EMORY UNIVERSITY HIPAA PRIVACY RULE POLICIES

ADOPTION DATE: September 1, 2016

Table of Contents

GLOSSARY

NOTE: Defined terms are capitalized in text..

"Access" means the ability to read, write, modify, or communicate data/information.

"**Abuse of an Elder Person or Disabled Adult**" means the willful infliction of physical pain, physical injury, Sexual Abuse (as that term is defined in OCGA §30-5-3), mental anguish, unreasonable confinement, or the willful deprivation of Essential Services (as that term is defined in OCGA §30-5-3) to a Disabled Adult or Elder Person. [OCGA §30-5-3].

"Affiliated Covered Entity" means an entity composed of legally separate Covered Entities that are affiliated and that have elected to designate themselves as a single Covered Entity. [45 CFR §164.105(b)(1)].

"**AIDS Confidential Information**" means information which discloses that a person: (a) has been diagnosed as having AIDS; (b) has been or is being treated for AIDS; (c) has been determined to be infected with HIV; (d) has submitted to an HIV test; (e) has had a positive of negative result from an HIV test; (f) has sought and received counseling regarding AIDS; or (g) has been determined to be a person ar risk of being infected with AIDS; and which permits the identification of that person. [OCGA §31-22-9.1].

"Authorization" means written permission from a person to use or disclose his/her Protected Health Information (PHI), which permission contains all of the required elements specified in 45 CFR §164.508(b) unless otherwise appropriately altered by an Institutional Review Board (IRB) or Privacy Board. [45 CFR §164.508].

"Breach" is the acquisition, Access, Use, or Disclosure of Protected Health Information (PHI) in a manner that is not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the PHI.

1. Breach <u>excludes</u>:
    a. Any unintentional Access or Use of PHI by a Covered Component of the Emory University Hybrid Covered Entity, including a Business Associate, if such Access or Use was made in good faith and within the scope of work and does not result in further inappropriate Use or Disclosure.
    b. Any inadvertent Disclosure by a person who is authorized to access PHI controlled by a Covered Component of the Emory University Hybrid Covered Entity to another person also authorized to access PHI controlled by a Covered Component, as long as the information received as a result of such Disclosure does not result in further inappropriate Use or disclosure.
    c. A Disclosure of PHI where an employee of a Covered Component of the Emory University Hybrid Covered Entity has a good faith belief that an unauthorized person who received the information would not reasonably be able to retain such information.

2. An acquisition, Access, Use, or Disclosure of Protected Health Information is presumed to be a Breach unless the Emory University Hybrid Covered Entity, or applicable Business Associate, can demonstrate that there is a low probability that the Protected Health Information has been compromised based on a risk assessment of at least the following factors:
    a. The nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification,
    b. The unauthorized person who used the Protected Health Information or to whom the Disclosure was made,
    c. Whether the Protected Health Information was actually acquired or viewed,
    d. The extent to which the risk to the Protected Health Information has been mitigated, including the extent and efficacy of mitigation, and

    Other mitigating factors considered by the Emory University Hybrid Covered Entity that are relevant to the risk assessment. [45 CFR §164.402].

"Business Associate" is a person or organization (a) that performs for a Covered Entity or Health Care Covered Component, or assists in the performance of, managerial, administrative or consultative-type tasks that help the Covered Entity/Health Care Covered Component carry out its Covered Functions; and (b) that requires access to Protected Health Information (PHI) from a Covered Entity/Health Care Covered Component in order to perform the services that the Business Associate is performing for the Covered Entity/HealthCare Covered Component. Examples of administrative, managerial or consultative type services that a Business Associate might perform for a Covered Entity/Health Care Covered Component to assist in its performance of Covered Functions including claims processing; utilization review; quality assurance; billing benefit management; legal services; accounting; consulting; data aggregation; management; administration; accreditation; or financial services. [45 CFR §160.103].

"Business Associate Agreement" or **"BAA"** means a contractual agreement per which a Business Associate agrees to be bound by all applicable requirements of HIPAA and to handle PHI in accordance with all such requirements. [45 CFR §164.504(e)].

"Business Associate-like Activities" means activities that require access to PHI to perform activities for or on behalf of a Covered Entity or Covered Component to assist the Covered Entity/Component in performing Covered Functions, which activities would make the Emory University unit a Business Associate if it were a separate legal entity.

"**Child**" means any person under 18 years of age. [OCGA § 19-7-5].

"**Child Abuse**" means:

(A) Physical injury or death inflicted upon a Child by a parent or caretaker thereof by other than accidental means; provided, however, that physical forms of discipline may be used as long as there is no physical injury to the Child;

(B) Neglect or exploitation of a Child by a parent or caretaker thereof;

(C) Sexual Abuse (as that term is defined in OCGA §19-7-5) of a Child; or

(D) Sexual Exploitation (as that term is defined in OCGA §19-7-5) of a Child.

However, no Child who in good faith is being treated solely by spiritual means through prayer in accordance with the tenets and practices of a recognized church or religious denomination by a duly accredited practitioner thereof shall, for that reason alone, be considered to be an "abused" Child. [O.C.G.A. §19-7-5]

"**Common Control**" means that an entity has the power, directly or indirectly, to significantly influence or direct the actions or policies of another entity. [45 CFR §164.103].

"**Common Ownership**" means that an entity or entities possess an ownership or equity interest of 5% or more in another entity. [45 CFR §164.103].

"**Confidential Raw Research Data**" means medical information, interview responses, reports, statements, memoranda, or other data relating to the condition, treatment, or characteristics of any person which are gathered by or provided to a researcher:

(a) In support of a Research study approved by an appropriate research oversight committee of a hospital, health care facility, or educational institution; and
(b) With the objective to develop, study or report aggregate or anonymous information not intended to be used in any way in which the identity of an individual is material to the results.

The term Confidential Raw Research Data does not include published compliations of the raw research data created by the researcher or the researcher's published summaries, finding, analyses, or conclusions related to the Research study. [OCGA §24-12-2]

"**Covered Component"** is a component of a Hybird Covered Entity that functions as a Health Plan, Health Care Clearinghouse; or Health Care Provider that transmits any Health Information in electronic form in connection with a transaction covered under HIPAA regulations, as each of the foregoing capitalized terms is defined at 45 CFR §160.103. [45 CFR §160.103].

"Covered Entity" 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 under HIPAA regulations, as each of the foregoing capitalized terms is defined at 45 CFR §160.103,. [45 CFR §160.103].

"Covered Functions" are those functions that a Health Care Covered Component or Covered Entity perform that make it a Health Plan, Health Care Provider or Health Care Clearinghouse. [45 CFR §164.103].

"Data Use Agreement" a written agreement between a Covered Entity or Covered Component of a Hybrid Covered Entity and a person or entity that is seeking access to a Limited Data Set held by the Covered Entity or Covered Component for Research, Health Care Operations or

public health purposes. The agreement must contain the elements set forth at 45 CFR §164.514(e)(4)(ii). [45 CFR §164.514(e)].

"**Deceased Individual**" means and Individual who is deceased.

"Designated Record Set" means (a) a group of records maintained by or for a Covered Entity or Health Care Covered Component that is: (i) the medical records and billing records about Individuals maintained by or for a covered Health Care Provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a Health Plan; or (iii) used, in whole or part, by or for the Covered Entity to make decisions about Individuals. As used in this definition "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 or a Health Care Covered Component. [45 CFR §164.501].

"**Disabled Adult**" means a person 18 years of age or older who is not a resident of a long-term care facility, but who:

(A) Is mentally or physically incapacitated;

(B) Has Alzheimer's disease, as defined in OCGA §31-8-180; or

(C) Has dementia, as defined in OCGA § 16-5-100.

"Disclosure" (or "Disclose/d" or "Disclosing") means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information. [45 CFR §160.103].

"**Elder Person**" means a person 65 years of age or older who is not a resident of a long-term care facility. [OCGA §30-5-3]

"**Electronic Media**" means (a) electronic storage material on which data is or may be recorded electronically; (b) transmission media used to exchange information already in electronic storage media (e.g., the Internet), excluding paper facsimile and voice via telephone if the information being exchange did not exist in electronic form immediately before the transmission. [45 CFR §160.103].

"**Electronic Protected Health Information**" or "**ePHI**" means individually identifiable health information that is transmitted by electronic media or maintained in electronic media. [45 CFR §160.103].

"Emory" means Emory University.

"**Emory Healthcare"** or "**EHC**" means Emory Healthcare, Inc.

"Emory Healthcare Affiliated Covered Entity" is the name of the Affiliated Covered Entity that legally separate Covered Entities under Common Ownership or Common Control with the Emory Healthcare, Inc. have elected to form. [45 CFR §164.105(b)]

"Emory University Hybrid Covered Entity" is the name of the Hybrid Covered Entity that the Health Care Covered Components of the Emory University Hybrid Covered Entity have elected to form.

"**Financial Remuneration**" means direct or indirect payment from or on behalf of a third party whose product or service is being described, excluding any payment for treatment of an Individual. [45 CFR §164.501].

"**Health Care**" means care, services, or supplies related to the health of an Individual. Health Care includes but is not limited to (a) preventative, 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 that affects the structure or function of the body; and (b) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. [45 CFR §160.103].

"Health Care Clearinghouse" means a public or private entity that (a) processes or facilitates the processing of Health Information received from another entity in a nonstandard format, or containing nonstandard data content, into standard data elements or a standard transaction; or (b) receives a standard transaction from another entity and processes or facilitates the processing of Health Information into nonstandard format or nonstandard data content for the receiving entity. [45 CFR §160.103].

"Health Care Covered Component" or "**Covered Component**" is a unit of a Hybrid Covered Entity that performs Covered Functions, and in the case of a Health Care Provider transmits any Health Information in electronic form in connection with a transaction covered under HIPAA regulations, but only to the extent it performs Covered Functions, or activities that would make it a Business Associate of a component that performs Covered Functions if the two components were separate legal entities. [45 CFR §§164.103 & .105(a)(2)(iii)(C)].

"Health Care Operations" means any of the activities listed at 45 CFR §164.501 under the definition of this term when such activities are carried out by a Covered Entity or Covered Component and are related to Covered Functions. Examples of these activities include, but are not limited to, quality assessment and improvement; reviewing health care professional competence; training health care and non-health care providers; conducting or arranging for medical review, legal or audit services; business planning and development; and customer service. Health Care Operations do not include Research. [45 CFR § 164.501].

"Health Care Provider" or **"Provider"** means any person or organization that furnishes, bills or is paid for Health Care in the normal course of business. [45 CFR § 160.103].

