Georgia Department of Public Health

GEORGIA DEPARTMENT OF PUBLIC HEALTH
POLICY # GC-09013
CONFIDENTIALITY OF PERSONAL HEALTH INFORMATION AND COMPLIANCE WITH HIPAA

Approval:	Sidney R. Barrett, Jr., General Counsel	30 August 2013 Date
	James C. Howgate, Chief of Staff	9/10/13 Date

TABLE OF CONTENTS

1.0 POLICY

The Department is committed to protecting the confidentiality of personal health information in accordance with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and all state and federal privacy laws. This policy sets forth the standards and procedures for Department employees to follow in protecting personal health information.

It is Department policy that an individual's health information should only be disclosed to people who have a legal right to receive it, whose identity has been verified, and whose authority to receive it has been verified. Health information shall not be disclosed or made available to unauthorized persons, and precautions shall be taken to ensure that health information is not disclosed to unauthorized persons.

This Policy does not list every possible situation in which the Department may lawfully disclose personal health information to third parties. Employees are directed to consult the DPH Privacy Officer if they believe it may be necessary to disclose an individual's personal health information without that individual's authorization.

1.1 AUTHORITY

45 C.F.R. Part 160: "General Administrative Requirements"

45 C.F.R, Part 162: "Administrative Requirements"

45 C.F.R, Part 164: "Security and Privacy"

1.2 DEFINITION OF TERMS AND ACRONYMS

1.2.1 **Administrative Safeguards**: Administrative actions, and policies and procedures, to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

1.2.2 **Breach**: The acquisition, access, use, loss, or disclosure of protected health information in circumstances where it might be accessed by unauthorized individuals or entities. If protected health information is acquired, accessed, used, lost, or disclosed in a manner not permitted under HIPAA or other privacy laws, then it shall be presumed to be a breach unless an investigation and risk assessment show that there is a low probability that the information was actually compromised.

1.2.3 **Business Associate**: An outside person or entity that performs or assists the Department in the performance of a function or activity involving the use or disclosure of individually identifiable health information.

1.2.4 **Covered Entity**: An entity that is subject to HIPAA because it is a health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA.

1.2.5 **Covered Components**: Those Divisions, Programs, or Offices within DPH that have been designated as being subject to HIPAA because they perform the functions of a health plan, health care provider, or health care clearinghouse.

1.2.6 **Designated Record Set**: A group of records that includes (1) the medical records and billing records about patients maintained by or for a covered health care provider; (2) records of the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) records used by or for the covered entity to make decisions about the patient. 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.

1.2.7 **Disclosure**: The release or transfer of protected health information in any manner to a person or entity outside the Covered Component, including the act of allowing access to protected health information.

1.2.8 **Electronic Media**: Electronic storage media including memory storage components in computers and any removable or transportable digital memory medium, such as magnetic tape or disk, optical disk, hard drive, or digital memory card; or transmission media used to exchange information already in electronic storage media. Examples of transmission media include the internet, extranet, leased lines, dial-up lines, private networks, and the physical movement of removable/ transportable electronic storage media. Certain transmissions, such as facsimile messages, telephone conversations, or VOIP (voice over internet), are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission.

1.2.9 **Electronic Protected Health Information**: Individually identifiable health information that is transmitted by electronic media or maintained in electronic media.

1.2.10 **Health Care Operations**: Any of the following activities of the covered entity to the extent that the activities are related to covered functions:

1.2.10.1 Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;

1.2.10.2 Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;

1.2.10.3 Underwriting and other activities relating to the creation, renewal, or replacement of a health insurance or health benefits contract, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;

1.2.10.4 Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;

1.2.10.5 Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and

1.2.10.6 Business management and general administrative activities including de-identifying protected health information, and creating a limited data set.

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

1.2.12 **Health Information**: Any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, and which relates to the past, present or future physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present or future payment for the provision of health care to a patient.

1.2.13 **Health Oversight Agency**: An agency or authority of the United States, a territory, a political subdivision of a State or territory, an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors, that is authorized by law to oversee the health care system (whether public or private) 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.

1.2.14 **Individually Identifiable Health Information**: Health information pertaining to an identifiable named patient, and which 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 condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient, and that identifies the patient, or for which there is a reasonable basis to believe the information can be linked to the patient.

1.2.15 **Minor**: An unmarried person under the age of eighteen who has not been emancipated by order of the courts.

1.2.16 **Patient**: The person who is the subject of the protected health information.

1.2.17 **Protected Health Information (PHI)**: Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

1.2.18 **Psychotherapy Notes**: Notes recorded in any medium by a health care provider who is 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 patient's medical record. Psychotherapy notes excludes medication prescription and 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, the treatment plan, symptoms, prognosis, and progress to date.

1.2.19 **Public Health Authority**: An agency or authority of the United States, a state, territory, a political subdivision of a state or territory, or an Indian tribe, or a person acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency, that is responsible for public health matters as part of its official mandate.

