



Chapter: Information Management and Information Technology
Subject: Confidentiality and HIPAA

Applicability: DBHDD, including the state office, regional offices, state operated DBHDD hospitals and any state operated community programs.

Effective Date: September 1, 2011
Full Implementation Date: November 1, 2011
Next Review Date: September 2013

Approved:

Attachments: Attachment A: Notice of Privacy Practices
Attachment B: Authorization for Release of Information

Signature of Elizabeth Bentley Watson, Esq. dated 8/22/11
Privacy Officer

Signature of Frank E. Shelp, M.D., M.P.H., Commissioner dated 8/22/11

POLICY

The right of an individual to confidentiality and privacy of his/her health care information, including information about mental health, developmental disabilities, or addictive disease, is protected by state laws and regulations and by federal laws and regulations. Individuals also have certain legal rights regarding access to their own records and information.

It is the policy of the Department of Behavioral Health and Developmental Disabilities (DBHDD) to ensure compliance with applicable state and federal laws and regulations regarding confidentiality and privacy. These laws and regulations govern topics including but not limited to:

- Mental health information
Developmental disability information
Addictive disease information
Protected health information (PHI) as defined by HIPAA
Rights of individuals regarding their protected health information
Notice of Privacy Rights
Disclosures of protected health information
Reporting of violations and breaches, and resulting sanctions
Complaints
Business Associates
Accounting of disclosures
AIDS confidential information
Medicare/Medicaid information
Open Records Act requests.

When there is a conflict between state and federal law, DBHDD shall seek legal counsel regarding the conflict. Generally, DBHDD will follow the law which provides greater

DBHDD	SUBJECT: Confidentiality and HIPAA	Policy 23-100
		Page 2 of 14

access to and rights of the individual, or which provides the greatest protection of confidentiality and privacy. HIPAA does not supersede or negate more stringent federal and state laws, rules and regulations. In the event of an apparent conflict in laws, or between the confidentiality laws regarding any specific program and the terms of this policy, the responsible employee shall seek direction from Legal Services.

Unless otherwise specifically stated, DBHDD policy and procedures regarding confidentiality do not compel or require disclosure. If there is an exception to the rule of confidentiality and a disclosure is allowed, such disclosure is not required unless a law, rule or regulation, or DBHDD policy or procedure states that the disclosure is required.

APPLICABILITY

State laws and regulations on confidentiality of mental health, developmental disabilities, and addictive disease information, as well as other health information, govern the Department of Behavioral Health and Developmental Disabilities (DBHDD) and its facilities, as defined herein. DBHDD is also a “covered entity” as defined in, and as governed by, the Health Insurance Portability and Accountability Act of 1996 and its regulations (HIPAA).

This policy is therefore applicable to any facility or program that is a part of DBHDD, including the state office, regional offices, state operated DBHDD hospitals and any state operated community programs. All employees, agents, trainees, volunteers and contractors of DBHDD shall abide by federal and state laws and regulations regarding confidentiality, relevant DBHDD policies and procedures, and all federal laws regarding the disclosure and use of confidential and protected health information. DBHDD providers, as defined herein, who are under contract or have a letter of agreement with DBHDD through DBHDD and its Regional Offices have an independent duty to follow state confidentiality laws; if they are also covered entities under HIPAA, they have an independent duty to follow HIPAA and its regulations. If they also conduct business functions on behalf of DBHDD, they are also business associates of DBHDD and must comply with applicable provisions of the HIPAA through a Business Associate Agreement with DBHDD.

This policy and associated forms are available as resources for providers, but DBHDD makes no representation or warranty that compliance with the provisions of this policy will ensure a provider's compliance with all applicable laws and regulations. Providers should seek their own legal counsel regarding compliance with laws and regulations on the subject matter of this policy.

DEFINITIONS

Unless a different meaning is required by the context, the terms as used in this policy and procedures and in all DBHDD policies and procedures regarding confidentiality and

DBHDD	SUBJECT: Confidentiality and HIPAA	Policy 23-100
		Page 3 of 14

HIPAA shall have the following meanings:

Accounting of disclosures – A history of when and to whom disclosures of protected health information are made for purposes other than treatment, payment, and health care operations and certain other exceptions.

Advance directive for health care – A document voluntarily executed by an individual in accordance with O.C.G.A. § 31-32-5. A living will or a durable power of attorney for health care may be an advance directive.

AIDS confidential information – Information which permits identification of an individual and discloses that the individual;

- Has been diagnosed as having Acquired Immunodeficiency Syndrome (AIDS) or AIDS Related Complex (ARC)
- Has been or is being treated for AIDS
- Has been determined to be infected with any type of Human Immunodeficiency Virus (HIV) as defined in Georgia law
- Has submitted to an HIV test
- Has had a positive OR a negative result from an HIV test
- Has sought and received counseling regarding AIDS, **OR**
- Has been determined to be a person at risk of being infected with AIDS.

Authorization – Permission by an individual or a person legally authorized to consent on the individual's behalf, to the release or use of protected health information relating to the individual.