"**Health Information**" means any information, including genetic information, whether oral or recorded in any form, that (a) 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 that (b) 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. [45 CFR §160.103].

"Health Oversight Agency" means an agency or authority of the United States, a U.S. state/territory or political subdivision thereof, an Indian tribe, or a person or entity acting under a grant of authority from, or contract with, such agency or authority that is authorized by law to oversee the Health Care system (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. The term includes employees, agents or contractors of the agency/authority or of the persons/entities to whom it has granted authority. [45 CFR §164.501].

"Health Plan" means an individual or group plan that provides, or pays the cost of, medical care, but excluding those entities listed within the definition of that term provided at 45 CFR §160.103. [45 CFR § 165.103].

"HIPAA" means the United States Health Insurance Portability and Accountability Act of 1996 and all implementing regulations.

"HIPAA-Covered Billing" means transmitting Health Information in electronic form in connection with a transaction covered under HIPAA (i.e. submitting a claim to a health plan electronically).

"Hybrid Covered Entity" means a single legal entity (a) that is a Covered Entity; (b) that conducts business activities that include both Covered and Non-Covered Functions; and (c) that designates Health Care Covered Components in accordance with 45 CFR §164.105(a)(2)(iii)(C). [45 CFR § 164.103].

"**Individual**" means a person who is the subject of Protected Health Information. [45 CFR §160.103].

"Individually Identifiable Health Information" means Health Information, including demographic information collected from an Individual that is: (a) created or received by a Health Care Provider, Health Plan, employer, or Health Care Clearinghouse; and (b) 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 (i) that identifies the Individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual. [45 CFR §160.103].

"Institutional Review Board (IRB)" is a committee established pursuant to the federal Common Rule (as described at 45 CFR Part 46 and 21 CFR Parts 50 and 56) to initially review and provide continuing oversight for Research that involves human subjects. At Emory, the IRB is the Emory University IRB, or another lawfully constituted IRB with which Emory has

contracted to provide review and oversight for Research involving human subjects. [45 CFR Part 46; 21 CFR Parts 50 & 56].

"**Marketing**" means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service excluding communications made:

(a) to provide refill reminders or communicate about a drug/biologic currently being prescribed for an Individual only if any Financial Remuneration received by a Covered Entity in exchange for making the communication is reasonably related to a Covered Entity's cost of making the communication; or

(b) for the following Treatment and Health Care Operations purposes when the Covered Entity does not receive Financial Remuneration in exchange for making the communication: (i) Treatment of an Individual by a Health Care Provider; (ii) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits, of the Covered Entity making the communication; or (iii) for case management or care coordination, contacting Individuals with information about Treatment alternatives, and related functions that are not Treatment. [45 CFR §165.501].

"**Medical Facility**" includes, facility without being limited to, an ambulatory surgical treatment center as defined in subparagraph (C) of paragraph (4) of OCGA §31-7-1 and a freestanding imaging center as defined in subparagraph (G) of paragraph (4) of OCGA §31-7-1. [OCGA § 31-7-9].

"Minimum Necessary" means the minimum necessary type and amount of Health Information necessary to accomplish the intended purpose of the Use, Disclosure or request for information. [45 CFR §164.502(b)].

"**Neglect of an Elder Person or Disabled Adult**" means the absence or omission of essential services to the degree that it harms or threatens with harm the physical or emotional health of a Disabled Adult or Elder Person. [OCGA §30-5-3]

"Non-Covered Component" means any unit of a Hybrid Covered Entity that (a) does not perform Covered Functions or act as a Business Associate on behalf of a Covered Component; or (b) in the case of units that have activities in addition to the performance of Covered Functions, is performing an activity that does not constitute a Covered Function or serving as a Business Associate of a Covered Component; or (c) a Health Care Provider that does not transmit any Health Information in electronic form in connection with a transaction covered under HIPAA regulations. [45 CFR §§164.103, .105].

"**Organized Health Care Arrangement (OHCA)**" means:

(a) A clinically integrated care setting in which Individuals typically receive Health Care from more than one Health Care Provider;

(b) An organized system of Health Care in which more than one Covered Entity participates and in which the participating Covered Entities:

i. Hold themselves out to the public as participating in a joint arrangement; and
ii. Participate in joint activities that include at least one of the activities described in the definition of Organized Health Care Arrangement at 45 CFR §§160.103(2)(ii)(A)-(C).

(c) Certain group Health Plan arrangements as described at 45 CFR §§160.103(3)-(5). [45 CFR §160.103].

"Licensed Mental Health Professional" means a licensed psychiatrist, psychologist, clinical social worker, clinical nurse specialist in psychiatry/mental health, marriage and family therapist or professional counselor. [OCGA §24-5-501]

"Notice of Privacy Practices (NPP)" means the written document that summarizes the Emory Hybrid Affiliated Covered Entity's privacy practices and which is provided to Individuals as prescribed by HIPAA. [45 CFR § 164.520].

"Payment" means activities (a) undertaken by a Health Plan to obtain premiums or determine coverage and provision of benefits; or (b) undertaken by a Health Care Provider or Health Plan to obtain or provide reimbursement for providing Health Care. [45 CFR § 164.501].

"Protected Health Information" or **"PHI"** means Individually Identifiable Health Information that is (a) transmitted by electronic media; (b) maintained in electronic media; or (c) transmitted or maintained in any other form or medium; provided, however, that PHI does not include any Individually Identifiable Health Information in (i) Education Records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, and all implementing regulations, including, but not limited to, records described at 20 U.S.C. §1232g(a)(4)(B)(iv) of FERPA; and (ii) employment records held by a Covered Entity in its role as an employer. [45 CFR §160.103].

"Privacy Board" means a committee that has members with varying backgrounds and appropriate professional competency a s necessary to review the effect of a Research protocol on an Individual's privacy rights and related interests. The committee must include at least one member who is not affiliated with the Covered Entity; not affiliated with the Research sponsor; and not related to any person affiliated with the Covered Entity or sponsor. No member of the committee can review any project in which the member has a conflict of interest. [45 CFR §164.512(i)(B)].

"Psychotherapy" means the employment of Psychotherapeutic Techniques. [OCGA. §24-5-501].

"**Psychotherapy Notes**" means 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 Individual's medical record excluding: medication prescription and monitoring; counseling session start and stop times; modalities and frequencies of treatment furnished; results of clinical tests; and any summary of diagnosis, functional status, treatment plan, symptoms, prognosis and progress to date. [45 CFR §164.501].

"Psychotherapeutic Techniques" means those specific techniques involving the in-depth exploration and treatment of interpersonal and intrapersonal dynamics by professionals who are licensed to administer such techniques under the laws of the State of Georgia (i.e., licensed psychiatrists, psychologists, clinical social worker, clinical nurse specialist in psychiatry/mental health, marriage and family therapist or professional counselor). [OCGA §§24-5-501 & 43-10A-3].

"Public Health Authority" means an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as a part of its official mandate. [45 CFR §164.501].

"Research" means a systematic investigation, including Research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. [45 CFR §164.501].

"Sale of PHI" means the transaction that takes place when a Covered Component of the Emory University Hybrid Covered Entity or its Business Associate directly or indirectly receives Financial Remuneration from, or on behalf of, the recipient of the PHI in exchange for the PHI; provided, however, that certain Disclosures by a Covered Component described in *Policy A.10, Sale of PHI* are not considered to be a Sale of PHI.

"**School**" means any public or private pre-kindergarten, elementary school, secondary school, technical school, vocational school, college, university, or institution of postsecondary education. [OCGA § 19-7-5]

"**Subcontractor**" means a person to whom a Business Associate delegates a function, activity, or service other than in the capacity of a member of the workforce of the Business Associate. [45 CFR § 160.103].

"**Transaction**" means the transmission of information between two parties to carry out financial or administrative activities related to Health Care (e.g., payment for a Health Care claim, coordination of benefits). [45 CFR §160.103].

"Treatment" means the provision, coordination, or management of Health Care and related services by one or more Health Care Providers, including the coordination or management of Health Care by a Health Care Provider with a third party; consultation between Health Care Providers relating to a patient; or referral of a patient from one Health Care Provider to another. Additionally, and solely for purposes of determining whether Research includes Treatment, the definition of Treatment shall also include the administration of a drug, device or procedure to normal, healthy volunteers in the context of a clinical investigation. [45 CFR §164.501].

“Use” means sharing, employment, application, utilization, examination, or analysis of Individually Identifiable Health Information within an entity that maintains such information. [45 CFR §160.103].

“Use Preparatory to Research” means Use or Disclosure of PHI sought solely to review the PHI as necessary to prepare a Research protocol or for similar purposes preparatory to Research. [45 CFR §164.512(i)(1)(ii)].

“Workforce” means employees,volunteers, trainees and other persons whose conduct, in the performance of work for a Covered Entity or Business Associate is under the direct control of the Covered Entity or Business Associate, whether or not they are paid. [45 CFR §160.103].

“**Waiver of Authorization**” means a alteration to or waiver, in whole or part, of the Indiviudal Authorization required for use of PHI for Research granted by an Institutional Review Board or a Privacy Board pursuant to the criteria set forth at 45 CFR §164.512(i). [45 CFR §164.512(i)].

SECTION A: GENERAL HIPAA POLICIES

A.1. FORMAT AND ORGANIZATION OF THE EMORY UNIVERSITY HIPAA PRIVACY RULE POLICIES

PURPOSE OF POLICY

This policy sets forth information about the formatting and organization of the *Emory University HIPAA Privacy Rule Policies,* also sometimes referred to in this document as the "Policies."

POLICY

Defined Terms

Defined terms are capitalized and their definitions are included in the *Glossary* at the beginning of these Policies. Additionally, the definitions of certain defined terms may appear at the time of use within a policy for convenience and to provide additional clarity.

Organization of Policies

Policy A.2, *HIPAA Administrative Structure Policy* applies to, and has been adopted by Emory University and Emory Healthcare, Inc. Unless expressly stated otherwise in an individual policy, all Policies subsequent to Policy A.2 apply only to Protected Health Information (PHI) contained in records owned by Covered Components of the Emory University Hybrid Covered Entity (as defined in Policy A.2.) and conduct of such Covered Component with respect to such PHI, with the exception of the Emory University Health Plan, which has separate HIPAA privacy policies.