1.2.20 **Security Incident**: The attempted or successful unauthorized access, use, disclosure, modification, loss, or destruction of health information, or interference with system operations in an information system that stores health information.

1.2.21 **Technical Safeguards**: The technology and the policy and procedures for its use that protect electronic protected health information and control its access.

1.2.22 **Unsecured Protected Health Information**: Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through use of a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services.

2.0 APPLICABILITY AND RESPONSIBILITES

2.1 APPLICABILITY. The Department has elected to designate itself as a "Hybrid Entity" for purposes of HIPAA compliance. This means that certain divisions, office, and programs within the Department must comply fully with HIPAA, and the rest are not subject to HIPAA. The following entities within the Department are hereby designated as Covered Components subject to HIPAA:

2.1.1 Within the Division of Health Protection: Public Health Laboratories; Pharmacy; Refugee Health; Volunteer Health Care Program; Epidemiology; Infectious Disease and Immunization.

2.1.2 Within the Division of Health Promotion: Maternal and Child Health; Health Promotion & Disease Prevention; WIC.

2.1.3 The Division of Information Technology.

2.1.4 District Health Directors and District Cadre Staff.

2.1.4.1 The Department recognizes that County Boards of Health are separate legal entities employing their own public health employees, and that such County Boards of Health bear legal responsibility for their own HIPAA compliance. The District Health Director shall administer a legally sufficient HIPAA policy adopted by a County Board of Health with respect to its employees. If no such policy has been adopted by a County Board of Health, then the District Health Director shall administer this policy with respect to the county public health employees of that County.

2.1.5 DPH employees in Covered Components shall not disclose or allow access to PHI by DPH employees in other DPH divisions, offices, or programs except as specifically authorized by this policy or by the Privacy Officer. DPH employees in non-Covered DPH divisions, offices, or programs shall not have access to PHI except as authorized by the Privacy Officer.

2.1.6 Even though non-Covered DPH divisions, offices, and programs are not legally subject to HIPAA, it is expected that all DPH employees will familiarize themselves with the requirements of HIPAA and this policy, and will exercise their best efforts to protect the confidentiality of any individually identifiable health information which may come within their custody or control.

2.2 RESPONSIBILITES

2.2.1 The Office of the General Counsel shall designate one of its members to serve as Privacy Officer for the Department, to be responsible for the development of the Department's policies and procedures for the protection of PHI and compliance with HIPAA, administrative safeguards, assistance with training materials, and providing legal advice as needed.

2.2.2 The Chief Information Officer shall designate a member of his or her staff to serve as Information Security Officer for the Department, to be responsible for the implementation of appropriate technical safeguards as required by HIPAA to ensure the integrity of all electronic PHI that the Department creates, maintains, receives, or transmits.

2.2.3 The Office of Human Resources is responsible for training of DPH employees in privacy compliance, for documenting such training for individual employees, and for applying appropriate sanctions against employees who violate privacy policies and procedures.

2.2.4 The District Health Director of each Health District shall designate a DPH employee to serve as District Privacy Officer for the Health District, to carry out the same responsibilities as the DPH Privacy Officer for that District.

2.2.5 The Security Incident Response Team shall respond to any suspected breach of PHI in accordance with the Personal Health Information Security Incident Response Protocol. The Team shall consist of the Privacy Officer and the Information Security Officer. If circumstances warrant, the Team may request the support of the Director of Communications, the Inspector General, and the District Privacy Officer.

2.2.6 Supervisory personnel in each Covered Component are responsible for ensuring compliance with this policy by DPH employees under their supervision.

3.0 GENERAL STANDARDS FOR HANDLING PROTECTED HEALTH INFORMATION

PHI should only be disclosed to people who have a legal right to receive it, whose identity has been verified, and whose authority to receive the PHI has been verified. In addition, care must be taken to prevent accidental disclosure or access to PHI by unauthorized persons.

Note: These standards apply even if the patient is deceased.

3.1 Face to Face Discussions

Employees must take reasonable steps to protect the privacy of all face-to-face discussions of PHI, whether inside or outside of the office. When possible, employees should use enclosed offices or interview rooms for discussions involving PHI. If enclosed offices or rooms are not available, then employees should take reasonable precautions to ensure that their conversations are not overheard. In all cases, discussions of PHI should be limited to only that PHI which is necessary to conduct the business at hand.

3.2 Telephone Calls

3.2.1 Before discussing PHI over the telephone with a patient, including providing test results or contacting the patient about appointments, employees must confirm the identity of the patient. This may be done by asking the patient to confirm his or her full name, date of birth, and the last four digits of their Social Security number.

3.2.2 Employees must honor any previously agreed upon requests by the patient to use alternate means of communication, such as alternate phone numbers, or limiting calls to certain hours.

3.2.3 Telephone calls should be made in private locations where possible. The employee should be aware of the surroundings and make sure that the conversation is not heard by nearby persons. The employee should also ask the patient to confirm that there is no one else on the line.

