate, by contract or otherwise, sufficient to enable the Business Associate to fully comply with all provisions of this HIPAA Compliance Clause. Modifications or limitations that the Covered Entity has agreed to adhere to with regards to the use and disclosure of Protected Health Information of any individual that materially affects or limits the uses and disclosures that are otherwise permitted under the Privacy Rule will be communicated to the Business Associate, in writing, and in a timely fashion;

f. That it will reasonably cooperate with the Covered Entity in the performance of the mutual obligations under this Agreement;

g. That neither the Business Associate, nor its shareholders, members, directors, officers, agents, subcontractors, employees or members of its workforce have been excluded or served a notice of exclusion or have been served with a notice of proposed exclusion, or have committed any acts which are cause for exclusion, from participation in, or had any sanctions, or civil or criminal penalties imposed under, any federal or District healthcare program, including but not limited to Medicare or Medicaid, or have been convicted, under federal or District law (including without limitation following a plea of *nolo contendere* or participation in a first offender deferred adjudication or other arrangement whereby a judgment of conviction has been withheld), of a criminal offense related to (a) the neglect or abuse of a patient, (b) the delivery of an item or service, including the performance of management or administrative services related to the delivery of an item or service, under a federal or District healthcare program, (c) fraud, theft, embezzlement, breach of fiduciary responsibility, or other financial misconduct in connection with the delivery of a healthcare item or service or with respect to any act or omission in any program operated by or financed in whole or in part by any federal, District or local government agency, (d) the unlawful, manufacture, distribution, prescription or dispensing of a controlled substance, or (e) interference with or obstruction of any investigation into any criminal offense described in (a) through (d) above. The Business

Associate further agrees to notify the Covered Entity immediately after the Business Associate becomes aware that any of the foregoing representations and warranties may be inaccurate or may become incorrect

9. Term and Termination

a. *Term.* The requirements of this HIPAA Compliance Clause shall be effective as of the date of the contract award, and shall terminate when all of the Protected Health Information provided by the Covered Entity to the Business Associate, or created or received by the Business Associate on behalf of the Covered Entity, is confidentially destroyed or returned to the Covered Entity within five (5) business days of its request. The Protected Health Information shall be returned in a format mutually agreed upon by and between the Privacy Official and/or Privacy Officer or his or her designee and the appropriate and duly authorized workforce member of the Business Associate. If it is infeasible to return or confidentially destroy the Protected Health Information, protections shall be extended to such information, in accordance with the termination provisions in this Section and communicated to the Privacy Official or Privacy Officer or his or her designee. The requirement to return Protected Health Information to the District at the end of the contract term or if the contract is terminated applies irrespective of whether the Business Associate is also a covered entity under HIPAA. Where a business associate is also a covered entity, Protected Health Information provided by the District, or created or received by the Business Associate on behalf of the District, a duplicate of the record may be acceptable if mutually agreed.

b. *Termination for Cause.* Upon the Covered Entity's knowledge of a material breach of this HIPAA Compliance Clause by the Business Associate, the Covered Entity shall either:

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

ii. Immediately terminate the Contract if the Business Associate breaches a material term of this HIPAA Compliance Clause and a cure is not possible.

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

c. *Effect of Termination.*

i. Except as provided in paragraph (ii) of this section, upon termination of the Contract, for any reason, the Business Associate shall return in **a mutually agreed upon format or confidentially destroy** [*delete bolded material and insert negotiated terms and conditions if applicable*] all Protected Health Information received from the Covered Entity, or created or received by the Business Associate on behalf of the Covered Entity within five (5) business days of termination. This provision shall apply to Protected Health Information that is in the possession of ALL subcontractors, agents or workforce members of the Business Associate. The Business Associate shall retain no copies of Protected Health Information in any form.

ii. In the event that the Business Associate determines that returning or destroying the Protected Health Information is infeasible, the Business Associate shall

provide to the Covered Entity written notification of the conditions that make the return or confidential destruction infeasible. Upon determination by the agency Privacy Officer that the return or confidential destruction of the Protected Health Information is infeasible, the Business Associate shall extend the protections of this HIPAA Compliance Clause to such Protected Health Information and limit further uses and disclosures of such Protected Health Information for so long as the Business Associate maintains such Protected Health Information. Additionally, the Business Associate shall:

(1) Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;

(2) Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;

(3) Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;

(4) Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and

(5) Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

The obligations outlined in Section 2. Obligations and Activities of Business Associate shall survive the termination of this Contract.

10. Miscellaneous

a. *Regulatory References.* A reference in this HIPAA Compliance Clause to a section in the Privacy Rule means the section as in effect or as amended.

b. *Amendment.* The Parties agree to take such action as is necessary to amend this HIPAA Compliance Clause from time to time as is necessary for the Covered Entity to comply with the requirements of the Privacy Rule and HIPAA. Except for provisions required by law as defined herein, no provision hereof shall be deemed waived unless in writing and signed by duly 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 HIPAA Compliance Clause.

c. *Survival.* The respective rights and obligations of the Business Associate under Section 9. Term and Termination of this HIPAA Compliance Clause and Sections 9 and 20 of the Standard Contract Provisions for use with the District of Columbia Government Supply and Services Contracts, effective April 2003, shall survive termination of the Contract.

d. *Interpretation.* Any ambiguity in this HIPAA Compliance Clause shall be resolved to permit compliance with applicable federal and District of Columbia laws, rules and regulations, and the HIPAA Rules, and any requirements, rulings, interpretations, procedures, or other actions related thereto that are promulgated, issued or taken by or on behalf of the Secretary; provided that applicable federal and District of Columbia laws, rules and regulations shall supersede the Privacy Rule if, and to the extent that they impose additional requirements, have requirements that are more stringent than or provide greater protection of patient privacy or the security or safeguarding of Protected Health Information than those of the HIPAA Rules.

The terms of this HIPAA Compliance Clause amend and supplement the terms of the Contract, and whenever possible, all terms and conditions in this HIPAA Compliance Clause are to be harmonized. In the event of a conflict between the terms of the HIPAA Compliance Clause and the terms of the Contract, the terms of this HIPAA Compliance Clause shall control; provided, however, that this HIPAA Compliance Clause shall not supersede any other federal or District of Columbia law or regulation governing the legal relationship of the Parties, or the confidentiality of records or information, except to the extent that the Privacy Rule preempts those laws or regulations. In the event of any conflict between the provisions of the Contract (as amended by this HIPAA Compliance Clause) and the Privacy Rule, the Privacy Rule shall control.

e. *No Third-Party Beneficiaries.* The Covered Entity and the Business Associate are the only parties to this HIPAA Compliance Clause and are the only parties entitled to enforce its terms. Except for the rights of Individuals, as defined herein, to have access to and amend their Protected Health Information, and to an accounting of the uses and disclosures thereof, in accordance with Paragraphs (2)(f), (g) and (j), nothing in the HIPAA Compliance Clause 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.

f. *Compliance with Applicable Law.* The Business Associate shall comply with all federal and District of Columbia laws, regulations, executive orders and ordinances, as they may be amended from time to time during the term of this HIPAA Compliance Clause and the Contract; to the extent they are applicable to this HIPAA Compliance Clause and the Contract.

g. *Governing Law and Forum Selection.* This Contract shall be construed broadly to implement and comply with the requirements relating to the Privacy Rule, and other applicable laws and regulations. All other aspects of this Contract shall be governed under the laws of the District of Columbia. The Covered Entity and the Business Associate agree that all disputes which cannot be amicably resolved by the Covered Entity and the Business Associate regarding this HIPAA Compliance Clause shall be litigated before the District of Columbia Contract Appeals Board, the District of Columbia Court of Appeals, or the United States District Court for the District of Columbia having jurisdiction, as the case may be. The Covered Entity and the Business Associate expressly waive any and all rights to initiate litigation, arbitration, mediation,

negotiations and/or similar proceedings outside the physical boundaries of the District of Columbia and expressly consent to the jurisdiction of the above tribunals.

h. *Indemnification.* The Business Associate shall indemnify, hold harmless and defend the Covered Entity from and against any and all claims, losses, liabilities, costs, and other expenses incurred as a result or arising directly or indirectly out of or in connection with (a) any misrepresentation, breach of warranty or non-fulfillment of any undertaking of the Business Associate under this HIPAA Compliance Clause; and (b) any claims, demands, awards, judgments, actions and proceedings made by any person or organization, arising out of or in any way connected with the performance of the Business Associate under this HIPAA Compliance Clause.

i. *Injunctive Relief.* Notwithstanding any rights or remedies under this HIPAA Compliance Clause or provided by law, the Covered Entity retains all rights to seek injunctive relief to prevent or stop the unauthorized use or disclosure of Protected Health Information by the Business Associate, its workforce, any of its subcontractors, agents, or any third party who has received Protected Health Information from the Business Associate.

j. *Assistance in litigation or administrative proceedings.* The Business Associate shall make itself and any agents, affiliates, subsidiaries, subcontractors or its workforce assisting the Business Associate in the fulfillment of its obligations under this HIPAA Compliance Clause and the Contract, available to the Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Covered Entity, its directors, officers or employees based upon claimed violation of HIPAA, the Privacy Rule or other laws relating to security and privacy, except where the Business Associate or its agents, affiliates, subsidiaries, subcontractors or its workforce are a named adverse party.

k. *Notices.* Any notices between the Parties or notices to be given under this HIPAA Compliance Clause shall be given in writing and delivered by personal courier delivery or overnight courier delivery, or by certified mail with return receipt requested, to the Business Associate or to the Covered Entity, to the addresses given for each Party below or to the address either Party hereafter gives to the other Party. Any notice, being addressed and mailed in the foregoing manner, shall be deemed given five (5) business days after mailing. Any notice delivered by personal courier delivery or overnight courier delivery shall be deemed given upon notice upon receipt.