REFERENCES: 45 CFR §164.105
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

A.2. HIPAA ADMINISTRATIVE STRUCTURE POLICY

PURPOSE OF POLICY

Policy A.2. is adopted by both Emory University and Emory Healthcare, Inc., and sets forth the HIPAA administrative structure that has been adopted by and for Emory University, Emory Healthcare, Inc. and certain legally separate entities under common ownership and/or control of Emory Healthcare, Inc. as described below. This administrative structure is adopted and documented in satisfaction of the regulatory requirements at 45 CFR § 164.105. This Policy does the following:

(a) Reaffirms the designation of Emory University as a Hybrid Covered Entity and identifies Covered Components.
(b) Designates Emory Healthcare, Inc. and certain legally separate entities under common ownership and/or control of an Affiliated Covered Entity.

(c) Documents the Organized Health Care Arrangement (OHCA) between the Emory University Hybrid Covered Entity and the Emory Healthcare Affiliated Covered Entity.
(d) Documents the designation of privacy and security officers.
(E) Sets forth the scope and applicability of the Emory University HIPAA Privacy Rule Policies, Emory University Health Plan HIPAA Privacy Rule Policies and Emory Healthcare HIPAA Privacy Rule Policies.

DEFINITIONS

The following defined terms are listed here for convenience. These terms also appear in the Glossary.

"Business Associate-like Activities" means activities that require access to PHI to perform activities for or on behalf of a Covered Entity or Covered Component to assist the Covered Entity/Component in performing Covered Functions, which activities would make the Emory University unit a Business Associate if it were a separate legal entity.

"HIPAA-Covered Billing" means transmitting Health Information in electronic form in connection with a transaction covered under HIPAA (i.e. submitting a claim to a health plan electronically).

"Treatment" means the provision, coordination, or management of Health Care and related services by one or more Health Care Providers, including the coordination or management of Health Care by a Health Care Provider with a third party; consultation between Health Care Providers relating to a patient; or referral of a patient from one Health Care Provider to another. Additionally, and solely for purposes of determining whether Research includes Treatment, the definition of Treatment shall also include the administration of a drug, device or procedure to normal, healthy volunteers in the context of a clinical investigation. [45 CFR § 164.501].

POLICY

Designation of Emory University as Hybrid Covered Entity

By consensus of Emory University's President and other University administrative officials at a meeting held on February 25, 2003, Emory University elected to designate itself as a Hybrid Covered Entity under 45 CFR §164.105**.** This overarching designation is reaffirmed with the adoption of these Policies on their specified adoption date.

Health Care Covered Components within the Emory University Hybrid Covered Entity

Emory University hereby designates the following units as "Health Care Covered Components" or **"**Covered Components**"** of the Emory University Hybrid Covered Entity:

(a) **Emory University Health Plan** – NOTE: This Covered Component is governed by separate privacy and security policies.
(b) **Emory University Student Health Service** to the extent to which Educational Records subject to the Family Educational Rights and Privacy Act (FERPA) are not involved, and to the

extent that its Health Care Providers are providing Treatment through the Emory University Student Health Service and collecting Payment for such Treatment using HIPAA-Covered Billing.

(c) **Oxford College of Emory University Student Health Service** to the extent to which Educational Records subject to FERPA are not involved, and to the extent that its Health Care Providers are providing Treatment through the Oxford College of Emory University Student Health Service and collecting Payment for such Treatment using HIPAA-Covered Billing.

(d) **Emory University Autism Center** to the extent that its Health Care Providers are providing Treatment through the Emory University Autism Center and collecting Payment for such Treatment using HIPAA-Covered Billing.

(e) **Emory Psychoanalytic Institute** to the extent that its Health Care Providers are providing Treatment through the Emory Psychoanalytic Institute and collecting Payment for such Treatment using HIPAA-Covered Billing.

(f) **Emory Clinical and Translational Research Lab (ECTRL)** to the extent that its Health Care Providers are providing Treatment or Health Care services through ECTRL and collecting Payment for such services using HIPAA-Covered Billing.

(g) Emory University School-Based Health Care Providers:

(i) **Emory University School of Medicine Covered Component** consisting of School of Medicine Health Care Providers who are providing Treatment (or Research that includes Treatment) through the School of Medicine and collecting Payment using HIPAA-Covered Billing, if any.

(ii) **Emory University School of Nursing Covered Component** consisting of School of Nursing Health Care Providers who are providing Treatment (or Research that includes Treatment) through the School of Nursing and collecting Payment for such Treatment using HIPAA-Covered Billing, if any.

(h) **Units Performing Business Associate-like Activities**: Units or portions of units within Emory University that perform Business Associate-like Activities for or on behalf of a Covered Component are considered to be a Covered Component when performing those Business Associate-like Activities. These units include, but are not limited to:

Controller's Office
Bursar's Office
Office of Clinical Research
Schools or units within schools assisting a Covered Component in performing covered functions.
Clinical Trials Audit and Compliance
Finance Office
Compliance Office
Internal Audit
Libraries and Information Technology
Office of the General Counsel
Insurance & Risk Management
Radiation Control Council and Committees and Radiation Safety
Environmental Health & Safety Office
Institutional Review Board
Institutional Biosafety Committee

Administrative offices of any of Covered Component when assisting the Covered Component in performing Covered Functions.

List of Covered Components: From time to time, the Emory University Hybrid Covered Entity may add or remove Covered Components. The Emory University Privacy Officer shall maintain a current list of Covered Components within the Emory University Hybrid Covered Entity.

Provision of Treatment On Behalf of/Through the Emory Healthcare Affiliated Covered Entity: If, and when, any Emory University Health Care Provider provides Treatment and collects Payment for such Treatment on behalf of or through the Emory Healthcare Affiliated Covered Entity, that provider is considered to be operating as a part of the Emory Healthcare Affiliated Covered Entity and is subject to the Emory Healthcare Affiliated Covered Entity's HIPAA Privacy Rule Policies. Similarly, Treatment or other Covered Functions or Business Associate-like Activities provided by Emory University faculty, staff or students at, through, or on behalf of legally separate entities under common ownership and/or control of Emory Healthcare, Inc., come under the Emory Healthcare Affiliated Covered Entity's administrative structure and its HIPAA Privacy Rule Policies.

Appointment of Privacy Contact Person: Each Covered Component within the Emory University Hybrid Entity shall appoint an individual to serve as a Privacy Contact Person and shall inform the Emory University Privacy Officer of this individual's name, title and contact information. The Privacy Contact Person shall perform the responsibilities assigned to that position under these Policies and shall coordinate with the University Privacy Officer concerning implementation of these polices within the Privacy Contact Person's Covered Component.

Non-Covered Components: Any components of the Emory University Hybrid Covered Entity that are not designated as Covered Components are considered to be non-Covered Components. Covered Components of the Emory University Hybrid Covered Entity shall protect Protected Health Information (PHI) (including electronic PHI) and may not share or disclose PHI with non-Covered Components except as expressly permitted by HIPAA.

Units are only Covered Components to the Extent they Perform Covered Functions or Business Associate-like Activities: Units that perform both Covered Functions and non-Covered Functions are Covered Components of the Emory University Hybrid Covered Entity only to the extent that, and when, they perform Covered Functions, or Business Associate-like Activities.

Provision of Treatment without Charge or Without Use of HIPAA-Covered Billing: Certain Emory University units employ Health Care Providers who provide Treatment without charge, or collect Payment for such Treatment without using HIPAA-Covered Billing. Such units/Health Care Providers are not considered to be a Covered Component of the Emory University Hybrid Covered Entity. Units/Health Care Providers that currently fall within this category include, but are not limited to, the following:

- Emory University Faculty Staff Assistance Program
- Emory University Counseling and Psychological Services (CAPS).

●Emory University Psychological Center
●Emory University Child Study Center
●Emory University First Responders
●Emory University Hope Clinic
●Schools of Public Health, Nursing and Medicine and Department of Psychology Health Care Providers who provide Treatment without charge or without using HIPAA-Covered Billing.

Research: Research activities carried out by the Emory University Hybrid Covered Entity fall into one of the following categories, as determined by the Emory IRB:

(a) **Research Activities that Do Not Include Treatment** – Research activities carried out by the Emory University Hybrid Covered Entity that do not include Treatment shall take place in a non-Covered Component, and results/data/records from such Research activities shall be kept in a Research record that is separate from any medical record or other portion of a Designated Record Set maintained by a Covered Entity/Covered Component concerning a Research participant, and any Individually Identifiable Health Information contained in the Research record shall not be considered to be PHI.

(b) **Research Activities that Include Treatment and HIPAA-Covered Billing** -- Research activities carried out by the Emory University Hybrid Covered Entity that include Treatment and for which Payment is collected using HIPAA-Covered Billing will take place within a Covered Component of the Emory University Hybrid Covered Entity, and any Individually Identifiable Health Information collected as part of the Research shall be considered to be PHI. Any results/data/records from such Research conducted within a Covered Component may be included, as appropriate, in a medical record or other portion of a Designated Record Set maintained by a Covered Entity/Covered Component and/or in a separate Research record concerning a Research participant.

(c) **Research Activities that Include Treatment, but do not Include HIPAA-Covered Billing** – Research activities carried out by the Emory University Hybrid Covered Entity that include Treatment but for which there is no HIPAA-Covered Billing must take place in a non-Covered Component, and results/data/records from such Research activities kept in a Research record that is separate from any medical record or other portion of a Designated Record Set maintained by a Covered Entity/Covered Component concerning a Research participant, and any Individually Identifiable Health Information contained in the Research record shall not be considered to be PHI. Any Individually Identifiable Health Information related to the Research Participant's Treatment, however, may be included in a Designated Record Set maintained by a Covered Entity/Covered Component in accordance with the rules for medical documentation established by the unit maintaining the Designated Record Set; provided, however, that such information shall be considered to be the PHI of the Covered Enity/Covered Component and may only be accessed in accordance with HIPAA requirements and the Covered Entity's/Covered Component's HIPAA policies.

Role of the IRB: The Emory IRB is responsible for determining when Research involves personnel from a Covered Component and includes Treatment for which Payment is collected using HIPAA-Covered Billing, as those terms are defined in these Policies.

Persons Who Work for a Health Care Covered Component and a Non-Covered Component: If a person is a member of the workforce of a Health Care Covered Component and a Non-Covered Component, that person may not Use or Disclose PHI created or received in the course of work for the Health Care Covered Component except as expressly permitted by HIPAA.