3.2.4 If the employee gets the patient's voicemail and decides to leave a message, then the message should only include the name and phone number of the person to be called back. Do not leave any other information, such as the name of the program from which the employee is calling or the fact that test results have been received, since that may compromise patient confidentiality if someone else retrieves the message.

3.3 Visual Access to PHI Displayed on Computer Screens

3.3.1 Employees must ensure that PHI displayed on computer screens is adequately shielded from view by unauthorized persons. Polarized screens or other screen overlay devices that shield information on the computer screen should be used when possible.

3.3.2 Computer workstations must be locked when not in use, and PHI must be cleared from the screen when it is not being used.

3.3.3 Computers and other electronic storage devices containing PHI must be stored in a secured location at all times.

3.4 Paper Records and Files

3.4.1 Employees must store files and documents containing PHI in secure filing cabinets, rooms, or storage systems. If lockable storage is not available, staff must take reasonable steps to ensure the safeguarding of documents containing PHI.

3.4.2 Papers containing PHI must be shredded before they are placed in the trash.

3.4.3 Documents containing PHI must be shielded from view by unauthorized persons, and should not be left unattended in open areas.

3.5 Outgoing Mail (Including Inter-office or Intra-office Mail)

3.5.1 Documents or other medium containing PHI should be mailed in sealed envelopes or other secure container, properly addressed to the recipient, and the outer envelope should be clearly labeled "Confidential".

3.5.2 If PHI is stored on electronic media, then the media should be password protected before mailing.

3.5.3 The information sent should be the minimum necessary for the intended purpose.

3.5.4 All outgoing mail containing PHI should clearly display a return name and address on the outer envelope, so that misdirected mail can be returned to the sender.

3.6 Facsimile Communications

3.6.1 Covered Components must designate specific fax machines to send and receive documents containing PHI. The fax machines should be located in a non-public place and near to the intended recipients.

3.6.2 When receiving a fax containing PHI, employees should request a call from the sender prior to transmission, so that someone will be standing by to retrieve the document from the machine as soon as it received.

3.6.3 When sending a fax containing PHI, employees must contact the recipient to schedule transmission, confirm the fax number, and ensure that the fax will be retrieved by an authorized person after it is sent. Outgoing faxes containing PHI must have a cover page labeled "CONFIDENTIAL." After sending the fax, employees must confirm that delivery was made to the intended recipient by either contacting the recipient to confirm receipt or reviewing the fax transmission confirmation.

3.6.4 The information sent should be the minimum necessary for the intended purpose.

3.6.5 In the event that a fax is inadvertently sent to an unintended recipient, the recipient must be contacted immediately and asked to destroy the information. Misdirected faxes are considered a security incident and must be reported to the Privacy Officer.

3.7 Emails

3.7.1 Emails should not contain PHI unless the PHI is in encrypted form. Where feasible, the PHI should be sent in a password-protected attachment instead of in the body of the email, with the password being sent in a separate email or communication which should also notify the recipient that the information has been emailed.

3.7.2 Emails containing PHI must be marked "CONFIDENTIAL" in the subject line, and should only be sent to persons who understand the Department's privacy policies and applicable privacy laws and regulations, and will not forward the email to unauthorized persons.

3.7.3 The information sent should be the minimum necessary for the intended purpose.

3.7.4 Employees should verify and review the recipient's email address prior to sending the email. In the event an email is inadvertently sent to the unintended recipient, the recipient must be contacted immediately and asked to delete the email and attachment. Misdirected emails are considered a security incident and must be reported to the Privacy Officer.

4.0 THE "MINIMUM NECESSARY" RULE WHEN USING OR DISCLOSING PHI

Even when disclosure of PHI is appropriate, employees must ensure that only the minimum PHI necessary to accomplish the intended purpose will be used or disclosed.

4.1 Necessary Access and Use.

Access and use should be restricted based on specific roles of persons working within a Covered Component. Each division, office, and program supervisor in a Covered Component must identify the persons or groups of persons who need access to PHI to carry out their job functions, identify the type of PHI to which each person or group needs access, as well as the conditions under which they need access, and make reasonable efforts to limit the access of its staff to only the information appropriate and necessary for their job requirements. Access to PHI should not be granted to any unit or program that does not need access to perform its job functions.

4.2 Minimum Necessary Disclosures:

Before disclosing PHI, staff must evaluate the purpose of the disclosure and limit the disclosure to the minimum necessary to satisfy the intent of the disclosure. Covered Components should identify routine and recurring disclosures and determine what information is reasonably necessary to fulfill the purpose of these requests so that the disclosure can be limited to the minimum necessary. In making this determination, Covered Components should evaluate whether the purpose of the disclosure can be fulfilled with de-identified information or a limited data set. Non-routine and non-recurring requests should be reviewed on an individual basis to ensure only the minimum necessary is disclosed for each of these requests.