Breach – The acquisition, access, use or disclosure of protected health information in a manner not permitted by HIPAA or this policy which compromises the security or privacy of the protected health information.

Business associate – A person or entity who is not a member of DBHDD's workforce and who, on behalf of DBHDD, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information.

Chief Medical Officer – The physician with overall responsibility for treatment or habilitation services at a facility or a physician appointed in writing as the designee of such chief medical officer.

Clinical record – A written record pertaining to an individual, including all medical records, progress notes, charts, admission and discharge data, and all other information recorded by a facility or other entities responsible for an individual's care and treatment or habilitation, and pertaining to the individual's hospitalization and treatment or habilitation. Such other information as may be required by rules and regulations of DBHDD shall also be included. The clinical record may be maintained electronically.

DBHDD	SUBJECT: Confidentiality and HIPAA	Policy 23-100
		Page 4 of 14

Confidential – The property that data or information is private and is not made available or disclosed to persons who are not authorized to access such data or information.

Confirmed positive HIV test – The results of at least two separate types of HIV tests, both of which indicate the presence of HIV.

Court – In the case of an individual who is 17 years of age or older, the probate court for the county of residence of the individual or the county in which such individual is found, and, in the case of an individual who is under the age of 17 years, the juvenile court for the county of residence of the individual or the county in which such individual is found.

Covered entity – A health care provider, health plan, or health care clearinghouse that transmits any health information in electronic form in connection with a HIPAA transaction; DBHDD is a covered entity.

De-identified information – Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

Department – The Georgia Department of Behavioral Health and Developmental Disabilities (DBHDD), including its duly authorized agents and designees.

Designated record set – A group of records maintained by or for DBHDD that is used, in whole or in part, by or for DBHDD to make decisions about individuals, including but not limited to clinical and billing records.

Determined to be infected with HIV – Having a confirmed positive HIV test or having been clinically diagnosed as having AIDS.

Diagnosis (with regard to alcohol or drug abuse) – Any reference to an individual’s alcohol or drug abuse or to a condition which is identified as having been caused by that abuse which is made for the purpose of treatment or referral for treatment.

Direct treatment relationship – A treatment or service relationship between an individual and a health care provider that is not an indirect treatment relationship. In an indirect treatment relationship, the health care provider delivers health care to the individual based on the order of another health care provider and the health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

Disclosure – The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information. Disclosure includes the affirmative verification of another person’s communication of individually identifiable health information, or the communication of any information from the record of an individual who has been identified. “Release” also means disclosure, for purposes of this policy.

DBHDD	SUBJECT: Confidentiality and HIPAA	Policy 23-100
		Page 5 of 14

Facility – Any hospital, community mental health center, or other facility that is state owned or state operated and is utilized for the diagnosis, care, treatment, or hospitalization or services of individuals for mental illness, developmental disability or addictive disease.

Guardian – A person appointed by written court order to be legally responsible for the person of an adult or of a minor. The individual for whom a guardian is appointed is known as the “ward.” Whenever “individual” is used in confidentiality and HIPAA policies and procedures, a guardian is entitled to exercise the individual’s rights on behalf of the individual (ward). “Guardian” as used in this policy does not include a conservator or a guardian of property alone.

Health and Human Services (HHS) – The federal government department that has overall responsibility for implementing HIPAA.

Health care – Care, services, or supplies related to the health of an individual. 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 an individual or that affects the structure or function of the body; and
- (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care agent – A person appointed by an individual to act for and on behalf of an individual, as set forth in an advance directive for health care executed by the individual.

Health care provider – A provider of health care services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. NOTE: For purposes of this policy, the term “health care provider” follows the definition in HIPAA and refers to all health care providers generally. This term is not limited to those providers who have contracts, letters of agreement, or other legal or funding arrangements with DBHDD. **See** the separate definition of “provider” in this policy.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) – Public Law 104-191– A Federal law that governs the use, access, and disclosure of protected health information (see definition) regarding individuals. HIPAA gives HHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care consumers, health care providers, payers, and employers; to specify the types of measures required to protect the security and privacy of personally identifiable health care information; and to specify requirements for reporting breaches of HIPAA to HHS and others. As defined in DBHDD confidentiality and HIPAA policies and procedures, HIPAA refers to the federal act and also to related federal regulations known as the Privacy Rule, the Security Rule, and

DBHDD	SUBJECT: Confidentiality and HIPAA	Policy 23-100
		Page 6 of 14

regulations implementing the “Health Information Technology for Economic and Clinical Health Act” (“HITECH Act”), located at 45 CFR Parts 160, 162, and 164.

Individual – Any person who is seeking, applying for, currently receiving, or formerly received treatment or services from DBHDD or any of its state operated facilities or programs or providers, for mental illness, developmental disability, or addictive disease or co-occurring combinations thereof. For purposes of this Policy, “individual” means the person who is the subject of protected health information.