REFERENCES: 45 CFR § 164.105; https://privacyruleandresearch.nih.gov/pr_06.asp

Designation of Emory Healthcare Affiliated Covered Entity

In accordance with 45 CFR § 164.105(b)(1), legally separate Covered Entities that are affiliated and under common ownership and control have designated themselves as an Affiliated Covered Entity, referred to in these Policies as the "Emory Healthcare Affiliated Covered Entity." All legally separate entities that fall under the jurisdiction of Emory Healthcare's Privacy Officer and the Emory Healthcare HIPAA Privacy Rule Policies are included within the Emory Healthcare Affiliated Covered Entity. As of this time, these entities include, but are not limited to Emory Healthcare, Inc., Emory University Hospital, Emory University Hospital Midtown, and The Emory Clinic, Inc., as well as others. From time to time, the Emory Healthcare Affiliated Covered Entity may add or remove Covered Entities. The designated Privacy Officer for the Emory Healthcare Affiliated Covered Entity shall maintain a current list of the entities included within the Emory Healthcare Affiliated Covered Entity.

REFERENCE: 45 CFR §164.105(b)(1).

Designation of Emory University Hybrid Covered Entity and Emory Healthcare Affiliated Covered Entity Organized Health Care Arrangement

The Emory University Hybrid Covered Entity and the Emory Healthcare Affiliated Covered Entity have entered into and participate in an Organized Health Care Arrangement (OHCA).

Designation of Other Organized Health Care Arrangements (OHCA) in which the Emory University and/or Emory Healthcare, Inc. is a Participant

Emory University and Emory Healthcare, Inc. participate in the following OHCA:

(a) Emory/Grady Hospital OHCA created per agreement between Emory University, Emory Healthcare, Inc. and Grady Hospital.

REFERENCE: 45 CFR § 160.103.

Designation of Privacy and Security Officers

Emory University Hybrid Covered Entity Privacy Officer: Emory University has designated the Emory University Chief Compliance Officer to serve as the Privacy Officer for all Covered Components within the Emory University Hybrid Cover Entity except for the Emory University Health Plan.

Contact information for the Emory University Privacy Officer is as follows: Emory University, Office of Research Compliance, Ste. 4-105, 1599 Clifton Rd., N.E., Atlanta, GA 30322, Mailstop: 1599/001/1AY. Phone: (404) 727 2398. FAX: (404) 727-2328.
Email: orc@emory.edu.

Emory University Health Plan: Emory University has designated a Privacy Officer for the Emory University Health Plan Covered Component. The Emory University Health Plan has a separate Notice of Privacy Practices and separate polices. Contact information the Emory University Health Plan Privacy Officer is as follows: First Floor 1599 Clifton Rd., Atlanta, GA 30322. Phone: (404) 727-7613.

Emory Healthcare Affiliated Covered Entity Privacy Officer: Emory Healthcare, Inc. has designated the Emory Healthcare Chief Compliance Officer to serve as the Privacy Officer for the Emory Healthcare Affiliated Covered Entity. Contact information for the Emory Healthcare Affiliated Covered Entity Privacy Officer is as follows: Emory Healthcare, Inc., Chief Compliance Officer, Ste. 610, Decatur Plaza, 101 W. Ponce de Leon Ave., Decatur, GA 30030. Phone: (404) 778-2186. FAX: (404) 778-2755. Email: anne.adams@emoryhealthcare.org

Emory University Hybrid Covered Entity and Emory Health Care Affiliated Covered Entity Security Officer: Emory University and Emory Healthcare, Inc. have designated the Chief Information Security Officer for Emory Enterprise-wide Information Technology Systems as the Security Officer for all Covered Components within the Emory University Hybrid Covered Entity, including the Emory University Health Plan, and for the Emory Healthcare Affiliated Covered Entity. Additionally, both the Emory University Hybrid Covered Entity and the Emory Health Care Affiliated Covered Entity operate under a single set of security policies (the "Security Policies").
Contact information for the Chief Information Security Officer is as follows: Emory University, Information and Technology Services, Ste. 500, North Decatur Bldg., 1784 N. Decatur Rd., Atlanta, GA 30322, Mailstop: 1784-001-1AF (OIT VP & CIO). Phone: (404) 727-2630. FAX:
Email: brad.sanford@emory.edu

Scope and Applicability of Policies

Adoption of Policies: The Emory University Hybrid Covered Entity, Emory University Health Plan and Emory Healthcare Affiliated Covered Entity have each adopted and implemented policies and procedures that are designed to meet all HIPAA requirements regarding PHI. From time to time, each entity will make such changes to its policies and procedures as may be necessary, including changes required in order to comply with law.

Emory University Hybrid Covered Entity: The Emory University HIPAA Privacy Rule Policies apply to all Covered Components within the Emory University Hybrid Covered Entity except for the Emory University Health Plan. Within such Covered Components, the Emory University HIPAA Privacy Rule Policies apply to (a) all employees, students, residents, fellows, visiting scholars, students, professionals, volunteers, and agents, who are involved in the performance of Covered Functions for or on behalf of Covered Components, or the performance of Business Associate-like Activities; (b) who Use or Disclose PHI owned by the Covered

Components of the Emory University Hybrid Covered. Additionally, *Policy D.14, HIPAA Policy Regarding the Use and Disclosure of PHI for Research Purposes and the Role of the Institutional Review Board* applies to any employees; students; residents; fellows; visiting scholars; students and professionals; and volunteers who Use or Disclose for Research PHI owned by the Covered Components of the Emory University Hybrid Covered Entity or by the Emory Healthcare Affiliated Covered Entity.

Emory University Health Plan: The Emory University Health Plan has separate HIPAA privacy policies. Thes Emory University HIPAA Privacy Rules Policies do not include within their scope the Emory University Health Plan.

Emory Healthcare Affiliated Covered Entity: The Emory Healthcare HIPAA Privacy Rule Policies apply to all Covered Entities within the Emory Healthcare Affiliated Covered Entity. Within such Covered Entities, applicable Emory Healthcare HIPAA Privacy Rule Policies apply to all employees, students, residents, fellows, visiting scholars, students, professionals, and volunteers, who: (a) are involved in the performance of Covered Functions for or on behalf of the Covered Entities, or the performance of functions that would make them Business Associates of the Covered Entities; or (b) who use or disclose Protected Health Information owned by the Covered Entities of the Emory Healthcare Affiliated Covered Entity. The Emory Healthcare HIPAA Privacy Rule Policies are located at https://hipaa.emory.edu/home/Policies/index.html. Emory Healthcare log-in credentials are required to access these policies.

Impact of State Law: The Emory Hybrid Covered Entity is subject to the laws of the State of Georgia. In the event of a conflict between HIPAA requirements and the laws of the State of Georgia, the laws that have the stricter privacy obligations or that confer the most rights upon Individuals will govern. Accordingly, throughout these Policies references are included to the laws of the State of Georgia that must be followed in addition to, or in lieu of, HIPAA requirements.

REFERENCES: 45 CFR §§ 164.103, .105; 164.530(i)(1).

Policy Jurisdiction and Jurisdiction of Security and Privacy Officers

Policy Jurisdiction: Policy jurisdiction with respect to specific records is determined by ownership and type of records. Specifically:

- Records containing PHI that are owned by the Emory University Hybrid Covered Entity and/or a Covered Component thereof are subject to the Emory University Hybrid Covered Entity's HIPAA Privacy Rule Policies.
- Records containing PHI that are owned by that Emory Healthcare Affiliated Covered Entity are subject to the Emory Healthcare HIPAA Privacy Rule Policies.
- In addition to being covered by one of the aforesaid set of privacy policies, records containing ePHI are also subject to the Security Policies.

Security Officer Jurisdiction:
The Security Officer shall have jurisdiction over all activities subject to HIPAA Security Policies that are undertaken by or on behalf of the Emory University Hybrid Covered Entity or the Emory Healthcare Affiliated Covered Entity, or that involve e-PHI owned by either of these entities.

Privacy Officer Jurisdiction:
●The Privacy Officer for the Emory University Hybrid Covered Entity has jurisdiction over all activities subject to Emory University HIPAA Privacy Rule Policies that are undertaken by or on behalf of the Emory University Hybrid Covered Entity and/or that involve any records containing PHI owned by the Emory University Hybrid Covered Entity or a Covered Component thereof.

●The Privacy Officer for the Emory Healthcare Affiliated Covered Entity has jurisdiction over all activities subject to the Emory Healthcare HIPAA Privacy Rule Policies that are undertaken by or on behalf of the Emory Healthcare Affiliated Covered Entity and/or that involve any records containing PHI owned by the Emory Healthcare Affiliated Covered Entity.

Jurisdiction Over Matters Involving Possible Unauthorized Uses or Disclosures (e.g., Breaches):
●In the event of a matter involving a possible unauthorized Use or Disclosure of records or other materials consisting entirely or primarily of electronic PHI ("ePHI") owned by the Emory University Hybrid Covered Entity or the Emory Healthcare Affiliated Covered Entity, the Security Officer will have primary responsibility for the investigation and management of the matter.

●In the event of a matter involving possible unauthorized Use or Disclosure of records or other materials consisting entirely or primarily of hardcopy PHI owned by the Emory University Hybrid Covered Entity, the Privacy Officer for the Emory University Hybrid Covered Entity will have primary responsibility for investigation and management of the matter.

●In the event of a matter involving possible unauthorized Use or disclosure of records or other materials consisting entirely or primarily of hardcopy PHI owned by the Emory Health Care Affiliated Covered Entity, the Privacy Officer for the Emory Healthcare Affiliated Covered Entity will have primary responsibility for investigation and management of the matter.

●In matters involving multiple types of PHI owned by multiple parties, the Privacy Officers and Security Officer shall mutually agree amongst themselves as to who will have primary responsibility for management of the matter. Each Privacy Officer and Security Officer agrees to cooperate with and assist in the investigation and management of any matter arising under these Policies, no matter which Privacy or Security Officer has primary responsibility for the matter.

REFERENCES: 45 CFR §§ 164.308(a)(2); .530(a)(1)(i), (2) & (j).

REFERENCES: Listed within Policy.
DATE OF POLICY: April 14, 2003
REVISED: November 22, 2016

A.3. GENERAL ADMINISTRATIVE POLICIES

PURPOSE OF POLICY

The purpose of this policy is to set forth several general administrative policies and processes, including those regarding: (a) complaints; (b) training; (c) safeguards; (d) sanctions; (e) mitigation of harm; and (f) prohibitions against intimidation, retaliation or waivers of rights.