4.2.1 **Situations in which the minimum necessary requirement does not apply:**

4.2.1.1 disclosures to or requests by a health care provider for treatment of the patient;

4.2.1.2 disclosures made to the patient or her authorized representative;

4.2.1.3 disclosures made pursuant to a valid authorization

4.2.1.4 disclosures made to the Secretary of the U. S. Department of Health & Human Services;

4.2.1.5 disclosures required by law; or

4.2.1.6 disclosures required for compliance with HIPAA regulations.

5.0 RESPONDING TO REQUESTS FOR DISCLOSURE OF PHI

5.1 Requests for Disclosure Made By the Patient

5.1.1 The Department shall disclose PHI to a patient when the patient requests access to their own PHI. However, there is one exception: a therapist's psychotherapy notes may not be disclosed to a patient without prior approval from the Privacy Officer.

5.1.2 The patient's identity shall be verified in accordance with Paragraph 5.5.1 before releasing PHI.

5.2 Requests for Disclosure Made By the Patient's Authorized Representative

5.2.1 The Department shall disclose PHI to a third party who is legally authorized to act as a representative of the patient with regard to health matters.

5.2.2 The scope of the representative's authority to act for the patient depends on his or her authority to make health care decisions for the patient. If the authority to act for a patient is limited to a particular health care decision, the person should be treated as the patient's representative only with respect to PHI relevant to that decision. Employees are encouraged to consult with the Privacy Officer if they have any doubt about the representative's authority.

Common situations involving a patient authorized representative include:

5.2.2.1 *Adult or Emancipated Minor*: If a person is authorized to act on behalf of an adult or emancipated minor in making health care decisions, then this person

must be treated as a personal representative with respect to PHI related to such representation. Examples include persons acting pursuant to a health care power of attorney or general power of attorney, or a court appointed legal guardian.

5.2.2.2 *Deceased Patient*: Privacy rights under HIPAA continue for fifty years after the patient dies. An executor, administrator, or other person authorized by law to act on behalf of the deceased person's estate may be treated as personal representative with respect to the deceased's PHI.

5.2.2.3 *Minor Children*: If a parent, guardian, or other person acting in the place of a parent (*in loco parentis*) is authorized to act on behalf of a minor in making health care decisions, then this person may be treated as a personal representative with respect to PHI related to such representation. It may be necessary in some cases to require proof of a parent or other person's authority to have access to the child's PHI; for example, a divorced parent without authority to make health care decisions for the child should not have access to the child's PHI. In addition, the Department must *not* make disclosures to a parent or guardian if

5.2.2.3.1 the minor consented to care and the consent of the parent is not required under State or other applicable law (*e.g.*, testing or treatment of venereal disease);

5.2.2.3.2 the minor obtained care at the direction of a court or a person appointed by the court; or

5.2.2.3.3 the parent or guardian agreed that the minor and the health care provider may have a confidential relationship.

5.2.2.4 *Married persons*: Employees are cautioned that a married person should *not* be given access to a spouse's PHI, unless that person presents proof of authorization in accordance with either this Paragraph or Paragraph 5.3.

5.2.3 The identity *and* authority of a third party seeking the PHI must be verified as specified in Paragraph 5.5 prior to disclosure of PHI to the third party. The proof needed to verify authority will vary depending on the nature of the authority. For example, a court-appointed guardian or the executor of a deceased person's estate will have an order of appointment from the probate court, and a person acting pursuant to a health care power of attorney will have a written power of attorney. Consult the Privacy Officer if you have any concerns about proof of authority.

5.2.4 The Department may refuse a request for PHI from a person acting as the patient's personal representative if it appears that the personal representative may have subjected the patient to violence, abuse, or neglect; if treating the person as a personal representative could endanger the patient; or if a licensed healthcare professional determines, in the exercise of professional judgment, that it is not in the best interest of the patient to treat the person as a personal representative.

5.3 Requests for Disclosure Made By Third Parties With a Written Authorization From the Patient

A patient's PHI shall be disclosed to a third party pursuant to a valid written authorization signed by the patient. Patients should be encouraged to use the standard DPH Authorization For Release of PHI Form, but any authorization form that meets the requirements of Paragraph 5.3.1 should be honored. Upon request, the Privacy Officer shall review an authorization form to ensure that it is legally sufficient. The Department must retain a copy of all signed authorizations.

5.3.1 **Criteria for a Valid Authorization**

If an employee receives a request for disclosure of PHI from a third party with an Authorization Form signed by the patient attached, the form will be honored only if it contains all of the elements below in plain language:

5.3.1.1 A specific description of the information requested;

5.3.1.2 The name or other specific identification of the person(s), or class of persons, authorized to request the information;

5.3.1.3 The name or other specific identification of the person(s), or class of persons, to whom the Department may give the requested information;

5.3.1.4 A description of the purposes for which the information is requested;

5.3.1.5 An expiration date or an expiration event that relates to the patient or the purpose of the request;

5.3.1.6 Signature of the patient and date;

5.3.1.7 A statement adequate to place the patient on notice of his or her right to revoke the authorization in writing, a list of the exceptions to the right to revoke, and a description of how the individual may revoke the authorization;

5.3.1.8 A statement adequate to place the patient on notice of whether or not treatment, payment, enrollment or eligibility for benefits will be conditioned on whether the patient signs the authorization; and

5.3.1.9 A statement adequate to place the patient on notice of the potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer be protected by HIPAA.