If to the Business Associate, to	If to the Covered Entity, to
_____	_____
_____	_____
_____	_____
Attention: _____	Attention: _____
Fax: _____	Fax: _____

l. *Headings.* Headings are for convenience only and form no part of this HIPAA Compliance Clause and shall not affect its interpretation.

m. *Counterparts; Facsimiles.* This HIPAA Compliance Clause may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies hereof shall be deemed to be originals.

n. *Successors and Assigns.* The provisions of this HIPAA Compliance Clause shall be binding upon and shall inure to the benefit of the Parties hereto and their respective successors and permitted assigns, if any.

o. *Severance.* In the event that any provision of this HIPAA Compliance Clause is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this HIPAA Compliance Clause will remain in full force and effect. In addition, in the event a Party believes in good faith that any provision of this HIPAA Compliance Clause fails to comply with the then-current requirements of the Privacy Rule, such party shall notify the other Party in writing, in the manner set forth in Section 10. Miscellaneous, Paragraph k. Notices. Within ten (10) business days from receipt of notice, the Parties shall address in good faith such concern and amend the terms of this HIPAA Compliance Clause, if necessary to bring it into compliance. If, after thirty (30) days, the HIPAA Compliance Clause fails to comply with the Privacy Rule, then either Party has the right to terminate this HIPAA Compliance Clause upon written notice to the other Party.

p. *Independent Contractor.* The Business Associate will function as an independent contractor and shall not be considered an employee of the Covered Entity for any purpose. Nothing in this HIPAA Compliance Clause shall be interpreted as authorizing the Business Associate workforce, its subcontractor(s) or its agent(s) or employee(s) to act as an agent or representative for or on behalf of the Covered Entity.

q. *Entire Agreement.* This HIPAA Compliance Clause, as may be amended from time to time pursuant to Section 10. Miscellaneous, Paragraph b. Amendment, which incorporates by reference the Contract, and specific procedures from the District of Columbia Department of Health Privacy Policy Operations Manual, constitutes the entire agreement and understanding between the Parties and supersedes all prior oral and written agreements and understandings between them with respect to applicable District of Columbia and federal laws, rules and regulations, HIPAA and the Privacy Rule, and any rules, regulations, requirements, rulings, interpretations, procedures, or other actions related thereto that are promulgated, issued or taken by or on behalf of the Secretary.

Attachments:

Exhibit A *Identity and Procedure Verification*

DBH-HIPAA FORMS/LETTERS

Form 1 – Joint Notice of Privacy Practices
Form 2 –Reserved
Form 3 – Authorization to Use or Disclose PHI
Form 4 – Reserved
Form 5 – Reserved

Form 6 – Disclosure Log
Letters: 6.1 – Notification to Consumer of Unauthorized Disclosure
6.2 – Notification to Inadvertent Recipient of Unauthorized Disclosure

Form 7 – Access Request Form
Form 7a - Access Request Processing Form
Letters: 7.1 – Grant of Access to Records (to consumer)
7.1a – Direction to Retrieve Records (to business associates)
7.2 – Denial of Access to Records (to consumer)

Form 8 – Designated Personnel and Record Sets

Form 9 – Amendment Request
Form 9a – Amendment Request Processing Form
Letters: 9.1 – Grant of Amendment to Records (to consumer)
9.1a – Notification to Amend Records (to business associates)
9.2 – Denial of Amendment to Records (to consumer)
9.2a – Notification of Record Amendment Denial (to business associates)

Form 10 – Request for Accounting of Disclosures of PHI
Form 10a – Disclosure Accounting Processing Form
Letters: 10.1 – Direction to Account for Disclosures (to business associates)
10.2 – Disclosure Accounting (to consumer)

Form 11 – Restriction Request
Form 11a – Restriction Request Processing Form
Letters: 11.1 – Agreement to Restriction Request (to consumer)
11.1a – Notification of Restriction on PHI (to business associates)
11.2 – Denial of Restriction Request (to consumer)

Form 11b – Termination of Restriction (by consumer or clinician)
Letters: 11.3 – Notice of Termination of Restriction Agreement (to consumer)
11.3a – Notice of Termination of Restriction Agreement
(to business associates)

Form 12 – Confidential Communication Request
Form 12a – Confidential Communication Request Processing Form
Letters: 12.1 – Accommodation of Confidential Communication Request (to consumer)
12.1a – Notification of Confidential Communication Requirement (to business associates)
12.2 – Denial of Confidential Communication Request (to consumer)

Form 13 – Data Use Agreement

Form 14 – Complaint Form
Form 14a – Complaint Investigation and Processing Form
Letters: 14.1 – Complaint Response Letter (to consumer)

Form 15 – Confidentiality and Security of Protected Health Information

GOVERNMENT OF THE DISTRICT OF COLUMBIA
DEPARTMENT OF BEHAVIORAL HEALTH

JOINT NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW PROTECTED HEALTH INFORMATION (PHI) INCLUDING MENTAL HEALTH INFORMATION AND ALCOHOL/DRUG TREATMENT AND PREVENTION INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED. PLEASE REVIEW THIS NOTICE CAREFULLY.

The Department of Behavioral Health (DBH) Network includes DBH and all providers that are certified, licensed, or otherwise regulated by DBH or have entered into a contract or agreement with DBH to provide mental health services or supports and or alcohol/drug treatment and prevention services. This notice explains how your PHI will be used, shared, and protected by the participating Network providers.

What is PHI? PHI is any written, recorded, or oral information which:

(1) identifies, or could be used to identify, a consumer; and
(2) relates to: (a) the physical or mental health or condition of a consumer,
(b) provision of health care to a consumer, or
(c) payment for health care provided to a consumer.

USES AND DISCLOSURES OF YOUR PHI WHEN AUTHORIZATION IS NOT REQUIRED

Under what circumstances can my PHI be shared without my consent or authorization?

(1) Your PHI (including mental health information, and alcohol/drug treatment and prevention information maintained by an alcohol/drug treatment and prevention provider) may be disclosed without your prior consent or authorization in the following situations:

- To report suspected child abuse or neglect;
- In a medical emergency when there is a threat to health of individual that requires immediate medical attention.
- For health oversight activities such as evaluating programs and audits;
- In response to a court order;
- For research purposes, such as research related to the development of better treatments, provided the research study meets certain privacy requirements;
- To report a crime or a threat of crime occurring on the provider's premises or directed against the provider's staff; and
- Pursuant to a qualified service organization or business associate agreement.

(2) <u>For Mental Health Information Only</u>. In addition, mental health PHI may also be disclosed without prior consent or authorization as follows:

- With Network providers or those D.C. Health and Human Service Agencies and their respective service providers that are covered entities under HIPAA, including Department of Human Services, Child and Family Services Agency, Department of Health, and Department of Health Care Finance, to coordinate treatment benefits and services;
- When a mental health professional believes it is necessary to ask for emergency psychiatric hospitalization, or to protect you or someone else from serious physical harm;
- For certain judicial and administrative proceedings;

- To report suspected adult or child abuse or neglect;
- When requested by a designated agency representative for the District of Columbia protection and advocacy agency when investigating allegations of abuse or neglect for persons with mental illness;
- At the request of your legal representative;
- To correctional institutions or law enforcement officials having lawful custody of you in order to facilitate the delivery of mental health services and supports; and
- To monitor your compliance with a condition of pretrial release, probation, parole, supervised release, or diversion agreement regarding mental health treatment.

FREQUENTLY ASKED QUESTIONS

If I am in an alcohol/drug treatment and prevention program, can the provider share my alcohol/drug treatment and prevention information with another Network provider without my consent?

No. 42 CFR Part 2 specifically requires written consent to disclose alcohol/drug treatment and prevention information unless an exception noted in (1) above applies.

Can my PHI be used or disclosed for other purposes if I give permission?

Yes. Your PHI can be shared for purposes other than those described above, but only if you give specific permission by signing an authorization form. For example, you might give us permission to release your PHI to a provider outside of the Network to allow that provider to give you a service or treatment that you need. You have the option of saying that the authorization will remain in effect for any period of time up to 365 days, except in cases where you authorized the disclosure in order to obtain life insurance or non-cancellable or guaranteed renewable health insurance, in which case the authorization can be up to two (2) years from the date of the policy.

If I authorize disclosure, can I revoke my authorization?

Yes. Except for insurance purposes, you can revoke your authorization anytime by giving written notice to your provider. But you must do this in writing and bring it to your provider so that Network providers will stop using and disclosing your PHI. Network providers are permitted to use and disclose your PHI based on your authorization until the Network provider receives your revocation in writing. The revocation of your authorization will not affect any action by the Network provider before it was received.

OUR DUTY TO PROTECT YOUR PHI

What is the Network required to do to protect my PHI?

All Network providers are required by law to protect the privacy of your PHI, and to provide you with this Notice of their legal duties and privacy practices. If the law requires changes to the terms of this Notice, all Network providers will be required to follow the terms of the changed Notice.

YOUR RIGHTS REGARDING YOUR PHI

What rights do I have concerning my PHI?

- You have the right to see and copy your PHI with limited exceptions.
- You have the right to request that your record of PHI be amended.

- You have the right to be informed about your PHI in a confidential manner that you choose. The manner you choose must be reasonable for us to do.
- You have the right to request that we limit certain uses and disclosures of your PHI. Network providers do not have to agree to your restrictions, but if we do agree, we must follow the restrictions.
- You have a right to restrict disclosure of PHI when paid out of pocket.
- You have the right to obtain information about disclosures that the Network providers have made of your PHI.
- You have the right to have a paper copy of this Privacy Notice.
- You have a right to be notified of a breach of your PHI.

What can I do if I wish to exercise my rights, have questions, or want to complain about the use and disclosure of my PHI?

If you wish to exercise your rights, or you have a question or complaint about the use and disclosure of your PHI, **you should contact the privacy officer at the agency providing you treatment**. You may also contact one or both of the organizations listed below:

DBH Privacy Officer
D.C. Department of Behavioral Health
64 New York Avenue, NE, 3rd Floor
Washington, D.C. 20002
(202) 671-4088
TTY/TTD: (202) 673-7500
E-mail: dbh.privacy@dc.gov

District-wide Privacy and Security Official
Office of Attorney General
441 4th Street, NW, 11th Floor
Washington D.C. 20001
(202) 442-9373
TTD: (202) 724-5055
TTY: (202) 727-3363
E-mail: dcprivacy@dc.gov or tina.curtis@dc.gov

You may also complain to the U.S. Department of Health and Human Services, by sending a written complaint to the following address:

Office for Civil Rights – Region III
U.S. Department of Health and Human Services
150 S. Independence Mall West, Suite 372, Public Ledger Building
Philadelphia, PA 19106-9111
Main Line (215) 861-4441; Hotline (800) 368-1019; Fax (215) 861-4431
TDD (215) 861-4440
E-mail: ocrmail@hhs.gov

You always have the right to file a grievance through the DBH grievance procedures. No one may take any action against you for complaining about the use and disclosure of your PHI.