POLICY

Complaints and Designation of an Office to Receive Complaints

The Emory University Hybrid Covered Entity has designated the Emory Healthcare Privacy Officer, Emory Healthcare, 101 W. Ponce de Leon Ave., 2nd Floor, Suite 242, Decatur, GA 30030 to serve as the unit that is available to receive such complaints. The Emory Healthcare Privacy Officer shall review any complaints as they are received and refer them to the appropriate Privacy Officer and/or Security Officer for handling. Additional contact information for the Emory Healthcare Privacy Officer is as follows: Phone: (404) 778-2186. FAX: (404) 778-2755. Email: anne.adams@emoryhealthcare.org

Complaints also may be made directly to the Emory University Privacy Officer or to the Security Officer and/or through the independently operated Emory Trust Line at 1-888-550-8850 or via the internet at www.mycompliancereport.com/EmoryTrustLineOnline. In the event that any other unit or person within the Emory University Hybrid Covered Entity receives a complaint regarding HIPAA compliance, it shall forward the complaint to the Office of Risk Management for appropriate routing.

When complaints are received they will be documented and investigated. Documentation of the resolution of the complaints shall be made including findings, any corrective actions taken, and any sanctions imposed. Such documentation shall be retained for six years from receipt of the complaint.

REFERENCES: 45 CFR §§ 164.530(a)(1)(ii), (2), (d)(1) – (2) & (j).

Training

The Emory University Hybrid Covered Entity will provide the members of its workforce with training on these revised Policies promply after their adoption. Thereafter each new member of the workforce shall be trained within in a reasonable period of time after joining the workforce. Additionally, any member of the workforce whose duties are affected by any material change in these Policies will receive training regarding such change within a reasonable period of time after the change becomes effective. The Emory University Hybrid Covered Entity will keep appropriate documentation regarding such training.

Designated Privacy and Security Officers in connection with appropriate administrative officials for the Emory University Hybrid Covered Entity will organize/provide required training regarding these Policies and HIPAA regulations. The Emory University Hybrid Covered Entity

may accept HIPAA training provided by the Emory Healthcare Affiliated Covered Entity as equivalent to training provided by the Emory University Hybrid Covered Entity.

REFERENCE: 45 CFR §164.530(b).

Safeguards

The Emory University Hybrid Covered Entity will put in place appropriate administrative, technical and physical safeguards to protect the privacy of PHI. The safeguards will be designed to reasonably protect PHI from any intentional or unintentional Use or disclosure that violates HIPAA. The Emory University Hybrid Covered Entity also will put in place safeguards to limit incidental Uses or Disclosures that are made pursuant to permitted or required Uses or Disclosures. In this regard, units that are a part of the Emory University Hybrid Covered Entity will utilize these Policies to evaluate their specific operations and settings and to determine the nature of the safeguards to be put in place.

Sanctions

The Emory University Hybrid Covered Entity shall apply appropriate sanctions, up to and including termination, to members of the workforce who violate HIPAA requirements and/or these Policies. These sanctions shall be imposed by Emory Human Resources and/or other appropriate units of Emory University. Units shall document any sanctions that are imposed upon workforce members, and shall provide such documentation to designated Privacy or Security Officers upon request.

REFERENCE: 45 CFR §164.530(e)

Mitigation of any Harm Caused by a HIPAA Violation

In the event that there is a Use or Disclosure of PHI by a Covered Component of the Emory University Hybrid Covered Entity, or one of its Business Associates, in violation of HIPAA or these Policies, then the Emory University Hybrid Covered Entity shall take such steps as are necessary to mitigate, to the extent practicable, any harmful effect known to it of such Use or Disclosure. Action in mitigation of any such harm shall be taken by the unit within the Covered Component of the Emory University Hybrid Covered Entity that had responsibility for the PHI that was compromised, and costs for such mitigation shall be borne by that unit.

REFERENCE: 45 CFR §164.530(f)

No Intimidation or Retaliatory Acts

No component of the Emory University Hybrid Covered Entity, or any member of the workforce thereof, will take any action to intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

(a) Any Individual who exercised his/her rights or participated in any process required under HIPAA.

(b) Any Individual who in good faith filed a complaint with the Emory University Hybrid Covered Entity, the Emory Healthcare Affiliated Covered Entity, or

the the U.S. Secretary of Health and Human Services regarding the Emory University Hybrid Covered Entity's or the Emory Healthcare Affiliated Covered Entity's compliance with HIPAA.

(c) Any Individual who assisted or participated in an investigation, compliance review, hearing or other proceeding concerning HIPAA compliance by the Emory University Hybrid Covered Entity or Emory Healthcare Affilated Covered Entity.

(d) Any Individual who refuses to take or opposes any act that the individual in reasonably and in good faith believes is in violation of HIPAA, provided that the manner of opposition is reasonable and does not involve disclosure of PHI.

Sanctions may be imposed against any member of the workforce of the Emory University Hybrid Covered Entity who violates this prohibition against such intimidating or retaliatory acts.

REFERENCE: 45 CFR §164.530(g).

No Waiver of Rights

The Emory University Hybrid Covered Entity will not require any Individual to waive his/her rights under HIPAA as a condition of Treatment, Payment, enrollment in a Health Plan or determining eligibility for benefits.

REFERENCE: 45 CFR §164.530(h)

REFERENCES: Listed within policy.
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

A.4. IMPLEMENTATION OF AND MODIFICATION TO HIPAA POLICIES; DOCUMENTATION; DOCUMENT RETENTION

PURPOSE OF POLICY

This policy sets forth the process by which the Emory University Hybrid Covered Entity will promulgate HIPAA policies and procedures and make changes thereto as necessary to ensure compliance with applicable laws and regulations. This policy also sets forth standards for documentation associated with these policies, including a document retention period for all documents required under HIPAA.

POLICY

Adoption of Policies

The Emory University Hybrid Covered Entity has adopted and will promulgate these Emory HIPAA Privacy Rule Policies in compliance with 45 CFR § 164.530(i).

Modifications to Emory HIPAA Privacy Rule Policies

The Emory University Hybrid Covered Entity shall make modifications to these Policies as necessary to comply with any changes in HIPAA laws and regulations. In the event that any policy, or portion of a policy, is not in accord with HIPAA laws and regulations or with any state law not pre-empted by HIPAA laws and regulations, then the provisions of the applicable laws and regulations shall control and pre-empt the policy (or portion thereof) that is out of compliance until appropriate changes are made to cause it to conform. Additionally, the Emory University Hybrid Covered Entity may make modifications to the Emory University HIPAA Privacy Rule Policies that are not required by law, such as, but not limited to, those required by any changes in Emory University entities, policies or processes.

In the event that any modification to the Emory University HIPAA Privacy Rule Policies has a material affect on the content of the Emory University Hybrid Covered Entity's Notice of Privacy Practices (NPP), or alternatively, if a change to the NPP necessitates a change in the policies, the Emory University Hybrid Covered Entity shall revise the NPP to reflect any such changes. The modified policies, and if applicable, the modified NPP shall contain an effective date for the revisions. Changes to policies and procedures that affect the NPP will not be implemented prior to the effective date of the revised NPP. The modified NPP shall be published and distributed as required by HIPAA.

Effect of Modifications on PHI Created or Received
The Emory University Hybrid Covered Entity has included a statement within its NPP that provides that modifications that it makes to the Policies shall apply to PHI that it created or received prior to the effective date of the modification to the NPP.

Documentation

These Policies and any modifications thereto, shall be maintained in hard-copy and/or electronic form by the designated Privacy Officer. Policies shall be available on websites accessible to the workforce of the Emory University Hybrid Covered Entity. Access to Policies shall be made available to Business Associates as necessary and appropriated.

Communication

Any communication required under HIPAA and/or these Policies will be in writing and will be maintained in hard-copy and/or electronic form. Any actions that are required under HIPAA and/or these policies shall be documented and likewise maintained.

Documentation Retention

All documents required by HIPAA and/or these Policies will be maintained for a period of six (6) years from the date of its creation or the date on which it was last in effect, whichever is later.

REFERENCE: 45 CFR § 164.530(i) & (j).
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

A.5. COOPERATION WITH GOVERNMENT OFFICIALS IN COMPLIANCE REVIEWS AND COMPLAINT INVESTIGATIONS

PURPOSE OF POLICY

This policy sets forth the ways in which the Emory University Hybrid Covered Entity will cooperate with the Secretary of the Department of Health and Human Services and its agents (the "Secretary") in the Secretary's conduct of any compliance reviews or investigations, including the provision of records and access to information.

POLICY

Compliance Reviews and Complaint Investigations

The Secretary of the Department of Health and Human Services may conduct compliance reviews and investigations into complaints received to determine if the Emory University Hybrid Covered Entity and/or its Business Associates are complying with HIPAA.

Provision of Records and Compliance Reports:
The Emory University Hybrid Covered Entity and/or its Business Associates will permit the Secretary to have access to its facilities, books, records, accounts and other sources of information, including PHI, that are pertinent to ascertaining whether the Emory University Hybrid Covered Entity and/or its Business Associates is/are in compliance with HIPAA. Access will usually be sought during regular business hours, but may be sought at any time, without notice, if the Secretary determines that emergency circumstances so warrant. If the Secretary's personnel come to a facility of the Emory University Hybrid Covered Entity, then facility personnel should immediately contact their designated Privacy Officer and Security Officer, as well as the Emory University Office of the General Counsel. The Emory facility personnel should verify that identification and authority of government officials prior to providing access to books and records. If the Secretary's personnel come to the facility of a Business Associate, the Business Associate shall immediately notify the designated Privacy Officer at the Emory University Hybrid Covered Entity.

Documents/Information in another Person or Entity's Possession:
If the documents/information that the Secretary requests is in the exclusive possession of person or entity other than the Emory University Hybrid Covered Entity or its Business Associate and that person or entity fails to provide the information to the Emory University Hybrid Covered Entity or Business Associate upon request, then the Emory University Hybrid Covered Entity or Business Associate will certify this refusal to the Secretary along with the efforts that were made to obtain the documents/information.

REFERENCES: 45 CFR §§ 160.308, .310.
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

A.6. CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION (PHI); PERMITTED AND REQUIRED USES AND DISCLOSURE

PURPOSE OF POLICY

The purpose of this policy is to provide general standards for ensuring that the Emory University Hybrid Covered Entity has the PHI that it needs to care for each patient (the "Individual") while protecting the confidentiality of that PHI, and to generally describe the Uses and Disclosures of PHI that the Emory University Hybrid Covered Entity is permitted and/ore required to make.

NOTE: Individuals who are patients of facilities and whose PHI-containing records at issue are owned by the the Emory Healthcare Affiliated Covered Entity are governed by Emory Healthcare HIPAA Privacy Rule Policies.

POLICY

General Standards Regarding Confidentiality of PHI

All members of the workforce of the Emory University Hybrid Covered Entity will preserve the confidentiality of PHI in accordance with all applicable laws, regulations and policies. To that end, the Emory Hybrid Covered Entity will:

- Adhere to the standards set forth in its Notice of Privacy Practices.