5.3.2 **Authorization for Disclosure of Psychotherapy Notes**

A separate specific authorization form must be obtained for the disclosure of psychotherapy notes that are included within a patient's medical records. The form must specifically request psychotherapy notes in addition to having all the elements listed in Paragraph 5.2.1. Consult with the Privacy Officer if there are any questions regarding the sufficiency of an authorization for the disclosure of psychotherapy notes received from a third party.

5.3.3 **Invalid Authorization**

An authorization will not be honored by the Department if it has any of the following defects: (i) the expiration date or event has passed; (ii) the Authorization Form has not been filled out completely; (iii) the authorization has been revoked; (iv) any information on

the authorization is known to be false; (v) an authorization for psychotherapy notes is combined with a request for disclosure of information other than psychotherapy notes.

An invalid authorization should be returned to the person who submitted it, with an explanation of why the authorization cannot be honored. Consult with the Privacy Officer if you receive an authorization that may be invalid.

5.3.4 **Compound Authorization**

An authorization for use or disclosure of PHI must be a separate document, and may not be combined with any other document from the patient to create a compound authorization, except as follows: (i) an authorization for the use or disclosure of PHI for a research study may be combined with the informed consent document that will be used in the research project; (ii) an authorization for the use or disclosure of psychotherapy notes may be combined with authorization for the use or disclosure of psychotherapy notes to other persons (*e.g.,* a single authorization can be used for disclosure to multiple agencies or individuals); (iii) an authorization may be combined with authorization to other persons (*e.g.,* a single authorization can be used for disclosure to multiple agencies or individuals).

5.3.5 **Revocation of Authorization**

A patient may revoke his or her authorization in writing at any time. If the patient revokes an authorization, the Department cannot disclose information after the effective date of the revocation. A revocation should be maintained in the patient's file.

5.4 Requests for Disclosure Made By Third Parties Without Patient Authorization

Covered Components may disclose PHI to third parties without the written authorization of the patient only in certain limited circumstances. *All requests for disclosure without patient authorization must be sent to the Privacy Officer for review before any response is made.* The Privacy Officer may determine that disclosure of PHI without patient authorization is appropriate in the following situations:

5.4.1 To a healthcare provider covered by HIPAA for the purpose of treatment, payment, or healthcare operations;

5.4.2 Disclosures required by law;

5.4.3 Disclosures for public health activities to (i) Public Health Authorities that are authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including the reporting of disease, injury, vital events, and public health surveillance (*e.g.,* the CDC); (ii) public health or other government authority legally authorized to receive reports of child abuse or neglect; or (iii) a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition.

5.4.4 Disclosures about victims of abuse, neglect or domestic violence to a government authority authorized by law to receive such information under certain circumstances;

5.4.5 Disclosures for health oversight activities authorized by law (*e.g.*, audits);

5.4.6 Disclosures for court proceedings, including search warrants, court orders, subpoenas, interrogatories, or requests for production of documents.

Note: Any legal paper seeking PHI should be faxed, emailed, or hand-delivered to the Privacy Officer immediately upon receipt.

5.4.7 Disclosures for law enforcement purposes to a law enforcement official, if certain conditions are met;

5.4.7.1 Disclosures about decedents to a coroner or medical examiner to identify a deceased person or determine cause of death, and to funeral directors;

5.4.7.2 Disclosures for research purposes if approved in accordance with DPH Policy CO-12007 (Data Request Policy) and a DPH Data Use Agreement is signed;

5.4.7.3 Disclosures to avert a serious threat to the health or safety of a person or the public;

5.4.7.4 Disclosures for specialized government functions, including national security and intelligence activities;

5.4.7.5 Disclosures to comply with laws relating to workers' compensations;

5.4.7.6 Disclosures to persons involved in the patient's care and for notification of the patient's location, general condition, or death purposes. If the patient is present, he or she must be given the opportunity to agree or object to such disclosures.

Note: Disclosure of PHI is ordinarily *not* permitted in response to an Open Records Act request. Contact the Privacy Officer immediately if you receive an Open Records Act request for PHI.

5.5 Verification of Identity Prior to Disclosure of PHI

Prior to making any permitted disclosure of PHI, Covered Components must verify the identity of the person requesting the PHI and the authority of such person or entity to receive such disclosure, if their identity or authority is not already known. Covered Components must also obtain any documentation, statements, or representations that are a condition of the disclosure from the person or entity making the request.

5.5.1 **Verifying a Patient's Identity.**

The patient must provide their name, social security number, date of birth, address on file, and if available a copy of a government issued picture identification. Whenever practicable, requests should be in writing and signed by the patient. A copy of the request should be kept in the patient's file.