Individually identifiable health information – Any information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual, and identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. Individually identifiable health information contains some or all of the following elements:

- Name
- All address information
- Zip codes
- E-mail addresses
- Dates (except year) directly related to an individual, including dates of birth, admission, discharge, death
- Age, if over 89 years
- Telephone numbers
- Fax numbers
- Social Security number
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate numbers
- License numbers
- Device identifiers
- URLs
- IP addresses
- Facial photographs
- Biometric identifiers
- Any other unique identifying number, characteristic, or code

Minimum necessary – When using or disclosing protected health information or when requesting protected health information, the process of making reasonable effort to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

Notice of Privacy Practice – A notice that provides a clear explanation of DBHDD’s privacy practices and the privacy rights of individuals regarding their personal health information.

DBHDD	SUBJECT: Confidentiality and HIPAA	Policy 23-100
		Page 7 of 14

Person at risk of being infected with HIV – Any person who may have already come in contact with or who may in the future be reasonably expected to come in contact with the body fluids of an HIV infected person.

Person legally authorized to sign – A person authorized by law to give authorization for release of an individual's protected health information. These persons include: for minors, the parent, the court-appointed guardian or the court-appointed custodian; for adults, the court-appointed guardian of the person, if any. An individual may give his/her agent in an advance directive the authority to sign for release of the individual's protected health information, except for alcohol or drug information.

Personally identifying information – Any item, collection or grouping of information which contains the name of an individual or any unique grouping of information which makes an individual identifiable as if a name were affixed (such as address, telephone number, individual diagnosis, etc.).

Privacy – HIPAA regulations protect an individual's right to the privacy or confidentiality of his/her health care information to keep it from falling into the hands of people who are not legally authorized to obtain it. The HIPAA privacy regulations require health care providers to obtain a signed authorization to disclose PHI, unless otherwise authorized by applicable law or regulation.

Privacy Coordinator – The individual designated by a state hospital or Regional Office with responsibility for obtaining and maintaining a working knowledge of DBHDD's confidentiality and security policies and procedures, to respond to confidentiality and HIPAA-related inquiries arising within the hospital or region, provide information regarding the complaint process and the reporting process, and maintain adequate documentation of these activities.

Privacy Officer – The individual designated by DBHDD with responsibility for obtaining and maintaining a working knowledge of the Department's confidentiality and privacy policies and procedures, to respond to confidentiality and HIPAA-related inquiries arising within DBHDD, provide information regarding the complaint process and reporting process, and maintain adequate documentation of these activities. The Privacy Officer also has responsibility for coordination of Privacy Coordinators and for overseeing certain HIPAA-related reporting.

Privacy Rule – Standards for Privacy of Individually Identifiable Health Information, which implements the privacy requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) at 45 CFR parts 160 and 164.

Privileged – Protected by law from unauthorized disclosure. Privilege gives the legal right to an individual to prevent disclosure of communications between the individual and his/her: psychiatrist, licensed psychologist, or between an individual and his/her licensed

DBHDD	SUBJECT: Confidentiality and HIPAA	Policy 23-100
		Page 8 of 14

clinical social worker, clinical nurse specialist in psychiatric/mental health, licensed professional counselor or licensed marriage and family counselor during psychotherapy.

Protected Health Information (PHI) – All individually identifiable health information (e.g., name, diagnosis, medical record number, billing information, etc.) that is transmitted or maintained by a covered entity in any form or medium, including orally. **See** “individually identifiable health information,” above. Protected health information excludes education records covered by the Family Educational Rights and Privacy Act (FERPA) and employment records held by DBHDD in its role as employer.

Provider – Organizations or persons approved to serve individuals with mental illness, developmental disabilities and/or addictive diseases, wherein those services are financially supported in whole or in part by funds authorized through DBHDD. Providers typically have a contract or letter of agreement with DBHDD. (NOTE: For purposes of this policy, the term “provider” means only those entities which have contracts, letters of agreement or other legal or funding arrangements with DBHDD. **See** the separate and more general definition for “health care provider” as that term is used in this policy.)

Psychotherapy notes – Notes recorded in any medium by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's clinical record. Psychotherapy notes excludes medication and prescription monitoring, counseling session 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, treatment plan, symptoms, prognosis, and progress to date.

Records – Any information, whether recorded or not, received or acquired in connection with an individual's treatment or services. "Records" includes administrative and other documentation (such as incident reports) that relates to and identifies an individual, regardless of whether it is part of the individual's clinical record.

Record holder – The health care provider of treatment or services that maintains records or clinical records.

Release – See definition of “disclosure.”

Representatives – The persons designated under Title 37 of the Georgia Code to receive certain notices and, unless objected to by the individual, to consult with the facility regarding the individual's individualized plan and treatment under such plan.

Security Officer – The individual designated by DBHDD with responsibility for obtaining and maintaining a working knowledge of the HIPAA Security Rule and, as appropriate, the Department's confidentiality and security policies and procedures, to respond to inquiries regarding the Security Rule arising within the Department, provide information regarding the security complaint process and reporting process, and maintain adequate

DBHDD	SUBJECT: Confidentiality and HIPAA	Policy 23-100
		Page 9 of 14

documentation of these activities. With the Privacy Officer, has responsibility for coordination of Privacy Coordinators and for certain Security Rule related reporting.