- Collect, Use and Disclose PHI only in conformance with applicable federal and Georgia laws and/or Individuals' current Authorizations, or Waivers of Authorization, as granted by a Privacy Board or Institutional Review Board.

- Recognize that although PHI belongs to the Covered Components of the Emory University Hybrid Covered Entity, an Individual has the right to inspect and obtain a copy of his/her PHI maintained in a Designated Record Set and has a right to request an amendment to his/her PHI maintained in a Designated Record Set if he/she believes that the PHI in inaccurate or incomplete.

- Maintain an accounting of certain disclosures of PHI as required by HIPAA.

- Adhere to any restrictions concerning the Use or Disclosure of PHI that an Individual has requested and that the Emory University Hybrid Covered Entity has approved.

- Make members of the workforce of the Emory University Hybrid Covered Entity aware that violations of these Policies are not permitted; take reasonable steps to ensure workforce members abide by these Policies; and make workforce members aware that violations of these Policies and/or HIPAA are grounds for disciplinary action, up to and including termination of employment, in accordance with applicable personnel policies, and that criminal, civil and professional sanctions also may be applied for violations.

Permitted and Required Uses and Disclosures

Permitted Uses and Disclosures: In accordance with HIPAA and these Policies, the Emory University Hybrid Covered Entity is permitted to make the following Uses and Disclosures of PHI, subject to any additional special requirements that may apply to specific types of PHI under applicable federal or state law (e.g., Disclosure of privileged communications between a patient and a psychiatrist):

- To the Individual who is the subject of the PHI.
- For Treatment, Payment and Health Care Operations (TPO), as follows:
  - For the Emory University Hybrid Covered Entity's own TPO.
  - For the Treatment activities of a Health Care Provider.
  - To another Covered Entity, including a Health Care Provider, for the Payment activities of the entity that receives the information.
  - To another Covered Entity for the Health Care Operations of the entity that receives the information if each of the entities has, or had, a relationship with the Individual who is the subject of the PHI; the PHI pertains to the relationship; and the disclosure is for quality assurance, quality control or peer review purposes or for the purpose of Health Care fraud and abuse detection or compliance.
  - To a Covered Entity that participates in an Organized Health Care Arrangement (OHCA) with the Emory University Hybrid Covered Entity for the Health Care Operations of the OHCA.
- That is incident to a Use or Disclosure otherwise permitted under HIPAA, provided that all applicable HIPAA requirements have been met.
- As appropriate under HIPAA, made pursuant to a valid Authorization; or after giving the Individual who is the subject of the PHI and opportunity to agree or object; or made pursuant to the agreement of the Individual
- Other Disclosures required or permitted under HIPAA regulations and other applicable state and federal law.

Required Disclosures: The Emory University Hybrid Covered Entity will make the following required Disclosures in accordance with HIPAA:

- To an Individual when he/she requests the Disclosure of his/her own PHI in accordance with the Individual's right to access his/her PHI maintained in a Designated Record Set or seek an accounting of the Disclosure of his/her PHI under HIPAA regulations, subject to HIPAA requirements limiting any such Disclosure or accounting.
- When required by the Secretary of Health and Human Services to investigate or determine the Emory University Hybrid Covered Entity's compliance with HIPAA.

All Uses and Disclosures will be undertaken in a manner that is consistent with the Emory University Hybrid Covered Entity's Notice of Privacy Practices.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include

communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCES: 45 CFR §164.502(a)
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

A.7 MINIMUM NECESSARY RULE

PURPOSE OF POLICY

The purpose of this Policy is to ensure that access to, requests for, or Use and Disclosure of an Individual's PHI is based on a minimum necessary standard.

POLICY

Minimum Necessary Standard

Except as noted below, when Using or Disclosing PHI or when requesting PHI from another Covered Entity or Business Associate, the Emory University Hybrid Covered Entity or its Business Associates will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the Use, Disclosure or request. This rule applies to PHI in any format (e.g., hard-copy, oral, electronic).

Exceptions to the Applicability of the Minimum Necessary Standard

The minimum necessary standard does not apply in the following situations:

- Use and Disclosure of PHI pursuant to an Individual's Authorization.
- Use and Disclosure of PHI to a Health Care Provider for Treatment.
- Disclosure of PHI to an Individual who is the subject of the PHI.
- Use and Disclosure of PHI that is required by law (e.g., subpoenas, court orders); provided; however, that the PHI that is Used or Disclosed shall be limited to the type and amount that is required to comply with the law or that is specified in the legal request per which the PHI is being Used or Disclosed.
- Use and Disclosure of PHI for compliance with and enforcement of HIPAA.
- Use and Disclosure of PHI for complying with HIPAA electronic transaction standards.

Relationship between the Minimum Necessary Standard and Workforce Roles

For use of PHI by members of the Emory University Hybrid Covered Entity workforce within Covered Components, the determination of the minimum amount of PHI necessary is based on the role of the workforce member requesting the PHI and the task for which the PHI is being requested. All such workforce members of a Covered Component of the Emory University Hybrid Covered Entity should only access PHI as necessary to perform their job duties, and the amount and type of PHI that they access should be limited to that which is necessary to perform the job duty at hand.

PROCEDURE

Use of PHI

Identification of Units Requiring Access to PHI: Access to PHI should not be granted to any unit that does not need access to perform its job functions. Units that are a part of a Covered Component of the Emory University Hybrid Covered Entity have been determined to require access to PHI to perform their job functions.

Identification of Positions Requiring Access to PHI: Each job category within a unit that is in a Covered Component of the Emory University Hybrid Covered Entity must be evaluated in order to determine whether access to PHI is required in order for person in the job category to perform their duties. Each such unit will develop a list of job categories within the unit that require access to PHI to perform necessary job duties (referred to in this Policy as the "List").

Identification of Types of PHI to Which Certain Job Categories Require Access: For each job category on the List, the unit shall include a description of the categories of PHI to which the persons in that job category must have access in order to perform their job functions.

Limits on Access: Each unit within a Covered Component of the Emory University Hybrid Covered Entity will put in place reasonable processes to limit workforce access only that PHI which is necessary to perform job functions.

Use of Entire Medical Record: A unit within a Covered Component of the Emory University Hybrid Covered Entity will not grant access to use an entire medical record unless access to the entire file is specifically justified for performance of job duties. Use of the PHI for Treatment purposes is not subject to this restriction.

Disclosure of PHI

Routine and Recurring Disclosures: For any Disclosure that a unit within a Covered Component of the Emory University Hybrid Covered Entity makes on a routine and recurring basis, the unit will include on the List a description of the routine/recurring Disclosure and the PHI that will be provided for each. If no such routine/recurring Disclosures occur, the unit will document this fact instead.

Non-Routine and Non-Recurring Disclosures: For any Disclosure that a unit with a Covered Component of the Emory University Hybrid Covered Entity makes on non-routine and non-recurring basis, the unit will develop criteria that are designed to limit the PHI provided to the minimum necessary to accomplish the purpose of the Disclosure and review the requested Disclosure against these criteria on an individual basis.

Reliance on Position or Status of Requestor as Establishing Minimum Necessary Standard: If reasonable under the circumstances, a Covered Component of the Emory University Hybrid Covered Entity may rely on a request from one of the types of persons below as establishing the minimum necessary PHI that must be Disclosed (i.e., the PHI described in the request shall be considered to meet the minimum necessary rule):

- Public officials who are requesting PHI in accordance with the requirements of 45 CFR § 164.512 for the performance of public health functions, health oversight functions, law enforcement functions and specialized government functions, if the public official represents that the information is the minimum necessary to perform the function.
- Another Covered Entity.
- A professional who is a member of the workforce of the Emory University Hybrid Covered Entity or its' Business Associate, and who is requesting the information to provide professional services to the Emory University Hybrid Covered Entity, providing that the professional represents that the information requested is the minimum necessary for the purpose requested.
- A researcher who is requesting PHI for Research purposes and who provides an Authorization, Waiver of Authorization from an IRB or Privacy Board, Data Use Agreement, assurance regarding Use Preparatory to Research, or an assurance regarding the use of decedents' PHI.

In all such cases, a copy of the request shall be maintained in accordance with applicable record retention standards to document compliance with the foregoing standard.

Disclosure of Entire Medical Record: A Covered Component of the Emory University Hybrid Covered Entity will not Disclose an Individual's entire medical record unless such Disclosure is justified as being reasonably necessary to accomplish the purpose for which it is requested.

Emory University Hybrid Covered Entity's Requests for PHI Made to Other Covered Entities

Request to Another Covered Entity: Each Covered Component of the Emory University Hybrid Covered Entity will limit its requests to another Covered Entity for PHI to the amount of PHI that is reasonably necessary to accomplish the purpose for which the request is made.

Routine/Recurring Requests: For routine or recurring requests for PHI that a Covered Component of the Emory University Hybrid Covered Entity makes to another Covered Entity, the Covered Component will establish processes designed to limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

Non-Routine/Recurring Requests: For requests for PHI from a Covered Entity that are not made on a routine/recurring basis, the Covered Component of the Emory University Hybrid Covered Entity will implement processes designed to insure that the PHI requested is the minimum reasonably necessary to accomplish the purpose of the request and review each request against the criteria on an individual basis.

Request for Entire Medical Record: A Covered Component of the Emory University Hybrid Covered Entity will not request an Individual's entire medical record except when the entire record is justified as being reasonably necessary to accomplish the purpose for which the PHI is requested.

REFERENCES: 45 CFR §§ 164.502(b), .514(d).
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

A.8 BUSINESS ASSOCIATE POLICY

PURPOSE OF POLICY

The purpose of this Policy is to ensure (a) that all Covered Components of the Emory University Hybrid Covered Entity identify Business Associates; (b) that appropriate contractual requirements are in place (i.e., a Business Associate Agreement) with Business Associates governing Business Associates' use and disclosure of PHI; and (c) that appropriate a actions are taken with regard to Business Associates that the Emory University Hybrid Covered Entity determines to be in beach of such contractual requirements.