5.5.2 **Verifying the Identity and Authority of the Patient's Personal Representative.**

Covered Components must verify the identity *and* authority of personal representatives requesting access to a patient's PHI. Covered Components must (i) verify the name and date of birth of the patient who is the subject of the request; (ii) obtain appropriate documentation supporting the request for access to the PHI, such as guardianship documents, custody orders, power of attorney, or Authorization Form; (iii) verify the requestor's name and obtain a copy of a government issued picture identification; (iv) confirm any limitations regarding the disclosure of information to the personal representative (v) once identity and authority has been confirmed, disclose only the minimum information necessary to fulfill the request.

5.5.3 **Verifying the Identity and Authority of a Public Official.**

Covered Components may rely on any of the following to verify identity of a public official:

5.5.3.1 If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

5.5.3.2 If the request is in writing, the request is on the appropriate government letterhead; or

5.5.3.3 If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate governmental letterhead that the person is acting under the government's authority or other evidence or documentation, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

DPH may rely on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

5.5.3.4 A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority; or

5.5.3.5 If a request is made pursuant to legal process, then a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

5.5.4 **Verifying the Identity and Authority of Law Enforcement Official**.

Covered Components may disclose PHI to a law enforcement official for certain law enforcement purposes. The Covered Component should ask to see the law enforcement official's official identification and the subpoena, summons, request for records, civil or authorized investigative demand, or similar legal process by which the PHI is being requested, and then consult the Privacy Officer. A copy of this legal process should be kept in the patient's file.

6.0 OTHER REQUIREMENTS RELATING TO THE USE AND DISCLOSURE OF PHI

6.1 De-Identification of PHI

Disclosure of properly de-identified information is permitted by the HIPAA Privacy Rule. PHI is de-identified by removing certain individual identifiers to make it impossible to identify the health information as belonging to a particular patient. PHI is properly de-identified only if the information cannot be used alone or in combination with other information to identify a patient who is a subject of the information, **and** there is either a statistician determination pursuant to Paragraph 6.1.1 **or** removal of identifiers pursuant to Paragraph 6.1.2.

6.1.1 **De-Identification Through Statistician Determination**.

Data is "de-identified" if a DPH employee with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for de-identifying data applies such principles and methods to the Data, and determines that such application

results in a very small risk that the de-identified data could be used, alone or in combination with other reasonably available information, to identify an individual whose de-identified PHI will be disclosed. Such a determination must be properly documented.

6.1.2 **De-Identification Through Removal of Identifiers**.

Data is **"**de-identified" through removal of the following identifiers of the individual or the individual's relatives, household members, and employers: name, addresses (except for the State and the first three digits of the zip code, if the current total population of all zip codes with those three digits is more than 20,000), month and day of all dates directly related to an individual, all ages over 89 and all elements of dates indicative of such ages, telephone and facsimile numbers, email addresses, biometric identifiers (including finger and voice prints), unique identifying numbers or codes, full face photographic images, and numbers relating to Social Security, medical records, health plans, accounts, certificates, licenses, motor vehicles and license plates, drivers licenses, device and serial numbers, Internet Protocol (IP), and Universal Resource Locators (URLs).

6.1.3 **Re-identification**.

Covered Components may assign a code or other means to allow de-identified information to be re-identified, provided that the code or other means is not derived from or related to information about the patient and cannot be translated to identify the patient, and the Department does not disclose the code or mechanism for re-identification.

6.2 Limited Data Sets

Covered Components may disclose a limited data set in accordance with DPH Policy CO-12007 (Data Request Policy) and pursuant to a DPH Data Use Agreement with the recipient of the limited data set. A limited data set may contain the following: town, city, state, zip code, date of birth, date of death, admission date, discharge date, ages, gender, race, ethnicity, marital status. However, the following identifiers of the individual or individual's relatives, household members, employers must be removed: name, postal address information (other than town or city, State, and zip code), telephone and facsimile numbers, email addresses, biometric identifiers (including finger and voice prints), unique identifying numbers or codes, full face photographic images, and numbers relating to Social Security, medical records, health plans, accounts, certificates, licenses, motor vehicles and license plates, drivers licenses, device and serial numbers, Internet Protocol (IP), and Universal Resource Locators (URLs).

6.3 Business Associate Agreements

A business associate is a person or organization that, on behalf of the Department, performs or assists in the performance of a function or activity involving the use or disclosure of PHI, or provides services to or for the Department which require access to PHI. All Covered Components must identify Business Associates, so that the appropriate contractual requirements are in place to govern the Business Associates' use of PHI.

Before the Department discloses PHI to a business associate, the associate must sign the DPH Business Associate Agreement, or a contract to which the DPH Business Associate Agreement is attached. Any material breach or violation of the Business Associate Agreement must be reported to the Privacy Officer. If the Business Associate fails to cure the breach and end the violation, then its access to PHI must be cut off, and its contract with DPH must be terminated.