If you have a hard time understanding this Notice, please ask for assistance.

CHANGES TO THIS NOTICE

If the law requires changes to the terms of this Notice, all Network providers will be required to follow the terms of the changed Notice. If the notice is changed, the changes will apply to all PHI (including mental health information, and alcohol/drug treatment and prevention information maintained by an alcohol/drug treatment and prevention provider) created or received before the notice was changed. The amended notice will be posted on the DBH website, and should be provided to you at your next visit and posted at all service sites.

Acknowledgement of Receipt of the Notice of Privacy Practices

I confirm that I have been offered a copy of the DBH Provider Network's Joint Notice of Privacy Practices, and I have been offered a copy of the Notice.

Signature_____ **Date** _____

Please Print Name_____

Relationship if other than consumer_____

_____ **I refuse to sign this form.**

Note to Network personnel:

If consumer/representative refuses Notice or signature, acknowledge refusal by providing the following information:

Network Personnel's Name: _____

Title: _____

Signature: _____ Date _____

Comments: _____

Joint Notice of Privacy Practices & copy of Acknowledgement Form – Consumer
Original Acknowledgement Form – Clinical Record

GOVERNMENT OF THE DISTRICT OF COLUMBIA
DEPARTMENT OF BEHAVIORAL HEALTH

Authorization to Use or Disclose Protected Health Information
(including mental health information and alcohol/drug treatment and prevention information)

Name of Consumer (print) _____ **Identification Number** _____

Address _____ **Date of Birth** _____

City/State/Zip Code _____ **Other name(s) used** _____

RELEASE INFORMATION TO:	**INFORMATION TO BE RELEASED BY:**
Name/Title _____	Name/Title _____
Organization _____	Organization _____
Address _____	Address _____
Phone #: _____ Fax # _____	Phone # _____ Fax # _____

INFORMATION TO BE DISCLOSED: I voluntarily authorize and request disclosure (including paper, oral, and electronic interchange) of my clinical records. This includes specific permission to release all records and other information regarding my treatment, hospitalization, and outpatient care including: ***(The following items must be checked in order to be released)***

- ☐ Drug abuse, alcoholism or other substance abuse;
- ☐ Records which may indicate the presence of a communicable or non-communicable disease, and tests for records of HIV/AIDS.

Limitations for Release:

- ☐ Only for dates of service from _____ to _____
- ☐ Exclusions ***(must list if there are any exclusions)*** _____
- ☐ Only the following: ***(must list specific documents if applicable)*** _____

INFORMATION TO BE USED FOR THE FOLLOWING PURPOSE(S) ***(List):*** _____

_____

EXPIRATION: This authorization will expire 365 days from the date this form was signed unless one of the following is checked, in which case it will expire on the earliest date:

- ☐ On _____ (cannot be more than 365 days from the date of this form).
- ☐ On _____ when: _____ occurs.
  (Date required) *(identify specific event)*

RIGHT TO REVOKE: I understand that I may revoke this authorization at any time by giving written notice to the organization that was authorized to release this information. I understand that revocation of this authorization will *not* affect any action by the organization that was authorized to release this information before it received my written notice of revocation. I understand that my right to revoke this authorization may be limited if the purpose of this authorization involves applying for health or life insurance.

OTHER RIGHTS: I understand that this information cannot legally be redisclosed by the person or organization that received it without my authorization, except as allowed by law.

I understand that I have the right to inspect my record of protected health information. I also understand that I cannot be denied enrollment or services if I decide not to sign this form. However, I may not be able to apply for benefits or renewal of benefits that would help pay for these services.

SIGNATURE OF CONSUMER OR PERSONAL REPRESENTATIVE:

I, _____, understand that, by signing this form, I am authorizing the use and/or disclosure of the protected health information identified above.

Signature _____ Date _____

Print full name _____

AUTHORITY TO ACT ON BEHALF OF CONSUMER (check one):

Self _____ Parent _____ *Personal Representative _____ (includes legal guardian and power of attorney)
Other _____ **(must specify):** _____

Address: _____ Phone # _____

Supporting documentation required for a personal representative. Attach copy to this form.

SIGNATURE OF MINOR: If the consumer is at least 14 years of age, but under 18 years of age, this authorization is not valid unless the consumer signs in addition to the parent/legal guardian/other personal representative. A minor of any age may authorize disclosure based on his or her signature alone, if (1) he or she is an emancipated minor, or (2) he or she is receiving treatment or services without a parent or legal guardian giving consent.

Signature of Minor _____ Date _____

Print full name _____ DOB _____ Phone # _____

Address: _____

VERIFICATION OF IDENTITY OF CONSUMER OR PERSONAL REPRESENTATIVE PROVIDING CONSENT IS REQUIRED.

- ☐ Personal identification (government issued photo ID) ***Attach a copy.***
- ☐ Government official or Department of Behavioral Health provider's oral representation.

_____

_____

State what you were told and why your reliance on it was reasonable in the circumstances.

If form is mailed in, the signature on the form must be notarized or the person who is providing consent must have his/her signature notarized or attach a copy of his/her government issued ID.

I Have Verified the Identity of the Person Providing Consent.

Signature _____ Date _____

Print Name _____ Title _____

I Revoke this Authorization Effective: _____ **Signature** _____
(Date) ***(Consumer, or personal representative and relationship to consumer)***

TO THE RECORDS CUSTODIAN:

1. Provide a copy of this authorization to the consumer or personal representative.
2. Put signed original in the consumer's clinical record.
3. Log this authorization or forward to the Privacy Officer or designee for logging.
4. Send a copy of this form with the information to be disclosed.

DISCLOSURE LOG

Purpose: This form is used to document each disclosure of protected health information that does not require written authorization (described in Sections 3 and 4 of the DBH Privacy Manual) and unauthorized disclosures (described in Section 1f of the DBH Privacy Manual) that we make for which we are obligated to account on a consumer's request. Forward this form to the agency Privacy Officer or designee no later than within 24 hours.

SECTION A: Consumer whose protected health information was disclosed.

Name: _____ Maiden/Alias: _____

Address: _____

Telephone: _____ Identification Number: _____

SECTION B: Disclosure made.

Disclosure Date: ____/____/_____

Name and Address (if known) of Person or Entity to whom the Protected Health Information Was Disclosed:

_____

Protected Health Information Disclosed: _____

_____

_____

Purpose of the Disclosure: Describe the purpose for disclosing the protected health information, or attach a copy of any written request for the information received from a government agency.

_____

_____

Repetitive Disclosure:

☐ Check if this disclosure is one of a series of repetitive accountable disclosures for a single purpose to the same person or entity. State, if known, the date of the first disclosure of the series, and the frequency, periodicity or number of these repetitive disclosures made prior to the disclosure being reported on this form.

_____

Unauthorized Disclosure (Breach):

☐ Check if this disclosure was an unauthorized disclosure. If disclosure was unauthorized, the Privacy Officer must send a letter to consumer and inadvertent recipient sent via certified mail, (See sample DBH-HIPAA Letters 6.1 & 6.2).

I attest that the above information is correct.

Signature: _____ Date: _____

Print name: _____ Title: _____

NOTIFICATION TO CONSUMER OF UNAUTHORIZED DISCLOSURE

{DATE}

{CONSUMER'S NAME}
{CONSUMER'S ADDRESS}

Dear **{CONSUMER}**:

It is the policy of the Department of Behavioral Health (DBH) to comply with federal and District laws to protect the privacy of consumers' health information that DBH and its participating Network providers create, receive or maintain in their respective roles as health care providers.

Our employees are trained on the importance of using good judgment when using protected health information (PHI) in conversation, by mail, electronic transmission, or any other means, to avoid any unauthorized disclosure of PHI.

If information is disclosed to an entity without authorization, the agency must notify the person whose PHI was disclosed, and the inadvertent recipient.

We regret to inform you that this letter is being sent to notify you that PHI about you was inadvertently disclosed as indicated below:

☐ . A fax containing PHI was sent to an incorrect fax number.

☐ Copies of documents containing your PHI were sent to the wrong person by mistake.

☐ Other: _____.

A summary of the information disclosed follows (include details and date of disclosure):

We are taking the following actions to investigate this unauthorized disclosure, and we have notified the inadvertent recipient of their duty to destroy. We are taking the following actions to prevent further unauthorized disclosures: _____

_____

You may wish to consider taking the following steps to protect yourself: (insert information as appropriate as relevant to type of disclosure). _____

If you have questions or wish to discuss further, please contact **{CONTACT PERSON OR OFFICE}** at **{CONTACT INFORMATION}**

Sincerely,

_____
Privacy Officer or Designee
{ORGANIZATION NAME}

NOTIFICATION TO INADVERTENT RECIPIENT OF UNAUTHORIZED DISCLOSURE

{DATE}

{INADVERTENT RECIPIENT'S NAME OR ORGANIZATION NAME}
{ADDRESS}

Dear **{NAME OF RECIPIENT OR NAME OF ORGANIZATION}**:

It is the policy of the Department of Behavioral Health (DBH) to comply with federal and District laws to protect the privacy of consumers' health information that DBH and its participating Network providers create, receive or maintain in their respective roles as health care providers.

Our employees are trained on the importance of using good judgment when using protected health information (PHI) about our consumers in conversation, by mail, electronic transmission, or any other means, to avoid any unauthorized disclosure of PHI.

If information is disclosed to an entity without authorization, our agency must notify the person whose PHI was disclosed and the inadvertent recipient.

This letter is being sent to notify you that PHI was inadvertently disclosed to you as indicated below:

☐ A fax containing PHI about a consumer was sent to an incorrect fax number.

☐ Copies of documents containing PHI belonging to another person were sent to you by mistake.

☐ Other: _____.

A summary of the information disclosed follows (include information that allows recipient to know what needs to be returned or destroyed, such as consumer name, number of pages, date of disclosure. Do not include any other PHI.):_____

_____

_____

As an inadvertent recipient, you are hereby notified that any further re-disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. Please arrange for the return or destruction of these documents.