POLICY

Each Covered Component within the Emory University Hybrid Covered Entity is responsible for identifying those persons, companies, or other entities that work for it (or any units within the Covered Component) as a Business Associate and ensuring through appropriate contractual arrangements that the Business Associate provides satisfactory assurances that it will employ adequate safeguards for any PHI shared with the Business Associate. The Covered Component must obtain from each Business Associate a contractual agreement (i.e., a Business Associate Agreement" or "BAA") per which the Business Associate agrees to be bound by all applicable requirements of HIPAA and to handle PHI in accordance with all such requirements. The BAA shall meet the requirements set forth at 45 CFR Section 164.504(e)(2). A template BAA agreement in the format prescribed by Emory University Office of General Counsel shall be utilized, and modifications to such agreement or the use of another template must be specifically approved in advance by the Office of the General Counsel. The template BAA is located at the following website: https://www.ogc.emory.edu/downloads/BusinessAssociateAgreement09-2104.pdf

An Emory Covered Component may disclose PHI to a Business Associate for Treatment, Payment and Health Care Operations without an Authorization from the Individual after a BAA is in place. Business Associates also may perform Data Aggregation services for the Emory University Hybrid Covered Entity or an Organized Health Care Arrangement in which the Emory University Hybrid Covered participates. If the Emory University Hybrid Covered Entity is required to have an Authorization from an Individual in order to obtain or disclose PHI for a particular purpose, then an Authorization also is required in order to disclose that PHI to a Business Associate. Disclosures of PHI to Business Associates only may be made for the purpose of assisting the Emory Covered Component to carry out its Covered Functions, and not for the Business Associate's independent uses or purposes.

The Emory Hybrid Covered Entity is not required to monitor or oversee the means by which a Business Associate carries out privacy safeguards or privacy requirements of the BAA. If, however, the Emory University Hybrid Covered Entity, acting through one of its Covered Components, becomes aware of a pattern of activity or practice on the part of a Business Associate (including its agents or subcontractors) that constitutes a violation or material breach of the BAA, then the Emory Universtiy Hybrid Covered Entity will take reasonable steps to ensure that the violation or breach is cured. If the Business Associate cannot or will not cure the violation/breach, then the Emory University Hybrid Covered Entity will terminate the BAA, if feasible. If not feasible, then the Emory University Hybrid Covered Entity will contact the Emory University Privacy Officer, who, in turn, will report the matter to the Secretary of the U.S. Dept. of Health and Human Services. The BAA shall require the Business Associate to impose the foregoing requirements upon its subcontractors, if any.

PROCEDURE

Types of Business Associates Arrangements Covered by this Policy There are two types of Business Associate arrangements: (a) Business Associate of Emory University Hybrid Covered Entity – an arrangement by which a Covered Component of the Emory University Hybrid Covered Entity identifies an outside person/entity to perform a service that would cause that person/entity to be considered a Business Associate under HIPAA; or (b) Emory University Unit Serving as a Business Associate – a outside person/entity identifies a unit of Emory University to perform services for the outside person/entity that would cause the Emory University unit to be considered a Business Associate under HIPAA. Procedures for each type of Business Associate arrangement are described below.

Process for Business Associates of Emory University

Identification of Business Associates – Each Covered Component of the Emory University Hybrid Covered Entity will examine all relationships that its units have with vendors, consultants, service providers, etc. to determine if any of those persons/entities meet the definition of the term Business Associate, as set forth in the Glossary. In general, a Business Associate relationship will exist when the Covered Component must disclose PHI to an outside person/entity in order for the person/entity to perform administrative, managerial or consultative-type tasks to help the Covered Component perform Covered Functions. Note, that the following types of relationships do not constitute Business Associate relationships:

(a) Treatment: A relationship in which one Health Care Provider discloses PHI to another Health Care Provider for purposes of treating a Individual.
(b) Person/Entity who is not Performing Services for the Covered Component: A relationship in which the Covered Component is disclosing PHI to a person or entity for that person/entity to use for its own purposes, and not to provide services for the Covered Component, e.g., Emory Covered Component providing PHI to the sponsor of a clinical trial pursuant to an Authorization or Waiver of Authorization.
(c) Incidental Disclosure: A relationship in which there is only incidental, occasional disclosure of PHI to a person/entity that is performing services for the Covered Component, but whose job duties on behalf of the Covered Component do not involve the creation, receipt, maintenance or transmission of PHI, e.g., a plumber who may occasionally overhear PHI while performing services in a health care facility.
(d) Organized Health Care Arrangements: A relationship in which a Covered Component participates in an OHCA and PHI is disclosed when performing Covered Functions for or on behalf of the OHCA.
(e) Conduits: A relationship in which a person or entity acts only as a conduit for the transmission of PHI and does not maintain the PHI on any more than a transient basis, e.g., U.S. Postal Service, courier service.
(f) Financial Institution Processing a Consumer Conducted Financial Transaction: A relationship in which a financial institution processes a consumer-conducted financial transaction by debit card, credit card, check, or other payment method as payment for health care.
(g) Research: Persons/entities who are collaborating in Research activities and/or providing services for Research projects unless the services provided include Treatment for which Payment is collected using HIPAA-Covered Billing.

Flow Chart – The flowchart in **Attachment A.8 - 1** to this policy can be used by Covered Components to assist in identifying Business Associates.

Creation of Business Associates List -- Once Business Associates are identified, the Privacy Contact Person for each Covered Component should make a list containing for each Business Associate: name/contact information; description of services being performed; beginning and termination dates of contact(s) in place with Business Associate; and description of PHI being disclosed to Business Associate. Each Covered Component is required to keep its list of Business Associates current, and it shall provide a copy of this list to the Emory University Privacy Officer on request.

Contract – The Covered Component must enter into a BAA with the Business Associate prior to providing any PHI to the Business Associate. Copies of each executed BAA must be maintained by the Privacy Contact Person for each Covered Component. The form of the BAA shall be established by the Emory University Office of the General Counsel. The current form of the BAA is located at: https://www.ogc.emory.edu/downloads/BusinessAssociateAgreement09-2104.pdf. The Office of General Counsel's approval must be obtained prior to accepting any changes to the Emory BAA form or accepting an alternate BAA form. At a minimum the BAA must meet the criteria set forth at 45 CFR §164.504(e)(2), including:

- A description of the permitted and required uses of the PHI by the Business Associate.
- Prohibit the Business Associate from Using or Disclosing the PHI other than as permitted by the BAA or as required by law.
- Require the Business Associate to employ appropriate safeguards to protect the PHI, including reasonable administrative, technical and physical safeguards for electronic PHI.
- Require the Business Associate to immediately report to the Covered Component any Use or Disclosure of the PHI that is not permitted by contractual arrangements.
- Require the Business Associate to impose on any subcontractor the same requirements and restrictions that the Covered Component has imposed upon the Business Associate.
- Provide the Covered Component with any information necessary to permit the Covered Component to comply with patients' rights under HIPAA, including the right to access PHI; the right to receive an accounting of Disclosures of PHI; and the right to request an amendment of PHI.
- Require the Business Associate to make available to the Secretary of the U.S. Department of Health and Human Services any books, records or internal practices relating to the Use or Disclosure of PHI.
- If feasible, require the Business Associate to return or destroy PHI once the contract is ended, of if not feasible, to ensure that contractual requirements prevent further Use of the PHI apart from purposes that make return/destruction not feasible.

Approval and Signing of BAA – As with any contract that binds a unit of Emory University, any BAA or associated contractual arrangement must be approved and signed in accordance with Emory University Policy 1.2, *Contract Approval and Signature Authority* at http://policies.emory.edu/1.2.

Termination of BAA -- At the conclusion of the BAA, the Business Associate shall, if feasible, return to the Covered Component, or destroy, all PHI received from, or created or received by the Business Associate on behalf of, the Covered Component that the Business Associate maintains. If the PHI is destroyed, the Covered Component shall obtain a certificate of destruction from the Business Associate that describes the PHI destroyed and lists the date and method of destruction. The Privacy Contact Person for the Covered Component shall retain a copy of any certificate of destruction for the requisite retention period. If return of the PHI is not feasible, then the BAA protections must extend to the retained information and limit further uses and disclosures to those purposes that make return/destruction non-feasible.

Termination of BAA for Material Breach – If a Business Associate breaches a contract with the Covered Component, the Covered Component should follow the terms set forth in the contract documents governing breach and cure; provided, however, that per those documents, the Covered Component must be able to terminate the contract if the Business Associate violates a material term.

Business Associate Contracts with Subcontractors – If a Business Associate retains subcontractors to assist it in the performance of its duties for the Covered Component, the Business Associate must have a BAA with the subcontractor, and all requirements imposed upon the Business Associate by the Covered Component, must be imposed by the Business Associate upon any subcontractor.

Impermissible Use or Disclosure of PHI by Business Associate – If a Business Associate Uses or Discloses PHI outside of the requirements of the BAA or any underlying contract, the Business Associate must notify the Covered Component immediately. In turn, the Covered Component, must notify the Emory University Privacy Officer who, in conjunction with the Office of the General Counsel, will take necessary steps to ensure that the matter is handled appropriately under HIPAA and under applicable contractual terms.

Applicability of Minimum Necessary Rule – The Covered Component must only disclose to the Business Associate the Minimum Necessary type and amount of PHI that is required to permit the Business Associate to perform the requested services on behalf of the Covered Component.

Applicability of Accounting Rule – Except for Disclosures made pursuant to an Authorization, a Business Associate, and its subcontractors (if any), must document any Disclosure of PHI made for purposes other than Treatment, Payment or Health Care Operations. This documentation must be available to the Covered Component and must be maintained for six years after the Disclosure

Process for Emory Serving as a Business Associate

Applicability of HIPAA Requirements – The requirements outlined above that apply to any person or entity that serves as a Business Associate of the Emory University Hybrid Covered Entity also apply to any Emory unit that chooses to serve as the Business Associate of an outside party.

Review of BAA – Any Emory unit that desires to serve as a Business Associate for an outside person or entity must have the associated BAA and other contractual arrangements reviewed by the Office of General Counsel and approved and executed in accordance with Emory University Policy 1.2.

List of BAAs – Each Emory unit entering into Business Associate arrangements with outside parties shall maintain a list of any BAA into which the unit enters. For each such BAA arrangement the list shall state: name/contact information for Covered Entity on whose behalf the Emory unit is serving as a BAA; description of services being performed; beginning and termination dates of contact(s) in place with Covered Entity; and a description of PHI being disclosed to Emory Business Associate. A copy of this list shall be provided to the University Privacy Officer on request.