State - The State of Georgia.

Workforce – Employees, volunteers, trainees, and other persons under the direct control of DBHDD, whether or not they are paid by DBHDD.

PROCEDURES

- A. DBHDD shall implement policies and procedures that are designed to comply with confidentiality laws and HIPAA. Policies and procedures shall be reasonably designed and take into account the size and type of activities that relate to PHI undertaken by DBHDD. These policies and procedures shall:
1. Restrict access and use based on specific roles of members of DBHDD's workforce;
 2. Establish criteria to limit routing disclosures to minimum necessary to achieve the purpose of the disclosure;
 3. Limit requests to other covered entities to what is reasonably necessary for the particular use or disclosure; and
 4. Control when staff requests or discloses the entire clinical record. There must be specific justification of the need for the entire clinical record.
- B. DBHDD shall document confidentiality and HIPAA privacy policies and procedures, either on paper or in electronic form. Any change to a policy or procedure shall be documented. In addition to policies and procedures, any correspondence or other documents required to be created or maintained by DBHDD under such policies and procedures shall be maintained on file for six years, or longer if required under other applicable laws, regulations or policies.
- C. It is the policy of DBHDD that all information about individuals, whether oral or written and regardless of the form or location in which it is maintained, is confidential and may be disclosed only in accordance with applicable state and federal laws and regulations. DBHDD shall not confirm or deny whether an individual is receiving or has received services, unless such disclosure is authorized in writing by a valid authorization signed by the individual or authorized by applicable law.
- D. DBHDD shall maintain a clinical record for each individual. When disclosure is allowed, the original clinical record may be examined only under supervision by designated staff of the facility, at the facility which maintains custody of the record, at reasonable times as determined by the facility. The original clinical record shall not be removed from the facility unless authorized by an attorney in the Office of the Attorney General or specially appointed assistant attorney general representing DBHDD. The clinical record shall not be a public record.

DBHDD	SUBJECT: Confidentiality and HIPAA	Policy 23-100
		Page 10 of 14

- E. DBHDD shall establish standards relating to uses and disclosures, and de-identification and re-identification of PHI it creates, collects and maintains.
- F. Any disclosure authorized by law or any unauthorized disclosure of confidential or privileged information about an individual or communications shall not in any way abridge or destroy the confidential or privileged character of the information disclosed, except for the purpose for which such authorized disclosure is made. Any person making a disclosure authorized by law shall not be liable to the individual or any other person.
- G. DBHDD shall have administrative, technical and physical safeguards to protect the privacy of PHI. DBHDD shall have safeguard standards and access controls for PHI it collects and maintains.
- H. DBHDD shall provide adequate notice to individuals of the uses and disclosures of PHI it may make by providing a Notice of Privacy Practices to persons seeking or receiving services. DBHDD shall document its compliance with the notice requirements by retaining copies of the notices it issues. DBHDD shall not require individuals to waive their rights as provided in the notice as a condition of treatment, payment or eligibility for benefits.
- I. DBHDD will establish and implement minimum necessary requirements for uses and disclosures of PHI. DBHDD shall make reasonable efforts to limit PHI used, disclosed or requested from another covered entity to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
- J. DBHDD shall obtain a written authorization for release of information from an individual before using or disclosing PHI relating to the individual for any purpose not otherwise permitted or allowed by confidentiality laws or HIPAA. DBHDD shall maintain policies and procedures governing the form of authorization for release of information, and the procedures for making authorized disclosures.
- K. DBHDD shall maintain policies and procedures to protect the confidentiality of alcohol and drug abuse information as governed by federal law and regulations. It is the policy of DBHDD that an individual with alcohol or drug abuse records may be entitled to protections of the confidentiality of such information that are more stringent than the protections provided by HIPAA or by state law. Records pertaining to alcohol abuse or drug abuse may be produced in response to a court order issued by a court of competent jurisdiction pursuant to a full and fair show cause hearing, except for matters privileged under the laws of this state. Records pertaining to alcohol abuse or drug abuse shall not be produced in response to a subpoena alone. Records which are produced must bear notice to the recipient concerning restrictions on further use or disclosure by the recipient.
- L. DBHDD shall maintain policies and procedures to protect the confidentiality of AIDS confidential information, as that term is defined by law, including but not

DBHDD	SUBJECT: Confidentiality and HIPAA	Policy 23-100
		Page 11 of 14

limited to procedures for making authorized disclosures in accordance with applicable laws.