If you have questions or wish to discuss further, please contact **{CONTACT PERSON OR OFFICE}** at **{CONTACT INFORMATION}**

Sincerely,

_____
Privacy Officer or designee
{ORGANIZATION NAME}

ACCESS REQUEST FORM

Purpose: This form is used to document a Consumer's request to inspect and/or obtain a copy of his or her protected health information in a designated record set that we maintain or that our business associates maintain for us.

SECTION A: Consumer Requesting Access.

Name: _____ Maiden/Alias: _____

Address: _____ Date of Birth _____

Telephone: _____ Identification Number: _____

TO THE CONSUMER: Please read the following and complete the information requested.

You have the right to inspect and obtain a copy of your protected health information in our designated record sets. To exercise your right of access, please complete Section B.

SECTION B: Protected health information access requested and timeframe.

Please specify the records you wish to access: _____ **and**

Specify timeframe: For dates of service from _____ to _____.

Do you wish to: ☐ Inspect these records? ☐ Obtain a copy of these records?

We will charge you $._____ per page to copy these records. ***(Privacy Officer or designee: fill in charges prior to giving consumer copy of this form).***

Would you like us to make the records available to you: ☐ On paper? ☐ Electronically?

Delivery: (Check one) ☐Do you want to pick-up copies? **OR** Do you want us to: ☐ Mail the copies? If we mail the copies, we will charge you for the postage.

Please list the name and address of each person, including yourself or your personal representative, for whom you want us to make a copy. If you want us to provide access to or a copy of your records to any person other than you or your personal representative, you must provide us with a signed authorization. We can supply you with an authorization form.

_____ _____

_____ _____

Consumer:

Signature: _____ Date: _____

If this request is by a personal representative on behalf of the Consumer, complete the following:

Personal Representative:

Signature: _____ Date: _____

Printed Name: _____

Relationship to Consumer: _____

Notary Public (Complete only if this request is submitted by mail) _____

Transmit the form to the agency Privacy Officer/designee by next business day.

CONSUMER ENTITLED TO A COPY OF THIS REQUEST

Original – Clinical Record

ACCESS REQUEST PROCESSING FORM

To be completed by Privacy Officer or designee.

SECTION A: Access Request Processing

We must respond to an access request within 30 days of its receipt.

Date access request received: ____/____/____

Date appropriate departments and business associates directed to search for requested records: ____/____/____

Departments directed to search designated record sets for the requested records:

_____ _____

_____ _____

Business associates directed to search designated record sets for the requested records:

_____ _____

_____ _____

Section B: Authority to Act on Behalf of Consumer (check one):

Self _____ Parent _____ *Personal Representative _____ (includes legal guardian and power of attorney)
Other _____ **(must specify):** _____

Address: _____ Phone # _____

Supporting documentation required for a personal representative. Attach copy to this form.

Verification of Identity of Consumer or Personal Representative Providing Consent – Required

- ☐ Personal identification (government issued photo ID) ***Attach a copy.***
- ☐ Government official or Network provider's oral representation. _____

_____

_____

State what you were told and why your reliance on it was reasonable in the circumstances.

If form is mailed in, the signature on the form must be notarized or the person who is providing consent must have his/her signature notarized or attach a copy of his/her government issued ID.

I Have Verified the Identity of the Person Providing Consent.

Signature _____ Date _____

Print Name _____ Title _____

SECTION C: Licensed Health Care Professional Determination:

Request: ☐ Approved ☐ Denied

If Denied, reason for Denial: _____

_____

Name and Title of Licensed Health Care Professional _____

Signature: _____ Date: _____

Or attach copy of written determination.

ACCESS REQUEST PROCESSING FORM

SECTION D: Response to Access Request

☐ Access denied on ____/____/____ by transmittal of Denial of Access to Records letter to the Consumer.

Reason for denial: _____

☐ Consumer requested review on ____/____/____of licensed health care professional's recommendation to withhold records based on safety concerns. Attach sheet explaining disposition on review.

☐ Access granted on ____/____/____

☐ Records inspected: ____/____/____

☐ Copy supplied: ____/____/____ Charges: $_____ Paid: ____/____/____

_____ _____

Signature of Privacy Officer or Designee Date

GRANT OF ACCESS TO RECORDS

{DATE}

{CONSUMER'S NAME}
{CONSUMER'S ADDRESS}

Dear **{CONSUMER}**:

We are granting all or part of the request that we received from you on ____/____/____ to inspect and/or obtain a copy of your records. (If we are denying part of your request, you will receive an additional letter from us identifying the records that you requested that we are not providing and the reasons we are not providing them.)

☐ The records you requested are ready for inspection. Please contact **{CONTACT PERSON OR OFFICE}** at **{CONTACT INFORMATION}** to schedule the inspection.

☐ The records you requested are ready for copying. The copying charge will be $_____. Upon receipt of payment of this charge, we will promptly copy the records. Please contact **{CONTACT PERSON OR OFFICE}** at **{CONTACT INFORMATION}** to arrange to have the copy picked up by or mailed to the persons you designated on your authorization. If you want the copies mailed, the fee for postage will be charged to you.

If you have questions or wish to discuss arrangements, please contact me at **{CONTACT INFORMATION}**

Sincerely,

_____

Privacy Officer or designee
{ORGANIZATION NAME}

DIRECTION TO RETRIEVE RECORDS

{DATE}

To: {Business Associate}_____

_____

_____

From: **{ORGANIZATION NAME}**
{PRIVACY OFFICER NAME AND CONTACT INFORMATION}

On ____/____/_____, we received a request from the consumer below to inspect and copy the following records:

_____

_____

We believe you may have some or all of the requested records in a designated record set. Please promptly search your designated record sets, retrieve each of the requested records you find, and transmit those records to me. Please direct your subcontractors to do the same if you believe that they may have any of the requested records in a designated record set that they maintain for you. If you find none, please check the box below. Please sign and return this form to me.

As we must respond to this request by _____/_____/_____, please give this your immediate attention.

Privacy Officer or designee:

Signature: _____

Title: _____

Consumer requesting access:

Name: _____

Address: _____

Telephone: _____ Identification Number: _____

Response to direction to retrieve records:

After a diligent search of designated record sets we maintain for you, we:

☐ Found no records responsive to the consumer's request.

☐ Found the following responsive records and are transmitting these to you:

_____

_____

Signature: _____ Date:_____
(Business Associate Representative)

Title: _____
(Business Associate Representative)

DENIAL OF ACCESS TO RECORDS

{DATE}

{CONSUMER'S NAME}
{CONSUMER'S ADDRESS}

Dear **{CONSUMER}**:

We are denying all or part of the request that we received from you on ____/____/____ to inspect and/or obtain a copy of your records. (If we are granting part of your request, you will receive an additional letter from us with instructions for inspecting and/or obtaining a copy of the records we are providing.) The reasons we cannot accommodate your request are:

- ☐ We do not have the requested records.
- ☐ You may be able to obtain the requested records by contacting: _____.
- ☐ The records you requested were obtained in confidence from a source other than a health care provider, and providing you access to these records is likely to reveal the confidential source.
- ☐ The records were created or obtained in the course of research, and you agreed not to have access to them while the research remains in progress when you gave your authorization to participate in the research.
- ☐ Access is not allowed to psychotherapy notes.
- ☐ Access is not allowed to information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
- ☐ Access is not allowed to PHI maintained by a covered entity subject to the Clinical Laboratory Amendments Act of 1988, 42 USC §263a, or 42 USC §493.3(a)(2).
- ☐ The health care provider is a correctional institution or acting under the direction of a correctional institution and obtaining a copy would jeopardize the health, safety, security, custody or rehabilitation of the individual, other inmates, or other persons at the correctional facility.
- ☐ Other: _____.
- ☐ A licensed health care professional has determined that providing you or your personal representative access to these records is likely to endanger the safety or life or cause substantial harm to you or another; or that the records contain references to persons whose safety or life may be endangered if the access you request were granted. (safety concerns)

If you disagree with the safety concern recommendation of the licensed health care professional to deny access based on safety concerns, you may designate a different licensed health care professional who did not participate in the recommendation to deny you access to review that recommendation.

You may file a complaint about our denial of your access request with us or with the United States Department of Health and Human Services.

If you have questions, wish to discuss the denial or file a complaint, please contact me at **{CONTACT INFORMATION}**.

Sincerely,

_____
Privacy Officer or designee
{ORGANIZATION NAME}

DESIGNATED PERSONNEL AND RECORD SETS

Purpose: This form is used to document the designation of personnel in your department responsible for compliance with requests for access to, amendment of, and disclosure accounting for a consumer's protected health information. It is also used to document the locations and the paths where your department maintains paper or electronic documentation that makes up your department's designated record sets. Designated record sets include those medical and billing records maintained by your department, or those records that your department uses to make decisions about our consumers.

SECTION A: Department.

Department Name: _____

Director: _____

Telephone: _____ E-mail: _____

Location: _____

SECTION B: Designated personnel.

The following department personnel or positions are responsible for the department's compliance with requests for access to, amendment of, and disclosure accounting for protected health information in our department's designated record sets:

_____ _____

_____ _____

SECTION C: Designated record sets.

The file drawers and room locations of paper documentation that is part of the department's designated record sets:

_____ _____

_____ _____

The paths to electronic documentation that is part of the department's designated record sets:

_____ _____

_____ _____

An individual's protected health information may best be retrieved from the department's designated record sets by:

- ☐ Individual name
- ☐ Identification number
- ☐ Other identifiers: _____

SIGNATURE.

I attest that the above information is correct.

Program Director or designee:

Signature: _____ Date: _____

Print name: _____ Title: _____

Transmit this Form to Agency Medical Records Manager and Provide Copy to Privacy Officer/designee

Original – Agency Medical Records Manager/ Copy – DMH Privacy Officer/designee

AMENDMENT REQUEST

Purpose: This form is used for a Consumer's request to amend protected health information in designated record sets that we maintain or that our business associates maintain for us.

SECTION A: Consumer requesting records amendment.

Name: _____ Maiden/Alias: _____

Address: _____

Telephone: _____ Identification Number: _____

TO THE CONSUMER: Please read the following and complete the information requested.

You have the right to request us to amend your protected health information in our designated record sets. We may decline your request if the information is not part of our designated record sets, we did not create the information, we believe the information is complete and accurate, and for certain other reasons. To exercise your right to request amendment, please complete Section B.