7.0 REQUESTS FOR PHI CONTAINING RECORDS OF TREATMENT OR DIAGNOSIS OF MENTAL ILLNESS, HIV/AIDS, ALCOHOL OR DRUG DEPENDENCY, OR TREATMENT OF THE DEVELOPMENTALLY DISABLED

7.1 Employees are cautioned to consult with the Privacy Officer before releasing PHI which contains any reference to diagnosis or treatment of HIV/AIDS, drug or alcohol dependency or abuse, mental illness, or treatment of the developmentally disabled. Such records may be entitled to heightened legal protection in accordance with

7.1.1 O.C.G.A. § 37-3-166 (records of treatment of mental illness)

7.1.2 O.C.G.A. § 37-4-125 (records of treatment of the developmentally disabled)

7.1.3 O.C.G.A. § 37-7-166 (records of treatment for alcohol or drug dependency or abuse)

7.1.4 O.C.G.A. § 24-12-21 (records of testing, diagnosis, or treatment of HIV/AIDS).

8.0 DOCUMENT RETENTION

All documents required by this Policy must be retained for six years from the date of creation or the date when it was last in effect, whichever is later, including its policies, standard forms and notices, and procedures in written or electronic form, all communications required to be in writing, and any action, activity or designation required to be documented. Although the HIPAA document retention period is six years, consult the Department's Record Retention Policy to ensure compliance with the Department's record retention schedule as well.

9.0 TRAINING

The Office of Human Resources will develop online HIPAA training for use by all members of the workforce, and will collect and maintain a certificate of completion from each employee who completes the training. Training is required for all current employees, and for all new employees within 30 days of becoming employed, regardless of whether or not they work in a Covered Component. The content of the training will include key points of this Policy, and procedures for detecting, guarding against, and reporting malicious software. Periodic security updates will be distributed to the DPH workforce as changes are made to federal HIPAA regulations or this Policy and as needed.

10.0 PATIENT RIGHTS

10.1 Right to Notice of Privacy Practices

A copy of the current DPH Privacy Notice shall be given to each person receiving healthcare service from the Department. Covered Components must make a copy of the notice available to any person upon request, and for patients receiving treatment no later than the date of first service, or in an emergency treatment situation, as soon as reasonably practicable after the emergency. For patients receiving treatment, employees must make good faith efforts to obtain a written acknowledgement of receipt of the notice, and if unsuccessful, document good faith efforts to obtain the acknowledgement and the reasons it was not obtained. The written acknowledgement and documents showing efforts to obtain it must be maintained. The notice should be available at physical service delivery sites and posted in a clear and prominent location. The notice shall be posted on and made available through the Department's website.

10.2 Right to Request Restriction of Uses and Disclosures of PHI

10.2.1 Patients may request that the use and disclosure of their PHI be restricted to treatment, payment or health care operations, disclosures to persons involved in the patient's health care, or disclosures to notify family members or others about the patient's general condition, location or death. The Department is not required to honor such requests, but if it elects to do so, then the restriction must be documented and retained in the patient's file. Notwithstanding such a restriction, however, DPH may disclose the patient's PHI if it is needed for the purpose of treating the patient in the event of an emergency.

10.2.2 Patients may request that their PHI pertaining to a particular heath care item or service *not* be disclosed to the patient's health plan, if that particular health care item or service was paid for without assistance from the patient's health plan. The Department must honor such a restriction. The restriction must be documented and retained in the patient's file.

10.3 Right to Request That Communications Be Made In a Confidential Manner

Covered Components must accommodate reasonable requests by patients to receive communications of PHI by alternate means or at alternate locations or times. Employees must require that the request be in writing where possible. The patient must specify the requested alternate address or other method of contact, but need not give a reason for the request. The request must be documented and retained in the patient's file.

10.4 Right of Access to PHI

10.4.1 A patient has a right of access to inspect and obtain a copy of his or her PHI in a designated record set, for as long as the PHI is maintained in a designated record set. All requests for access must be in writing and must be immediately forwarded to the Privacy Officer, so that the Department can act on the request within 30 days of receipt. Covered Components must document the designated record sets that are disclosed to patients and retain such documentation.

10.4.2 A patient's access to his or her PHI may be denied only in the following circumstances: psychotherapy notes may not be disclosed; the PHI was obtained from someone other than a healthcare provider and confidentiality was promised; or a licensed health care professional has determined that disclosure would endanger the life or safety of the patient or any other person. If access to any part of the patient's PHI is denied, then the patient shall be notified and given an opportunity to have the decision reviewed by a licensed health care professional who was not involved in the original decision.

10.4.3 The patient may request either paper or electronic copies of his or her PHI, and may be charged a reasonable fee to cover the cost of finding, copying, and providing the PHI.