- M. DBHDD shall have a method to allow individuals to exercise their right to request that DBHDD amend PHI or a record about the individual in a designated record set used in whole or in part to make decisions about the individual, for as long as DBHDD maintains the PHI in the designated record set.
- N. DBHDD shall maintain policies and procedures to permit an individual to request a restriction of disclosures. DBHDD is not required to agree with the restriction.
- O. DBHDD shall establish policies and procedures for an individual to access and inspect his/her PHI in a designated record set for as long as DBHDD maintains the PHI in the designated record set. DBHDD shall provide for state law exceptions limiting an individual's access to his/her PHI under certain circumstances when the individual is currently an inpatient of a facility.
- P. DBHDD shall keep an accounting of when and to whom disclosures of PHI are made for purposes other than treatment, payment and health care operations, and shall be able to give an accounting of those disclosures to an individual, if requested. Authorizations from an individual to DBHDD are included in the information that is to be tracked and accounted for. A disclosure of PHI that does not require an authorization may, in some cases, have a tracking and accounting requirement.
- Q. DBHDD shall maintain policies and procedures:
 1. for representatives of individuals, as defined in Title 37 of the Georgia Code, to be named by individuals or by DBHDD;
 2. for certain required disclosures to representatives; and
 3. for certain disclosures to and consultation with representatives, unless the individual objects.
- R. DBHDD shall obtain from its business associates reasonable assurances that they will appropriately safeguard PHI disclosed by DBHDD and that agents, employees and subcontractors of the business associates agree to the same conditions applicable to the business associates with respect to such information. DBHDD shall include HIPAA compliance requirements in contracts, other written agreements and expressions of understanding, with business associates to whom DBHDD discloses PHI.
- S. DBHDD shall mitigate, to the extent practicable, any known harmful effect resulting from a use or disclosure of PHI by DBHDD or a business associate, provided such disclosure is in violation of DBHDD policies and procedures or the requirements of the confidentiality laws or HIPAA.
- T. DBHDD shall develop and communicate to individuals a process for filing complaints about the department's privacy practices or perceived violations of

DBHDD	SUBJECT: Confidentiality and HIPAA	Policy 23-100
		Page 12 of 14

confidentiality laws or HIPAA. Such process shall include expectations regarding cooperation with investigations regarding complaints and for reporting as required for compliance reviews.

- U. DBHDD shall have policies and procedures documented so that employees are aware of what actions are prohibited and punishable. Such policies and procedures shall provide for sanctions that comply with the HIPAA standard for sanctions against members of DBHDD’s workforce who fail to comply with its privacy policies and procedures. Appropriate sanctions shall be imposed for violations of DBHDD’s privacy policies and procedures, or related protocols, standards or directives. DBHDD policies and procedures shall provide appropriate protection for whistleblowers. Sanctions that may be imposed by DBHDD are cumulative of those that may be imposed by statute or regulation.

- V. Neither DBHDD or its employees, workforce members, or agents, shall intimidate, threaten, coerce, harass, discriminate against, or take other retaliatory action against any individual or other person for:
 - Exercising any right established, or for participation in any process provided for, by DBHDD policies and procedures regarding confidentiality and HIPAA;
 - Filing a complaint regarding DBHDD policies or procedures or compliance with such policies or procedures;
 - Testifying, assisting, or participating in an investigation, compliance review, proceeding, or administrative hearing regarding violations of HIPAA;
 - Opposing any act or practice made unlawful by HIPAA regulations, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of protected health information that violates HIPAA regulations.

- W. DBHDD facilities have custody of a variety of types of records, such as incident reports and other administrative records, which may contain confidential or protected health information about an individual. It is the policy of DBHDD to protect confidential and protected health information according to law, when such information is in records that are requested under the Georgia Open Records Act, in administrative hearings, in lawsuits, or by any other lawful means.

- X. DBHDD shall train all current and newly hired members of its workforce on its privacy policies and procedures as necessary and appropriate for them to carry out their functions within DBHDD, according to a training plan for HIPAA awareness. Newly hired persons shall be trained within a reasonable time after being hired. If the functions of workplace members are materially affected by a change in DBHDD policies, training will be provided within a reasonable time after such change in policy.

- Y. DBHDD shall designate a Privacy Officer who shall be responsible for receiving complaints and to provide privacy practice information. The Privacy Officer shall develop and implement, and maintain an adequate working knowledge of

DBHDD	SUBJECT: Confidentiality and HIPAA	Policy 23-100
		Page 13 of 14

DBHDD's privacy and security policies and procedures and of the confidentiality laws and HIPAA, to respond to HIPAA related inquiries arising within DBHDD, provide information regarding the complaint process and maintain adequate documentation of these activities. The Privacy Officer shall submit reports of privacy related activities periodically to the Commissioner of the Department upon request.