SECTION B: Protected health information to be amended.

Please specify the records you wish to amend and the amendment you wish to make: _____

_____

Please state the reason for the amendment: _____

_____

Please list the name and address of each person who you want us to notify of the amendment, should we agree to make the amendment you request. You must provide us with a signed authorization for us to notify these persons. We can supply you with the appropriate authorization form.

_____ _____

_____ _____

Consumer:

Signature: _____ Date: _____

Printed Name: _____

If this request is by a personal representative on behalf of the Consumer, complete the following:

Personal Representative:

Signature: _____ Date: _____

Printed Name: _____

Relationship to Consumer: _____

Notary Public (Complete only if this request is submitted by mail) _____

Transmit this form to the agency Privacy Officer/designee by next business day.

CONSUMER ENTITLED TO A COPY OF THIS REQUEST

AMENDMENT REQUEST PROCESSING FORM

SECTION A: Consumer's amendment request to be completed by Privacy Officer or designee.

We must respond to a Consumer's amendment request within 60 days of receipt.

Date amendment request received: ____/____/____ Date transmitted to Privacy Officer (PO): ____/____/____

Name and title of treating health care professional at Network Provider: _____
Date health care professional contacted by PO: ___/___/____

Request: ☐ Approved ☐ Denied

If Denied, reason for Denial: _____

Signature of treating health care professional: _____ Date: ____/____/____
Or attach copy of written determination.

Response to Consumer required by: _____/_____/_____ Response provided to consumer on: ____/____/____

Extension of response date:
We may take one 30 day extension of our response date by notifying the requester within the original 60 day response period of the reason for the extension and the date on which we will provide our response.

Extension notice sent on: ____/____/____ Response date promised in extension notice: ____/____/____

Reason given for extension: _____

SECTION B: Response to Consumer's amendment request.

☐ Amendment granted on ____/____/____ by DMH-HIPAA Letter 9.1, to the Consumer. Notify (on DMH HIPAA Letter 9.1a) departments, business associates, persons that the Consumer has authorized to receive notice, and others who we know have and may rely on the un-amended records to the Consumer's detriment, as listed below, to amend the records.

☐ Amendment denied on ____/____/____ by transmittal of Denial of Amendment to Records DMH HIPAA Letter 9.2 to the Consumer.

☐ Consumer requested on ____/____/____ that the amendment request and our denial be included in future disclosures of the record. Notify departments and business associates listed below on DMH HIPAA Letter 9.2a to append or link the amendment request and our denial, and any accurate summary of them that the Privacy Officer prepared, to the record for inclusion with future disclosures.

☐ Consumer submitted written disagreement on ____/____/____. Attach written disagreement and notify departments and business associates listed below to append or link the written disagreement, and any accurate summary of it that the Privacy Officer prepared, to the record for inclusion with future disclosures.

☐ We prepared rebuttal to Consumer's written disagreement and sent it to the Consumer on ____/____/____. Attach rebuttal and notify departments and business associates listed below to append or link the rebuttal, and any accurate summary that the Privacy Officer prepared of the Consumer's written disagreement and the rebuttal, to the record for inclusion with future disclosures.

☐ Consumer lodged a complaint on ____/____/____.

Departments, business associates and others to be notified of the grant or denial of the request to amend:

_____ _____

Privacy Officer or designee:
Signature: _____ Date: _____

Print name: _____ Title: _____

GRANT OF AMENDMENT TO RECORDS

{DATE}

{CONSUMER'S NAME}
{CONSUMER'S ADDRESS}

Dear **{CONSUMER}**:

We are granting the request that we received from you on ____/____/____ to amend your records.

We have amended our designated record sets to reflect the amendment on: _____, as follows:

We will notify our business associates and others as appropriate of the amendment. We will also notify the persons for whom you provided a signed authorization allowing us to give notice that your records have been amended.

If you have questions please contact me at **{CONTACT INFORMATION}**.

Sincerely,

_____
Privacy Officer or designee
{ORGANIZATION NAME}

NOTIFICATION TO AMEND RECORDS

{DATE}

TO: {Business Associate}_____

_____

_____

FROM: **{ ORGANIZATION NAME}**
{PRIVACY OFFICER NAME AND CONTACT INFORMATION}

On ____/____/_____, we granted a request from the consumer below or received notice from the covered entity below to amend the following records with the information attached to this letter:

_____

_____

We believe you may have these records in a designated record set you maintain for us. If so, please promptly amend the records by appending the attached amendment to them within five (5) business days. Please direct your subcontractors to do the same if you believe that they may have these records in a designated record set that they maintain for you. Please contact me should you have questions about the amendment.

Sincerely,

_____
Privacy Officer or designee
{ORGANIZATION NAME}

Consumer requesting or covered entity issuing notice to amend record:

Name: _____

DOB: _____ Identification Number: _____

DENIAL OF AMENDMENT TO RECORDS

{DATE}

{CONSUMER'S NAME}
{CONSUMER'S ADDRESS}

Dear **{INDIVIDUAL}**:

We are denying the request that we received from you on ____/____/____ to amend your records. The reasons we have determined that your request should be denied are:

☐ We do not have the records you wish to amend in our designated record sets.

☐ We did not create the records you wish to amend, and we have no basis to believe that the person or entity that did create the records is not available to amend them.

☐ We believe the records you wish to amend are complete and accurate.

☐ The information is not available to inspect.

☐ Other:_____

_____

Your options:

1. You may submit a written statement disagreeing with our decision. If you do, we will append or link your statement to the records you wanted to amend (if we have those records in our designated record sets) for inclusion in future disclosures of those records. We may prepare and send you a rebuttal to your statement. If we do, we will append or link our rebuttal to those same records for inclusion in future disclosures of those records. In the alternative, we may substitute an accurate summary of your written statement and our rebuttal with future disclosures of those records.
2. Instead of submitting a written statement of disagreement, you may ask that your request to amend the records and this denial be appended or linked to those records to be included with future disclosures. We may substitute an accurate summary of your request and this denial with future disclosures.
3. You may file a complaint about our denial of your amendment request with us or with the United States Department of Health and Human Services.

If you have questions, wish to discuss the denial, file a complaint or review your options, please contact me at **{CONTACT INFORMATION}**.

Sincerely,

_____
Privacy Officer or designee
{ORGANIZATION NAME}

NOTIFICATION OF RECORD AMENDMENT DENIAL

Date:

To: {Business Associate}

From: **{ORGANIZATION NAME}**
{PRIVACY OFFICER NAME AND CONTACT INFORMATION}

On ____/____/_____, we denied a request from the consumer below to amend the following records:

☐ The consumer's request to amend these records and our denial are attached.

☐ The consumer submitted a written statement disagreeing with our denial. It is attached along with any rebuttal we prepared.

☐ Attached is an accurate summary of the consumer's request, our denial, any written statement of disagreement from the consumer, and any rebuttal we prepared.

Please append or link these materials to these records in the designated record sets you maintain for us so they may be included as appropriate in future disclosures of these records. Please direct your subcontractors to do the same if you believe that they may have these records in a designated record set that they maintain for you.

Please contact me should you have questions.

Privacy Officer or designee
{ORGANIZATION NAME}

Consumer Requesting Record Amendment:

Name:

DOB: Identification Number:

REQUEST FOR ACCOUNTING OF DISCLOSURES OF PHI

Purpose: This form is used to document a consumer's request for an accounting of disclosures of protected health information that we maintain or that our business associates maintain for us.

SECTION A: Consumer requesting disclosure accounting.

Name: _____ Maiden/Alias: _____

Address: _____

Telephone: _____ Identification Number: _____

SECTION B: To the consumer—Please read the following.

You have the right to an accounting of the disclosures we or our business associates have made of your protected health information (a) without your permission as allowed by law and (b) to the Department of Health and Human Services for privacy compliance purposes. The accounting period is the 6 years prior to your request.

(Privacy Officer or designee, fill in the charges before giving to consumer)

You are entitled to one free disclosure accounting each 12 months. We will charge you $_____ for each additional disclosure accounting you request during the same 12 month period.

To request a disclosure accounting, please complete the signature block below.

Consumer:

I request an accounting of the accountable disclosures of my protected health information between ____/____/____ and ____/____/____. I understand that I am entitled to one free disclosure accounting each 12 months. I agree to pay $_____ for this disclosure accounting if I have already received a disclosure accounting from you within the previous 12 months.

Signature: _____ Date: _____

Printed Name: _____

If this request is by a personal representative on behalf of the consumer, complete the following:

Personal Representative:

Signature: _____ Date: _____

Printed Name: _____

Relationship to Consumer: _____

Transmit this form to the agency Privacy Officer or designee by the next business day.

CONSUMER ENTITLED TO A COPY OF THIS REQUEST

DISCLOSURE ACCOUNTING PROCESSING FORM

SECTION A: Disclosure accounting request processing—to be completed by Privacy Officer or Designee.

We must respond to a disclosure accounting request within 60 days of its receipt.

Date accounting request received: ____/____/____ Date transmitted to Privacy Officer or Designee: ____/____/____

Accounting period: From: ____/____/____ To: ____/____/____

Date of last accounting: ____/____/____

If last accounting was within 12 months of this request, charge consumer $ _____.

Date appropriate departments and business associates directed to account for disclosures: ____/____/____

Departments directed to account for disclosures:

_____ _____

_____ _____

Business associates directed to account for disclosures:

_____ _____

_____ _____

Extension of response date:

We may take one 30 day extension of our response date by notifying the requester within the original 60 day response period of the reason for the extension and the date on which we will provide our response.

Extension notice sent on: ____/____/____ Response date promised in extension notice: ____/____/____

Reason given for extension: _____

SECTION B: Response to accounting request—to be completed by Privacy Officer or Designee.

Disclosure accounting delivered on ____/____/____ by transmittal of DBH HIPAA Letter 10.2, Disclosure Accounting, to the consumer.

Charges assessed were $_____.

Privacy Officer or designee:

I attest that the above information is correct.