10.5 Right to Request Amendment of PHI

10.5.1 A patient has a right to have the Department amend PHI or a record about him or her in a designated record set, for as long as the PHI is maintained in a designated record set. All requests for amendments must be in writing and specify the reasons for the request, and shall be immediately forwarded to the Privacy Officer, so that the Department can act on the request within 60 days of receipt. The request must be documented and retained in the patient's file, along with any statement of disagreement submitted pursuant to Paragraph 10.5.2.

10.5.2 A patient's request for an amendment to his or her PHI may be denied only in the following circumstances: DPH did not create the PHI and the creator is available to act on the requested amendment; the information to be amended is not part of the designated record set; the PHI is

accurate and complete; or the information is not lawfully subject to access by the patient. If any part of the patient's request is denied, then the patient shall be notified of the reasons, and given an opportunity to submit a statement of disagreement and to have the decision reviewed by a licensed health care professional who was not involved in the original decision.

10.6 Right to Request an Accounting of Disclosures of PHI

A patient has a right to receive an accounting of disclosures of PHI made by the Department in the six years prior to the date on which the accounting is requested. All requests for accountings must be made in writing, and immediately forwarded to the Privacy Officer, so that the Department can act on the request within 30 days of receipt. The request should include the patient's name and specify the time period for which the accounting is being sought. The accounting must include disclosures of PHI for the time requested, including disclosures to or by Business Associates or for research purposes, date of the disclosure(s), name of the person or entity which received the PHI and, if known, the address, and a brief description of the information disclosed. A copy of the written request for an accounting and the accounting provided to the patient must be retained.

11.0 COMPLAINT PROCEDURES

Complaints about the Department's compliance with its privacy policies and procedures and the HIPAA Rule shall be forwarded immediately to the Privacy Officer, along with as much information regarding the complaint as possible, including the complainant's name, contact information, date of incident, nature of complaint, to whom the PHI was improperly disclosed, any harmful effects that resulted, steps requested to limit the harm, and any additional comments. The Privacy Officer will investigate or oversee the investigation of the complaint, determine the appropriate response, and provide a written response to the complainant. Corrective action shall be taken as necessary, and appropriate sanctions will be imposed upon any employee who failed to comply with DPH privacy policies or HIPAA requirements. Documentation of complaints and their disposition will be retained by the Office of the General Counsel.

12.0 SANCTIONS AGAINST EMPLOYEES FOR VIOLATION OF POLICY

12.1 Sanctions

The Department shall apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the Department or the requirements of the HIPAA regulations. Any violation of these policies or the HIPAA Privacy Rule will be reported to the employee's supervisor, the Privacy Officer, and the Office of Human Resources. The Office of Human Resources, will make a recommendation to the employee's supervisor about the appropriate sanction based on the nature of the violation. The type of sanction will vary depending on the severity of the violation, whether it was intentional or unintentional, and whether the employee engaged in a pattern of improper use or disclosure of PHI. Sanctions may include a warning, additional training, re-assignment of job functions, suspension, demotion, or other adverse actions up to and including termination of employment. The responsibility for training and managing the employee's job function will be considered. The employee will receive appropriate notice and opportunity to respond. Violations will be reviewed on a case by case basis, therefore sanctions may vary depending on the nature of violation. However, sanction will be applied with consistency to the extent possible. Sanctions will be documented and retained by the Office of Human Resources.

12.2 Disclosures by Whistleblowers

An employee shall not be subject to sanctions for the inappropriate disclosure of PHI if the employee believes in good faith that the Department has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the Department potentially endangers one or more patients, workers, or the public; and the disclosure is to (i) a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Department; or (ii) an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the Department; or (iii) an attorney retained by or on behalf of the employee for the purpose of determining the legal options of the employee.

12.3 Refraining from Intimidation or Retaliation

The Department may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any patient or other person for (i) filing of a complaint with the Secretary of the U.S. Department of Health and Human Services; (ii) testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing conducted by the Secretary of the U.S. Department of Health and Human Services; or (iii) opposing any act or practice made unlawful by this subchapter, provided the patient 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 PHI in violation of the HIPAA Privacy Rule.

13.0 RESPONDING TO SUSPECTED BREACH OF PHI

If any employee becomes aware of a possible acquisition, access, use, or disclosure of protected health information that is not permitted under HIPAA regulations and this policy, the employee must report the security incident within 24 hours to the Privacy Officer. All such incidents will be investigated by the Security Incident Response Team, and other staff as necessary, in accordance with the Personal Health Information Security Incident Response Protocol GC-00901E.

14.0 RELATED FORMS AND POLICIES

DPH Form GC-00901A Business Associate Agreement

DPH Form GC-00901B Notice of Privacy Practices

DPH Form GC-00901C Authorization For Release of Protected Health Information

DPH Form GC-00901D Authorization For Release of Psychotherapy Notes

DPH Form GC-00901E Personal Health Information Security Incident Response Protocol

DPH Form GC-00901F Technological Safeguards for the Protection of Personal Health Information

DPH Data Use Agreement

DPH Data Request Policy No. CO-12007