- Z. DBHDD shall designate a Security Officer who shall be responsible for receiving complaints regarding security and to provide Security Rule information. The Security Officer shall obtain and maintain an adequate working knowledge of DBHDD's privacy and security policies and procedures and of the confidentiality laws and HIPAA, respond to Security Rule related inquiries arising within DBHDD, provide information regarding the security complaint process and maintain adequate documentation of these activities. The Security Officer shall submit reports of security related activities periodically to the Commissioner of the Department upon request.
- AA. The Privacy Officer and Security Officer shall work jointly and coordinate on appropriate policies, procedures, reports and projects as applicable.
- BB. DBHDD may appoint Privacy Coordinators at the regional, institutional or other administrative level, who are responsible for receiving complaints. Privacy Coordinators shall obtain and maintain a working knowledge of DBHDD's privacy and security policies and procedures and of confidentiality laws and HIPAA. Privacy Coordinators must submit reports as required to the Privacy Officer and Security Officer.
- CC. DBHDD shall maintain policies and procedures regarding reporting of violations of confidentiality rights and HIPAA. Violation of DBHDD privacy policies and procedures shall be communicated to the Privacy Coordinator, and then to the Privacy Officer, and additionally to the Security Officer as appropriate. Violation reports shall include the date of discovery and the date of breach if known; a brief description of what happened; a brief description of the types of PHI involved in the breach; a description of any actions taken to investigate the breach, actions taken within the work unit to mitigate harmful effects of the violation and prevent recurrence; any steps the individual should take to protect himself/herself from potential harm from the breach; contact information for the individual to ask questions of the Privacy Coordinator or investigator; and if known, the name and title of the violator, information about the violator's intent and information on previous similar occurrences. Violation reports shall be in writing for documentation purposes.
- DD. DBHDD shall maintain policies and procedures regarding identification of breaches of HIPAA and reporting of breaches. Privacy Coordinators, in consultation with the Privacy Officer and/or the Office of Legal Services, shall determine whether violations also constitute breaches and ensure that notifications

DBHDD	SUBJECT: Confidentiality and HIPAA	Policy 23-100
		Page 14 of 14

are made, as required by the HITECH Act and HIPAA, to the individual, the Secretary of HHS, and the news media.

- EE. DBHDD shall allow authorized revisions of confidentiality and HIPAA policies and procedures in response to changes in administrative, operating or programmatic requirements. The DBHDD Privacy Officer must approve any and all revisions.
- FF. DBHDD shall adopt supplemental internal privacy policies and procedures where necessary to meet the requirements of specific programs, activities, or federal or state laws and regulations. Such policies and procedures shall conform to those of the Department, confidentiality laws and HIPAA, and are subject to review by the DBHDD Privacy Officer.
- GG. DBHDD shall examine and revise its confidentiality and HIPAA policies and procedures on an ongoing basis and as necessary to satisfy requirements of confidentiality laws and HIPAA.
- HH. DBHDD maintains policies and procedures regarding its activities which may address confidentiality or disclosures that are a part of such activity. The provisions of this policy apply generally to those policies and procedures unless specifically stated otherwise in such policies. Questions regarding policy applicability or interpretation should be sent to the Office of Legal Services. Such policies and activities include, but are not limited to:
 - 1. Research involving human subjects
 - 2. Reporting of abuse, neglect, or exploitation
 - 3. Required reporting of diseases or injuries
 - 4. Required reporting of criminal conduct
 - 5. Protection and Advocacy under federal regulations; and
 - 6. Advance Directives.

LEGAL REFERENCES

- 1. 42 United States Code Annotated, 290dd-2
- 2. 42 CFR Part 2
- 3. 45 CFR Parts 160 and 164.
- 4. Official Code of Georgia Annotated 24-9-40 and 24-9-47; 31-9-22.1; 31-32-1 et seq.; 37-1-1; 37-2-2; Chapter 3 of Title 37; 37-3-166 (Mental Illness); Chapter 4 of Title 37; 37-4-125 (Developmental disability); Chapter 7 of Title 37; 37-7-166 (Substance Abuse).
- 5. Rules and Regulations of the Department of Human Resources, Chapter 290-4-6, "Patients' Rights."

REFERENCE MATERIALS

- 1. SAMHSA and the Office of the National Coordinator (ONC) for Health Information Technology Frequently Asked Questions (FAQs) for Applying the Substance Abuse Confidentiality Regulations to the Health Information Exchange (HIE).



Georgia Department of Behavioral Health & Developmental Disabilities

Name of Individual/Consumer/Patient/Applicant

Social Security Number AND/OR Date of Birth

AUTHORIZATION FOR RELEASE OF INFORMATION

I hereby authorize:

(Name of Person or Agency to whom information should be given - requesting agency)

(Address)

to obtain from:

(Name of health care provider holding the information - releasing agency)

(Address)

the following type(s) of information from my records (and any specific portion thereof):

I authorize the disclosure of alcohol or drug abuse information, if any.(Please see paragraph 2 below)

Initials

I authorize the disclosure of information, if any, concerning testing for HIV (human immunodeficiency virus) and/or treatment for HIV or AIDS (acquired immune deficiency syndrome) and any related conditions.

for the purpose of:

- 1. I understand that the information disclosed pursuant to this Authorization may be subject to re-disclosure by the recipient and no longer protected by federal privacy regulations or other applicable state or federal laws (except as set forth in paragraph 2 below).
2. I understand that, pursuant to 42 C.F.R Part 2, alcohol and drug abuse records that I authorize to be disclosed pursuant to this document may not be further re-disclosed without my written consent, except by a court order that complies with the preconditions set forth at 42 C.F.R. 2.61 et seq., or the other limited circumstances specifically permitted by 42 C.F.R. Part 2. Any individual that makes such a disclosure in violation of these provisions may be reported to the United States Attorney and be subject to criminal penalties.
3. I understand that the Department or my healthcare provider will not condition my treatment, payment, or eligibility for any applicable benefits on whether I provide authorization for the requested release of information.
4. I intend this document to be a valid authorization conforming to all requirements of the Privacy Rule and state law, and understand that my authorization will remain in effect for: (PLEASE CHECK ONE)

one (1) year.

the period necessary to complete all transactions on matters related to services provided to me.