Signature: _____ Date: _____

Print name: _____ Title: _____

DIRECTION TO ACCOUNT FOR DISCLOSURES

Date:

To: {Business Associate}_____

_____

_____

From: **{ORGANIZATION NAME}**
{PRIVACY OFFICER NAME AND CONTACT INFORMATION}

On ____/____/_____, we received a request from the consumer below for an accounting of the disclosures of the consumer's protected health information made between ____/____/____ and ____/____/____ (the "accounting period"). Please promptly provide us with an accounting of each disclosure of this consumer's protected health information you have made within the accounting period within five (5) business days.

We do not have to account for disclosures that are exempt from accounting as follows: (a) anything disclosed prior to six (6) years from the date of the request for disclosure, (b) disclosures made within the Network for treatment, payment, or health care operations, (c) disclosures made to the consumer or the consumer's personal representative, (d) disclosures made pursuant to authorization, (e) disclosures made as part of a limited data set, (f) disclosures of de-identified PHI, (g) disclosures to business associates, (h) disclosures that are for national security or intelligence purposes, (i) disclosures made to correctional institutions or other law enforcement officials having lawful custody over an individual, and (j) disclosures made on an emergency basis pursuant to D.C. Official code 7-1203.03 and 42 CFR, Part 2.

For each accountable disclosure, please provide (a) the disclosure date, (b) the name and (if known) address of the person or entity to which the disclosure was made, (c) a description of the protected health information disclosed, and (d) the purpose for which the protected health information was disclosed. Instruct subcontractors to do the same as applicable.

For repetitive disclosures during the accounting period to the same person or entity for a single purpose, you must provide (a) the frequency, periodicity or number of these repetitive disclosures during the accounting period, and (b) the date of the last of these repetitive disclosures during the accounting period.

As we must provide the disclosure accounting by ____/____/____, please give this your immediate attention and provide to me within five (5) business days. Please contact me should you have questions or wish to discuss this request for disclosure information.

Privacy Officer or designee:

Signature: _____

Consumer requesting disclosure accounting:

Name: _____ Maiden/Alias: _____

DOB: _____ Identification Number: _____

DISCLOSURE ACCOUNTING

{DATE}

{CONSUMER'S NAME}
{CONSUMER'S ADDRESS}

Dear **{CONSUMER}**:

The accounting you requested on ____/____/____ of the disclosures of your protected health information that we or our business associates made between ___/___/___ and ___/___/___ is **{ready/enclosed}**. **{Because you have already received a disclosure accounting from us within the last 12 months, we are entitled to charge you for this disclosure accounting. The charge is $_____. Upon receipt of payment, we will send the disclosure accounting to you.}**

The disclosure accounting does not include disclosures we or our business associates made prior to six (6) years from the date of the request for disclosure or disclosures exempt from disclosure accounting requirements.

We have provided for each accountable disclosure (a) the disclosure date, (b) the name and (if known) address of the person or entity to which the disclosure was made, (c) a description of the protected health information disclosed, and (d) the purpose for which the protected health information was disclosed. For repetitive disclosures during the accounting period to the same person or entity for a single purpose, we have provided (a) the frequency, periodicity or number of these repetitive disclosures during the accounting period, and (b) the date of the last of these repetitive disclosures during the accounting period.

If you have questions regarding the disclosure accounting, please contact me at **{CONTACT INFORMATION}**

Sincerely,

_____
Privacy Officer or designee
{ORGANIZATION NAME}

RESTRICTION REQUEST

PURPOSE: This form is used for a consumer's request to restrict the use or disclosure of protected health information for treatment, payment or health care operations, or with specified persons involved with the consumer's care or payment for care.

SECTION A: Consumer Requesting Restriction.

Name: _____ Maiden/Alias: _____

Address: _____

Telephone: _____ Identification Number: _____

TO THE CONSUMER: Please read the following and complete the information requested.

You have the right to request that we restrict our use or disclosure of your protected health information for treatment, payment or health care operations or with persons involved in your care or payment for your care. We do not have to agree to a restriction, but, if we do, we must follow the restriction. Our agreement must be in writing. We will then restrict our use or disclosure of your protected health information as you request. We must agree to a restriction of PHI if you (or a person on your behalf) pays for item or service in full out of pocket. We may, notwithstanding our agreement, use or disclose the restricted information when needed to treat you in a medical/psychiatric emergency, or when required or authorized by law.

You may end a restriction agreement at any time by notifying us in writing. Your protected health information will then no longer be subject to the restriction. To exercise your right to terminate our use or disclosure of your protected health information, please complete DBH-HIPAA Form 11b, Termination of Restriction.

SECTION B: Restriction Requested.

Please specify the protected health information, the use or disclosure of which you want to restrict:

_____

_____

Please state the restriction you want to apply to that protected health information:

_____

_____

Consumer:

Signature: _____ Date: _____

Printed Name: _____

If this request is by a personal representative on behalf of the consumer, complete the following:

Personal Representative:

Signature: _____ Date: _____

Printed Name: _____ Relationship to Consumer: _____

_____ _____

Name of Agency Staff Member who Received Request **Date**

Clinical staff member must transmit this form to the agency Privacy Officer or designee by next business day.

CONSUMER ENTITLED TO A COPY OF THIS REQUEST

RESTRICTION REQUEST PROCESSING FORM

SECTION A:

Clinical Team Consulted and Agreed that Restriction is not Clinically Contraindicated to Restriction.

YES _____ **NO** _____ **If no, explain:** _____

_____

SECTION B:

Response to Restriction Request—to be completed by Privacy Officer or Designee.

☐ Request denied on ____/____/____ by transmittal of Denial of Restriction Request letter to the consumer.

☐ Request granted on ____/____/____ by transmittal of Agreement to Restriction Request letter to the consumer.

Departments and business associates notified of the accepted restriction:

_____ _____

_____ _____

I attest that the above information is correct.

Privacy Officer or Designee:

Signature: _____ Date: _____

Print name: _____ Title: _____

AGREEMENT TO RESTRICTION REQUEST

{DATE}

{CONSUMER'S NAME}
{CONSUMER'S ADDRESS}

Dear **{CONSUMER}**:

Effective as of ___/___/___, we agree to restrict our use or disclosure of your protected health information in accordance with your request received on ____/____/____. We will not use or disclose the protected health information you identified in your request contrary to the restriction you requested as long as this agreement remains in effect, *except* we may use or disclose the restricted information in a medical/psychiatric emergency for your treatment, when you authorize us in writing to use or disclose the information, or when the use or disclosure is required or authorized by law.

You may end this restriction agreement at any time by notifying us in writing. The restriction may also be ended by your clinician if clinically contraindicated, in which case you will be notified in writing. Your protected health information will then no longer be subject to the restriction.

If you have questions or wish further information, please contact me at **{CONTACT INFORMATION}**.

Sincerely,

_____

Privacy Officer or designee
{ORGANIZATION NAME}

NOTIFICATION OF RESTRICTION OF PROTECTED HEALTH INFORMATION

Date:

To: {Business Associate}_____

_____

_____

From: **{ORGANIZATION NAME}**
{PRIVACY OFFICER NAME AND CONTACT INFORMATION}

On ____/____/_____, we agreed to a request from the consumer below to restrict our use or disclosure of the following protected health information:

_____

_____

The restriction that applies to the above protected health information is:

_____

_____

Consumer:

Name: _____

DOB: _____

Identification Number: _____

You must ensure that the above protected health information is neither used nor disclosed in violation of the above restriction. Notify affected subcontractors to do the same. Should the restriction be modified or removed, we will notify you in writing. If you have questions, please contact me.

Sincerely,

_____

Privacy Officer or designee
{ORGANIZATION NAME}

DENIAL OF RESTRICTION REQUEST

{DATE}

{CONSUMER'S NAME}
{CONSUMER'S ADDRESS}

Dear **{CONSUMER}**:

We decline your ____/____/____ request that we restrict our use or disclosure of your protected health information. Your clinician has determined that the restriction is clinically contraindicated. That means we will be permitted to use or disclose the protected health information that we create, receive or maintain about you in accordance with our Privacy Practices Notice that we gave to you.

If you have questions or want to discuss the denial of your restriction request, please contact me at **{CONTACT INFORMATION}**.

Sincerely,

_____

Privacy Officer or designee
{ORGANIZATION NAME}

TERMINATION OF RESTRICTION

SECTION A. Consumer Requests to terminate the following restriction agreement:

_____

Consumer:

Signature: _____ Date: _____

Print name: _____

If this request is by a personal representative on behalf of the consumer, complete the following:

Personal Representative:

Signature: _____ Date: _____

Printed Name: _____ Relationship to Consumer: _____

_____ _____

Name of Agency Workforce Member who Received Request **Date**

SECTION B: Clinician Requests to Terminate Restriction Agreement.

Reason: Clinically Contraindicated to Restriction. Explain:

_____

_____

Clinician Name: _____ Date: _____

Signature: _____

Clinical staff must transmit this form to agency Privacy Officer by next business day.

SECTION C: Termination of Request Processing (completed by Privacy Officer).

Received by Privacy Officer on: _____

Notice of Termination of Restriction Agreement sent to the consumer on _____.

Departments and business associates notified of the termination of restriction agreement: (should conform to the list of departments and business associates above.)

_____

Privacy Officer or Designee:

Signature: _____ Date: _____

Print name: _____ Title: _____

NOTICE OF TERMINATION OF RESTRICTION AGREEMENT

{DATE}

{CONSUMER'S NAME}
{CONSUMER'S ADDRESS}

Dear **{CONSUMER}**:

Based on your request or the decision of your clinician, we are hereby terminating the agreement we made with you on ____/____/____ to restrict our use or disclosure of your protected health information. This termination is effective ____/____/____. After this termination effective date, we will no longer subject any protected health information we may create or receive about you to the restriction agreement. Rather, we will be permitted to use or disclose this protected health information in accordance with our Privacy Practices Notice that we gave to you.

If you have questions or wish further information, please contact me at **{CONTACT INFORMATION}**.

Sincerely,

_____

Privacy Officer or designee
{ORGANIZATION NAME}

NOTIFICATION OF TERMINATION OF RESTRICTION AGREEMENT

Date:

To: {Business Associate}_____

_____

_____

From: **{ORGANIZATION NAME}**
{PRIVACY OFFICER NAME AND CONTACT INFORMATION}

Effective ____/____/_____ we terminated our agreement with the consumer below to restrict our use or disclosure of the following protected health information:

_____

_____

The restriction to which we had agreed with respect to the above protected health information is:

_____

_____

Consumer:

Name: _____

DOB: _____

Telephone: _____ Identification Number: _____

Notify affected subcontractors of same. If you have questions or wish to discuss the matter, please contact me.

Sincerely,

_____

Privacy Officer or designee
{ORGANIZATION NAME}

Confidential Communication Request

Purpose: This form is used for a consumer's request that we use alternative means or an alternative location when communicating about protected health information.

SECTION A: Consumer requesting confidential communication.

Name: _____ Maiden/Alias: _____

Address: _____

Telephone: _____ Identification Number: _____

SECTION B: To the consumer—please read the following and complete the information requested.

You have the right to request that we communicate about all or part of your protected health information by alternative means or to an alternative location. We will accommodate your request (a) if it is reasonable, and (b) you provide reasonable alternative means or location for communicating with you. To exercise this right, please complete this Section B.

Please describe the protected heath information you want to make subject to confidential communication, and if you wish, also include the reason why.

_____

_____

☐ I request that you communicate with me about my protected health information by the following alternative means. Please provide full information on the alternative means you want us to use:

_____

_____

☐ I request that you communicate with me about my protected health information at the following alternative location. Please provide full information on the alternative location:

_____

_____

Consumer:

Signature: _____ Date: _____

Printed Name: _____

If this request is by a personal representative on behalf of the consumer, complete the following:

Personal Representative:

Signature: _____ Date: _____

Printed Name: _____ Relationship to Consumer: _____

SECTION C:

_____ _____

Date Request Received from Consumer Name and signature of agency representative who received request

Transmit this form to the agency Privacy Officer or designee by next business day.

CONSUMER ENTITLED TO A COPY OF THIS REQUEST.

Confidential Communication Request Processing Form

Confidential communication request processing to be completed by Privacy Officer or designee.

Date Agency received request from consumer: ____/____/____

Date received by Privacy Officer: ____/____/____

☐ This request is reasonable and reasonable alternative means of communication were provided. The consumer was notified on ____/____/____ by means and location appropriate to the confidentiality request that the request will be accommodated.

Departments and business associates notified to use alternative means or an alternative location to communicate about protected health information with the consumer.

_____ _____

_____ _____

☐ This request is not reasonable and reasonable alternative means were not provided. The consumer was notified on ____/____/____ by means and location appropriate to the confidentiality request that further information is required before we can accommodate the request.

SIGNATURE.

I attest that the above information is correct.

Privacy Officer or designee:

Signature: _____ Date: _____

Print name: _____ Title: _____

ACCOMMODATION OF CONFIDENTIAL COMMUNICATION REQUEST

{DATE}

{CONSUMER'S NAME}
{ALTERNATIVE LOCATION ADDRESS}

Dear **{CONSUMER}**:

This letter confirms that we will accommodate your request that we communicate about your protected health information by the alternative means or at the alternative location you requested. We will continue to use the alternative means or location you requested until further notice from you. Accordingly, please keep us informed of your need to have us communicate by the alternative means or location you requested.

If you have questions or want to discuss your request further, please contact me at **{CONTACT INFORMATION}**.

Sincerely,

_____

Privacy Officer or designee
{ORGANIZATION NAME}

NOTIFICATION OF CONFIDENTIAL COMMUNICATION REQUIREMENT

Date:

To: {Business Associate}_____

_____

_____

From: **{ORGANIZATION NAME}**
{PRIVACY OFFICER NAME AND CONTACT INFORMATION}

On ____/____/_____, the consumer below requested that we communicate about protected health information by alternative means or at an alternative location. We are required to accommodate this request. Until further notice from us, you must adhere to the following when communicating about protected health information with this consumer:

Protected health information subject to the consumer's confidential communication request:

_____

_____

☐ All communications about the above protected health information must be provided to the consumer by the following means:

_____

_____

_____

☐ All communications about the above protected health information must be sent to the following location:

_____

_____

_____

Notify any affected subcontractors of same. If you have questions, please contact me.

Sincerely,

_____

Privacy Officer or designee
{ORGANIZATION NAME}

Consumer requesting confidential communications:

Name: _____

Address: _____

Telephone: _____ Identification Number: _____

DENIAL OF CONFIDENTIAL COMMUNICATION REQUEST

{DATE}

{CONSUMER'S NAME}
{ALTERNATIVE LOCATION ADDRESS}

Dear **{CONSUMER}**:

We are not able to accommodate your ____/____/____ request that we communicate about your protected health information by the alternative means or at the alternative location you requested. We need the following additional information before we can accommodate your request:

_____

_____

_____

If you still want us to communicate with you about your protected health information by alternative means or location, please provide the additional information required. Until we have it, we will continue to communicate about your protected health information as follows:

_____

_____

_____

Please contact me at **{CONTACT INFORMATION}** with the additional information we need or if you have questions or want to discuss further your desire that we use confidential communications with you.

Sincerely,

_____
Privacy Officer or designee
{ORGANIZATION NAME}

DATA USE AGREEMENT

This data use agreement ("Agreement") is effective upon execution, and is entered into by and between _____ _____ ("Recipient") and Department of Behavioral Health, District of Columbia or other Network provider agency ("Data Provider").

Data Provider and Recipient mutually agree to enter into this Agreement to comply with the requirements of Section 514(e) of the Privacy Rule, 45 Code of Federal Regulations ("C.F.R.") § 164.514(e), issued pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

1. **Provision of Limited Data Set.** Upon Recipient's execution of this Agreement, Data Provider will provide Recipient a Limited Data Set:

   a) that contains the minimum amount of Protected Health Information reasonably necessary for the purposes, as set out in Section 2 of this Agreement, for which Recipient is to receive the Limited Data Set, and

   b) from which all of the direct identifiers, as specified in 45 C.F.R. § 164.514(e)(2), of the individuals whose Protected Health Information is included in the Limited Data Set and of the relatives, household members and employers of those individuals have been removed.

2. **Recipient's Permitted Uses and Disclosures.** Recipient is permitted to use and disclose the Limited Data Set for only the following purposes (which must be limited to Health Care Operations, Public Health Activities, or Research):

   _____

   _____

3. **Prohibition on Unauthorized Use or Disclosure.**

   a) Recipient will neither use nor disclose the Limited Data Set for any purpose other than as permitted by Section 2 of this Agreement, as otherwise permitted in writing by Data Provider, or as Required by Law.

   b) Recipient is not authorized to use or disclose the Limited Data Set in a manner that would violate the Privacy Rule, 45 C.F.R. Part 164, Subpart E.

   c) Recipient will not attempt to identify the information contained in the Limited Data Set or contact any individual who may be the subject of information contained in the Limited Data Set.

4. **Information Safeguards.** Recipient will adopt and use appropriate administrative, physical, and technical safeguards to preserve the integrity and confidentiality of the Limited Data Set and to prevent its use or disclosure, other than as permitted by Section 2 of this Agreement, as otherwise permitted in writing by Data Provider, or as Required by Law in light of the HIPAA Privacy Rules.

DATA USE AGREEMENT

5. **Permitted Recipients, Subcontractors, and Agents.** Recipient will require any agent or subcontractor, to which Recipient is permitted by this Agreement or in writing by Data Provider to disclose and let use the Limited Data Set, to agree by written contract to comply with the same restrictions and conditions that apply to Recipient's use and disclosure of the Limited Data Set pursuant to this Agreement.

In addition to Recipient, the following subcontractors, agents or other recipients are permitted to receive and use the Limited Data Set, provided that they agree to the same restrictions and conditions that apply to Recipient's use and disclosure of the Limited Data Set pursuant to this Agreement:

_____ _____

_____ _____

6. **Breach of Privacy Obligations.** Recipient will report to Data Provider any use or disclosure of the Limited Data Set that is not permitted by this Agreement or in writing by Data Provider. Recipient will make the report to Data Provider's Privacy Officer immediately, but no later than five (5) business days after Recipient learns of such non-permitted use or disclosure. Recipient's report will at least:

   a) Identify the nature of the non-permitted use or disclosure;

   b) Identify the Limited Data Set content used or disclosed;

   c) Identify who made the non-permitted use or disclosure and who received the non-permitted disclosure;

   d) Identify what corrective action Recipient took or will take to prevent further non-permitted uses or disclosures;

   e) Identify what Recipient did or will do to mitigate any deleterious effect of the non-permitted use or disclosure; and

   f) Provide such other information, including a written report, as Data Provider may reasonably request.

7. **Termination for Breach.** Data Provider may terminate this Agreement, and any related agreement, if it determines, in its sole discretion, that Recipient has breached any provision of this Agreement. Data Provider may exercise this termination right by providing Recipient written notice of termination that states the breach of this Agreement that provides the basis for the termination. Any such termination will be effective immediately or at such other date specified in Data Provider's notice of termination. The obligations of Section{s} 3 and 10 of this Agreement will survive termination of this Agreement.

8. **Expiration.** This Agreement will expire on _____. The obligations of Section{s} 3 and 10 of this Agreement will survive expiration of this Agreement.

9. **Return of Limited Data Set.**

   a) Upon termination or expiration of this Agreement, Recipient will, if feasible:

      i) return to Data Provider or destroy the Limited Data Set, and

      ii) obtain from each subcontractor, agent or other recipient, that received the Limited Data Set under Section 5 of this Agreement, the return or destruction of the Limited Data Set.

   The return or destruction must include (a) the Limited Data Set, (b) all copies of the Limited Data Set, and (c) any work derived from the Limited Data Set that may allow identification of any individual whose information is contained in the Limited Data Set, in the custody or under the control of Recipient or of such subcontractor, agent or other recipient, whether in tangible or electronic medium.

Recipient will complete such return or destruction as promptly as possible, but not later than 20 days after the effective date of the termination or expiration of this Agreement, and will within such period certify in writing to Data Provider that such return or destruction has been completed.

b) If return or destruction is not feasible, Recipient will, within 20 days after the effective date of the termination or expiration of this Agreement:

i) provide Data Provider with a written explanation why return or destruction is not feasible, and

ii) certify in writing to Data Provider that Recipient, or subcontractor, agent or other recipient under Section 5 of this Agreement, will neither use nor disclose the Limited Data Set for any purpose other than the purposes that make return or destruction of the Limited Data Set infeasible.