I understand that unless otherwise limited by state or federal regulation, and except to the extent that action has been taken based upon it, I may revoke this authorization at any time by sending written notice of my withdrawal of this authorization to the staff of the healthcare provider who is providing services to me, OR to the Department's Privacy Officer at 2 Peachtree St. NW, Suite 22.240 Atlanta, GA 30303-3142. Fax: 404-657-2173

Date

Signature of Individual/Consumer/Patient/Applicant

Signature of Witness (Title or Relationship to Individual)

Signature of (check one): Date
Parent Guardian Court-appointed Custodian of Minor
Agent designated by Individual's Advance Directive

USE THIS SPACE ONLY IF AUTHORIZATION IS WITHDRAWN

Date this authorization is revoked by Individual

Signature of Individual or legally authorized Representative

<p style="text-align: center;">Georgia Department of Behavioral Health & Developmental Disabilities</p> <p style="text-align: center;">Facility/Program/Hospital Name Address, City, State, Zip Contact numbers</p> <p style="text-align: center;">DBHDD Policies 23-100 and 23-101</p> <p style="text-align: center;">NOTICE OF PRIVACY PRACTICES FORM</p>	<p>Stamp Plate</p>
---	--------------------

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED BY THE DEPARTMENT AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY. This notice is effective September 1, 2011. It is provided to you under the Health Insurance Portability and Accountability Act of 1996 and related federal regulations (HIPAA). If you have questions about this Notice please contact your Treatment Provider or Services Provider, or the Department's Privacy Officer at the address below.

The Department of Behavioral Health and Developmental Disabilities (DBHDD) is an agency of the State of Georgia responsible for certain programs which deal with medical and other confidential information. Both federal and state laws establish strict requirements regarding the disclosure of confidential information, and the Department must comply with those laws. For situations where stricter disclosure requirements do not apply, this Notice of Privacy Practices describes how the Department may use and disclose your "protected health information" for treatment, payment, health care operations, and for certain other purposes. This notice also describes your rights regarding your protected health information. **Protected health information** is information that may personally identify you and relates to your past, present or future physical or mental health or condition and related health care services. The Department is required to provide you this Notice of Privacy Practices, and to abide by its terms, and may change the terms of this notice at any time. A new notice will be effective for all protected health information that the Department maintains at the time of issuance. The Department will provide you with any revised Notice of Privacy Practices by posting copies at its facilities, publication on the Department's website, in response to a telephone or facsimile request to the Privacy Officer, or in person at any facility where you receive services from the Department.

1. Uses and Disclosures of Protected Health Information: Your protected health information may be used and disclosed by the Department, its administrative and clinical staff and others involved in your care and treatment for the purpose of providing health care services to you, and to assist in obtaining payment of your health care bills.

a. Treatment: Your protected health information may be used to provide, coordinate, or manage your health care and any related services, including coordination of your health care with a third party that has your permission to have access to your protected health information, such as, for example, a health care professional who may be treating you, or to another health care provider such as a specialist or laboratory.

b. Payment: Your protected health information may be used to obtain payment for your health care services. For example, this may include activities that a health insurance plan requires before it approves or pays for health care services such as: making a determination of eligibility or coverage, reviewing services provided to you for medical necessity, and undertaking utilization review activities.

c. Health Care Operations: The Department may use or disclose your protected health information to support the business activities of the Department, including, for example, but not limited to, quality assessment activities, employee review activities, training, licensing, and other business activities. Your protected health information may be used to contact you about appointments or for other operational reasons. Your protected health information may be shared with third party "business associates" who perform various activities that assist us in the provision of your services.

2. Other Permitted or Required Uses and Disclosures with Your Authorization or Opportunity to Object: Other uses and disclosures of your protected health information will be made only with your written authorization, which you may revoke at any time to the extent that the Department has not acted upon your authorization, **except** as permitted or required by law as described below. The Department may use and disclose your protected health information when you authorize in writing such use or disclosure of all or part of your protected health information. If you are hospitalized, the Department may use and disclose certain protected health information to your representative, as that term is defined in the Georgia Mental Health Code, upon your admission or discharge; you may be given a chance to object to certain other disclosures to your representative.