10. Indemnity. Recipient will indemnify and hold harmless Data Provider and any affiliate, officer, director, employee or agent of Data Provider from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees and court or proceeding costs, arising out of or in connection with any non-permitted use or disclosure of the Limited Data Set or other breach of this Agreement by Recipient or any subcontractor, agent, person or entity under Recipient's control.

a) Right to Tender or Undertake Defense. If Data Provider is named a party in any judicial, administrative or other proceeding arising out of or in connection with any non-permitted use or disclosure of the Limited Data Set or other breach of this Agreement by Recipient or any subcontractor, agent, person or entity under Recipient's control, Data Provider will have the option at any time to either (i) tender its defense to Recipient, in which case Recipient will provide qualified attorneys, consultants, and other appropriate professionals to represent Data Provider's interests at Recipient's expense, or (ii) undertake its own defense, choosing the attorneys, consultants, and other appropriate professionals to represent its interests, in which case Recipient will be responsible for and pay the reasonable fees and expenses of such attorneys, consultants, and other professionals.

b) Right to Control Resolution. Data Provider will have the sole right and discretion to settle, compromise or otherwise resolve any and all claims, causes of actions, liabilities or damages against it, notwithstanding that Data Provider may have tendered its defense to Recipient. Any such resolution will not relieve Recipient of its obligation to indemnify Data Provider under this Section {10}.

11. General Provisions.

a) Definitions. The terms "Health Care," "Limited Data Set," "Protected Health Information," and "Research" have the meanings defined in the DBH Privacy Manual. The term "Public Health Activities" has the meaning set out in, 45 C.F.R. § 164.512(b).

b) Amendment to Agreement. Upon the compliance date of any final regulation or amendment to a final regulation, promulgated by the U.S. Department of Health and Human Services pursuant to the Administrative Simplification provisions of HIPAA Title II, Subtitle F, that affects Limited Data Sets, this Agreement will automatically amend such that the obligations imposed on Recipient remain in compliance with the final regulation and the Mental Health Information Act, unless either party elects to terminate this Agreement by providing written notice of termination to the other party at least 90 days before such compliance date. The obligations of Section {9} of this Agreement will apply to such termination, and the obligations of Section{s} 3 {10} of this Agreement will survive such termination.

12. Conflicts. The terms and conditions of this Agreement will override and control any conflicting term or condition of any other agreement between the parties to the extent that such conflicting term or condition affects Limited Data Sets.

DATA USE AGREEMENT

IN WITNESS WHEREOF, Data Provider and Recipient execute this Agreement in multiple originals to be effective on the last date written below.

Recipient	**Department of Behavioral Health – District of Columbia, or other Network Provider Agency (Data Provider)**
By: _____	By:
Its: _____	Its: _____
Date: _____	Date: _____

Complaint Form

Purpose: This form is used for a consumer to lodge a complaint about our privacy practices or compliance.

To the consumer lodging complaint:

You have the right to file a complaint with us about our privacy practices or our compliance with our Privacy Practices Notice, DBH Privacy Manual, or federal or DC privacy rules or law. We will investigate your complaint and provide you our written response. We will not require you to waive any right you may have under federal or DC privacy or other law to file your complaint, nor will filing your complaint adversely affect our treatment of you. To exercise this right, please complete Sections A and B below, sign and date, then submit this complaint to your agency's Privacy Officer at:

Address: _____

Telephone: _____

Fax: _____

Email: _____

If you have questions, need additional information or assistance in completing your complaint, please contact us at the above location. You may, in addition or in the alternative to filing a complaint with your agency's Privacy Officer, file a complaint with the DBH Privacy Officer, the District-wide Privacy and Security Official, or the United States Department of Health and Human Services. For information on the procedures for doing that, please contact us at the above location.

SECTION A: Consumer lodging complaint.

Name: _____ Maiden/Alias: _____

Address: _____

Telephone: _____ Identification Number: _____

SECTION B: Consumer's complaint.

Please give a concise, plain statement of your complaint:

_____

_____

_____

_____

_____

_____

Complaint Form

Please give a concise, plain statement of the resolution you seek for your complaint:

_____

_____

_____

_____

_____

_____

_____

Consumer:

I certify that the statements made in this complaint are true and correct to the best of my information and belief.

Signature: _____ Date: _____

Printed Name: _____

If this complaint is lodged by a personal representative on behalf of the consumer, complete the following:

Personal Representative:

Signature: _____ Date: _____

Printed Name: _____

Relationship to consumer: _____

Name of Staff Person who Received Form: _____ **Date Received** _____

Signature of Staff Person who Received Form: _____

Agency Name _____ **Agency Phone Number** _____

Transmit this form to the agency Privacy Officer or designee immediately.

CONSUMER IS ENTITLED TO A COPY OF THIS COMPLAINT.

Complaint Investigation and Processing Form

The Privacy Officer or designee will respond to the complaint on the organization's behalf and will proceess the complaint within 10 business days of receipt by the agency. See page 17.1 of privacy manual.

Date agency Privacy Officer received complaint: ____/____/____

Investigation undertaken: _____

_____

_____

_____

_____

Findings and Conclusions: _____

_____

_____

_____

If noncompliance found, corrective action instituted (including sanctioning any workforce member violating privacy policies and procedures, privacy rules or other federal or DC law, and reducing any harmful effect of the noncompliance):

_____

_____

_____

_____

Complaint Response Letter sent to consumer on ____/____/____. Attach copy of the Complaint Response Letter 14.1.

Matter concluded and closed on ____/____/____.

I attest that the above information is correct.

Privacy Officer or designee:

Signature: _____ Date: _____

Print name: _____ Title: _____

Original – Clinical Record/Copy – Privacy Officer & OCFA

COMPLAINT RESPONSE LETTER

{DATE}

{CONSUMER'S NAME}
{CONSUMER'S ADDRESS}

Dear **{CONSUMER}**:

We have completed our investigation of the complaint you filed with us on ____/____/____ regarding our privacy practices or our compliance with our Joint Notice of Privacy Practices, DBH Privacy Manual, or federal or DC privacy laws. We have concluded that your complaint **{has merit/is without merit}** for the following reasons:

_____

_____

_____

_____

_____

___ **Because we found no merit in your complaint, we are closing our file on the matter without further action.**

___ **We have implemented the following corrective action to resolve the matters about which you complained:**

_____

_____

_____.

If you are dissatisfied with our resolution of your complaint, you may complain to the DBH Privacy Officer, District-wide Privacy and Security Official or the U.S. Department of Health and Human Services. Please contact me at **{CONTACT INFORMATION}** if you want information or if you have questions or want to discuss further our resolution of your complaint.

Sincerely,

_____
Privacy Officer or designee
{ORGANIZATION NAME}

CONFIDENTIALITY AND SECURITY OF PROTECTED HEALTH INFORMATION

Protected health information (PHI) means any written, recorded, electronic (ePHI), or oral information which either (1) identifies, or could be used to identify, a consumer; or (2) relates to the physical or mental health or condition of a consumer, provision of health care to a consumer, or payment for health care provided to a consumer. Laws governing the confidentiality and security of PHI include HIPAA (Health Insurance Portability and Accountability Act of 1996) and 42 CFR Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records, under federal law, and the MHIA (Mental Health Information Act of 1978 as amended) and Data-Sharing and Information Coordination Amendment Act of 2010 under District law.

District of Columbia and federal laws require that PHI of all present and former consumers be kept confidential, subject to specific allowable uses and disclosures, and that PHI be appropriately safeguarded from unauthorized access.

I understand that mental health information, and alcohol/drug treatment and prevention information that is maintained by an alcohol/drug treatment and prevention program, is subject to greater restrictions than general health information in accordance with the MHIA, and 42 CFR Part 2 respectively.

I understand that I hold a position of trust relative to PHI owned and/or maintained by the District of Columbia in all formats and computer systems and I have a responsibility to preserve the confidentiality and security of such information.

Accordingly, I understand that I am prohibited from engaging in inappropriate conduct, which may include, but is not limited to, the types of actions listed below:

- Release of any PHI without the appropriate authorization, unless the release is specifically allowed under District or federal law.
- Inappropriate discussion or display of PHI in public areas.
- Failing to safeguard physical locations where PHI is available.
- Failing to safeguard PHI that is carried or maintained in my possession.
- Knowingly gaining, attempting to gain, causing access to, or permitting unauthorized use of or disclosure of any PHI owned and/or maintained by the District of Columbia in all formats and computer systems.
- Using, attempting to use, causing or permitting the use of PHI owned and/or maintained by the District of Columbia in all formats and computer systems for personal gain or motive.
- Knowingly including or causing to be included any false, inaccurate, or misleading entry into any publicly funded computer system.
- Removing or causing to be removed, without proper reason and authorization, any necessary and required information owned and/or maintained by the District of Columbia in all formats and computer systems.
- Abiding, abetting, or acting in conspiracy with another to violate this agreement.
- Divulging my access codes to anyone.
- Disclosure of information from an alcohol/drug treatment and prevention program that identifies a consumer as having a current or past drug/alcohol problem, unless the consumer consents or an exception applies as permitted by 42 CFR, Part 2.

I agree to adhere to the DBH Privacy Policies and Procedures regarding the protection of PHI. Any unauthorized or inappropriate use of PHI owned and/or maintained by the District of Columbia in all formats and computer systems, by the user or by another who has inappropriately been permitted or enabled access to the system by the user, may subject the user to criminal and civil sanctions pursuant to federal and state law as well as disciplinary action up to and including removal.

- MHIA violations can lead to civil penalties for damages and costs, and criminal penalties to include a fine of up to $5,000 and up to 90 days in jail.
- HIPAA violations can lead to civil penalties to include a fine up to $50,000 per violation with a calendar year cap of $1,500,000, and criminal penalties to include a fine up to $250,000 and up to 10 years in jail.
- Data Sharing Act violations can lead to civil penalties up to $1,000 for each violation, and criminal penalties up to $5,000, up to 180 days in jail, or both.
- Confidentiality of alcohol/drug record violations may result in criminal penalties to include a fine of up to $500 for 1st offense, and up to $5,000 for each subsequent offense.

I acknowledge that I have received a signed copy of this document.

Name of Employee (print) _____ **Program/Organization** _____

Signature of Employee _____ **Date** _____

Questions related to this form or PHI may be directed to the DBH Privacy Officer.