a. Confidentiality of Alcohol and Drug Abuse Patient Records: The confidentiality of patient records which disclose any information identifying you as an alcohol or drug abuser is protected by federal law and regulations. This information generally will not be disclosed unless you consent in writing, the disclosure is allowed by a court order, or the disclosure is made to medical personnel in a medical emergency or to qualified personnel for research, audit, or program evaluation. Violation of these federal laws and regulations by the facility, treatment or service provider, or the Department, is a crime. You may report violations to appropriate authorities in accordance with the federal regulations. Federal regulations do not protect any information about a crime committed by you either at a facility or program or against any person who works at a facility or program or about any threat to commit such a crime. Federal regulations do not protect any information about suspected child abuse or neglect from being reported under State law to appropriate State or local authorities.

b. AIDS confidential information: AIDS confidential information, including HIV status or testing information, is confidential under state law. Generally, the Department will not disclose AIDS confidential information without your authorization. The Department may disclose this information in certain circumstances to protect persons at risk of infection by you, including your family and health care providers. The

Department may disclose AIDS confidential information in certain circumstances as part of your mental health commitment or by other legal procedures.

3. Permitted or Required Uses and Disclosures without Your Authorization or Opportunity to Object: The Department may use or disclose your protected health information without your authorization for continuity of your care or for your treatment in an emergency or when clinically required; when required to do so by law; for public health purposes; to a person who may be at risk of contracting a communicable disease; to a health oversight agency; to an authority authorized to receive reports of abuse or neglect; in certain legal proceedings, such as hearings regarding your hospitalization or commitment or to comply with workers' compensation laws; and for certain law enforcement purposes. Protected health information may also be disclosed without your authorization to a coroner or medical examiner, and to the legal representative of your estate.

4. Required Uses and Disclosures: Under the law, the Department must make certain disclosures to you, and to the Secretary of the United States Department of Health and Human Services when required to investigate or determine the Department's compliance with the requirements of HIPAA regulations beginning at 45 CFR Section 164.500.

5. Your Rights: The following is a statement of your rights with respect to your protected health information and a brief description of how you may exercise these rights.

a. You have the right to inspect and copy your protected health information: You may inspect and obtain a copy of protected health information about you for as long as the Department maintains the protected health information. This information includes medical and billing records and other records the Department uses for making medical and other decisions about you. A reasonable, cost-based fee for copying, postage and labor expense may apply. Under federal law you may not inspect or copy psychotherapy notes; information compiled in anticipation of, or for use in, a civil, criminal, or administrative proceeding, or protected health information that is subject to a federal or state law prohibiting access to such information. While you are hospitalized, your physician may restrict your right to review your records if it would be harmful to your physical or mental health.

b. You have the right to request restriction of your protected health information: You may ask the Department not to use or disclose any part of your protected health information for the purposes of treatment, payment or healthcare operations, and not to disclose protected health information to family members or friends who may be involved in your care. Such a request must state the specific restriction requested and to whom you want the restriction to apply. The Department is not required to agree to a restriction you request, and if the Department believes it is in your best interest to permit use and disclosure of your protected health information, your protected health information will not be restricted, except as required by law. If the Department does agree to the requested restriction, the Department may not use or disclose your protected health information in violation of that restriction unless it is needed to provide emergency treatment.

c. You have the right to request to receive confidential communications from us by alternative means or at an alternative location: Upon written request to a person listed in section 6 below, the Department will accommodate reasonable requests for alternative means for the communication of confidential information with you, but may condition this accommodation upon your provision of an alternative address or other method of contact. The Department will not request an explanation from you as to the basis for the request.

d. You may have the right to request amendment of your protected health information: If the Department created your protected health information, you may request an amendment of that information for as long as it is maintained by the Department. The Department may deny your request for an amendment, and if it does so will provide information as to any further rights you may have with respect to such denial. Please contact one of the persons listed in section 6 below if you have questions about amending your protected health information.

e. You have the right to receive an accounting of certain disclosures the Department has made of your protected health information: This right applies only to disclosures for purposes other than treatment, payment or healthcare operations, and does not apply to any disclosures the Department made to you, to family members or friends or representatives, as defined in the Georgia Mental Health Code, who are involved in your care, or for national security, intelligence or notification purposes. You have the right to receive legally specified information regarding disclosures occurring in the six (6) years before your request, subject to certain exceptions, restrictions and limitations.

f. You have the right to obtain a paper copy of this notice from the Department, upon request.

6. Complaints: You may complain to us and to the United States Secretary of Health and Human Services if you believe your privacy rights have been violated. You may file a complaint in writing with the Department facility providing your treatment or services, or your treatment provider or services provider under contract or agreement with the Department which maintains your protected health information at telephone _____, facsimile _____, or by mail to _____. You must state the basis for your complaint. Neither the facility, the provider, nor the Department will retaliate against you for filing a complaint. You may also contact the **Department's Privacy Officer by telephone at (404) 657-2282, facsimile (404) 657-2173, or by mail to 2 Peachtree Street NW, Room 22.240, Atlanta, Georgia 30303-3142,** for further information about the complaint process or this notice.

Please sign a copy of this Notice of Privacy Practices for your provider's and the Department's records.

I have received a copy of this Notice on the date indicated below.

Signature of Individual or Legally Authorized Person

Date

Stamp Plate