REFERENCES: 45 CFR Sections §§160.103, 164.501; 164.502(e)(2); 164.504(e)(1); 164.524; 164.526; & 164.528.
See also,
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html;
http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/index.html

DATE OF POLICY: April 14, 2003

REVISED: September 1, 2016

Attachment A.8 – 1: Flowchart for Determining if Person/Entity is a Business Associate

Is the person performing services for or on behalf of a Covered Component of the Emory University Hybrid Covered Entity (hereafter the "Covered Component")? **No → Not a Business Associate**

↓ Yes

Do the services being provided by the person involve and require the receipt, creation, maintenance or transmission of PHI? **No → Not a Business Associate**

↓ Yes

Is the person a member of the workforce of the Covered Component? **Yes → Not a Business Associate**

↓ No

Is the person receiving/creating/maintaining the PHI as part of an Covered Component of the Emory University Hybrid Covered Entity in order to provide a service for or on behalf of an Organized Health Care Arrangement in which the Covered Component participates? **Yes → Not a Business Associate**

↓ No

Is the person receiving/creating/maintaining the PHI a Health Care Provider who is using the PHI for treatment? **Yes → Not a Business Associate**

↓ No

Is the person receiving the PHI a financial institution that is processing a financial transaction initiated by a consumer? **Yes → Not a Business Associate**

↓ No

Is the person couriering or transmitting the PHI and not maintaining the PHI in any more than in a transient way? **Yes → Not a Business Associate**

↓ No

Does the person perform a function or activity for the Emory Covered Component that utilizes PHI and is for Healthcare Operations or Payment for Healthcare including the following types of services:

▪Claims processing or administration ▪Billing ▪Benefit Management
▪Data analysis, processing or administration ▪Practice management or re-pricing services
▪Utilization review, quality assurance or patient safety activities
▪Legal, actuarial, accounting, or consulting services
▪Data aggregation, management, administrative or accreditation services
▪Health information, e-prescribing gateway or other data transmission service that requires access to the PHI on a routine basis or maintains the PHI for more than a transient period of time.
▪Service per which a personal health records is offered to one or more individuals on behalf of the Covered Component. **No → Not a Business Associate**

↓Yes

Entity is a Business Associate and BAA is required.

A.9 DISCLOSURES BY WHISTLEBLOWERS AND WORKFORCE MEMBER CRIME VICTIMS

PURPOSE OF POLICY

The purpose of this policy is to describe the PHI that may be disclosed by workforce members of a Covered Component of the Emory University Hybrid Covered Entity or one of its Business Associates who are (a) whistleblowers; or (b) victims of a crime.

POLICY

Disclosures Made by Whistleblowers

If member of the workforce of a Covered Component of the Emory University Hybrid Covered Entity (or one of its Business Associates) who has a good faith belief that the Covered Component or Business Associate has engaged in conduct that is unlawful; violates professional or clinical standards; or has created or maintained conditions, care or services that endanger patients, workers or members of the public (hereafter "Possible Reportable Conduct") may disclose PHI to:

(a) A Health Oversight Agency or Public Health Authority that is authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Covered Component or its Business Associate;

(b) An appropriate health care accreditation organization to report an allegation that the Covered Component or its Business Associate has committed misconduct or failed to meet professional standards;

(c) An attorney retained by or on behalf of a workforce member of a Covered Component or its Business Associate for purposes of determining the member's legal options with respect to the Possible Reportable Conduct.

Disclosures by Workforce Members who are Victims of a Crime

A workforce member of a Covered Component of the Emory University Hybrid Covered Entity who is a crime victime may disclose PHI to a law enforcement official if:

(a) The PHI being disclosed is about the person/entity suspected of perpetrating the criminal act; and

(b) The PHI being disclosed is limited to the following information regarding the perpetrator:

i. Name and address.
ii. Date and place of birth.
iii. Social Security Number.
iv. ABO blood type and rh factor.
v. Type of injury.
vi. Date and time of treatment.
vii. Date and time of death, if applicable.

viii. Description of distinguishing physical characteristics, including height, weight, gender, race, hair and color, presence or absence of facial hair (beard or moustache), scars and tattoos.

REFERENCES: 45 CFR §§164.502(j), 164.512(f)(2)(i)
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

A.10 SALE OF PHI

PURPOSE OF POLICY

The purpose of this Policy is to establish that a Covered Component of the Emory University Hybrid Covered Entity or its Business Associate may not sell an Individual's PHI without first obtaining Authorization for the Sale of PHI (as defined below) from the Individual.

DEFINITIONS

The definitions of the following terms are presented here for convenience. These terms also appear in the Glossary.

"Sale of PHI": A "Sale of PHI" takes place when a Covered Component of the Emory University Hybrid Covered Entity or its Business Associate directly or indirectly receives remuneration from, or on behalf of, the recipient of the PHI in exchange for the PHI. The following Disclosures by a Covered Component, however, are not considered to be a Sale of PHI:

(a) Disclosure for public health purposes under *Policy D.6, HIPAA Policy Regarding Use and Disclosure of PHI for Public Health Activities and Workplace Surveillance Related Activities and Student Immunizations* or as part of a Limited Data Set for public health purposes under *Policy C.5, Limited Data Sets.*

(b) Disclosure for Research purposes under *Policy D.14, HIPAA Policy Regarding the Use and Disclosure of PHI for Research Purposes and the Role of the Institutional Review Board* or as part of a Limited Data Set for Research purposes under *Policy C.5, Limited Data Sets* when the only remuneration received by the Covered Component or Business Associate is a reasonable cost-based fee that covers the cost of preparing and transmitting the PHI for Research purposes.

(c) Disclosure for Treatment or Payment for Health Care.

(d) Disclosure for sale, transfer, merger, or consolidation of all or part of a Covered Component(s) and for related due diligence undertaken as a part of Health Care Operations.

(e) Disclosure to or by a Business Associate for activities that the Business Associate undertakes for a Covered Component and the only remuneration provided is by the Covered Component to the Business Associate for the performance of such activities. The foregoing also applies to disclosure by a Business Associate to a subcontractor, and remuneration paid by the Business Associate to the subcontractor.

(f) Disclosure to an Individual who exercises his/her right to access his/her PHI or to request an accounting of his/her PHI.
(g) Disclosures as required by law as described in various Policies.
(h) Disclosure permitted by HIPAA when the only remuneration received by the Covered Component (or Business Associate) is a reasonable amount based on the cost of preparing and transmitting the PHI for such purpose or a fee otherwise expressly permitted by applicable law.

POLICY

Prohibition Against Sale of PHI without Authorization

A Covered Component of the Emory University Hybrid Covered Entity or its Business Associate is not permitted to make a Sale of PHI, as described in the preceding section, unless the Covered Component has an Authorization from the Individual (or his/her Legally Authorized Representative) whose PHI is being sold and the Authorization states the that disclosure of the PHI will result in remuneration to the Covered Component.

PROCEDURE

Prior to taking any type of Financial Remuneration in exchange for the Use or Disclosure of any PHI, the Covered Component must determined if the transaction falls into any of the categories of permitted disclosures described above under "Definition of the Term 'Sale of PHI.'" If not, then the Covered Component must obtain Authorization from the Individual whose PHI is the subject of the sale, and the Authorization must state that the Covered Component will receive compensation for disclosing the PHI.

The Covered Component should contact the Emory University Privacy Officer or the Office of the General Counsel for guidance if it is unsure whether or not a transaction meets the definition of "Sale of PHI."

REFERENCES: 45 CFR §§164.502(a)(5)(ii); 164.502(e); 164.504(e); 164.506(a); 164.508(a)(4); 164.512(b); 164.514(e); 164.512(a) & (i); 164.524; & 164.528.
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

SECTION B: HIPAA POLICIES REGARDING INDIVIDUAL RIGHTS UNDER HIPAA

B.1 NOTICE OF PRIVACY PRACTICES (NPP)

PURPOSE OF POLICY

The purpose of this Policy is to detail how the Emory University Hybrid Covered Entity will maintain and distribute a Notice of Privacy Practices.

POLICY

The Emory University Hybrid Covered Entity has prepared and maintains a Notice of Privacy Practices (NPP) located at the following website: https://www.ogc.emory.edu/downloads/BusinessAssociateAgreement09-2104.pdf. The most current version of the NPP will be maintained on this website. The NPP contains all required elements detailed in 45 CFR §164.520(b). The NPP is drafted by the Emory University Office of the General Counsel. Individual Covered Components are not permitted to make any changes to the NPP.

Revisions to the NPP

The Emory University Hybrid Covered Entity through the Emory Office of the General Counsel will revise the NPP whenever there is a material change in one of the items described below:

- Uses or Disclosures of PHI
- Individual's rights
- Emory University Hybrid Covered Entity's legal duties
- Other privacy practices described in the notice.

Unless required by law, a material change to the NPP may not be implemented prior to the effective date of the NPP in which the material changes is reflected.

Distribution & Posting of NPP

(a) Health Care Providers – (i)Time of Distribution: Health Care Providers within a Covered Component of the Emory University Hybrid Covered Entity that have a direct Treatment relationship with an Individual must provide the Individual with a copy of the NPP no later than at the time that services are first delivered (including service delivered electronically). If Treatment is provided in an emergency situation, then the NPP must be provided as soon as reasonably practicable after the emergency. (ii) Posting at Site: If the Health Care Provider has a physical site at which services are provided, that NPP must be available at the site to provide to persons upon request and the NPP also must be posted in a clear and prominent location where it is reasonable to expect that persons will be able to read the NPP. (iii) Distribution Electronically: If the first services that are provided are delivered electronically, then the Health Care Provider must electronically provide a copy of the NPP automatically at the time that the Individual's request for services is received. In all other cases, the NPP may be provided by email if the Individual agrees to receive the NPP in this matter and that agreement is documented. Otherwise, the NPP must be delivered in hard copy. If the Covered Component is aware that transmission by email has failed, it will provide the Individual with a hard copy of the NPP. The Individual retains the right to receive a hard-copy of the NPP on request.
(b) **Other Units**: A member of a Covered Component of the Emory University Hybrid Covered Entity that is not a Health Care Provider must provide the NPP to an Individual upon his/her request. The requirements regarding provision of the NPP by email described above apply to non-Health Care Providers as well, and the Individual retains the right to receive a hard-copy of the NPP on request.

(c) **Posting of NPP on Website**– Each Covered Component that maintains a website that provides information about the Covered Component's customer services will prominently post its NPP on the web site and make the NPP available for downloading.

Acknowledgement of Receipt of NPP

Except in an emergency situation, a Covered Component of the Emory University Hybrid Covered Entity must make a good faith effort to obtain a written acknowledgement from the individual of the receipt of the NPP. A form that may be used for this acknowledgement is attached to this policy as **Attachment B.1 - 1**. When an individual receives a hard copy of the NPP, the Covered Component will request the individual to sign the acknowledgement and the original signature page should be maintained in the individual's record. If a signed acknowledgement is not obtained, then the Covered Component must document in the individual's records that it made a good faith effort to obtain the acknowledgement and the reasons that the acknowledgement was not obtained. For copies of the NPP sent by email or other electronic means, the Covered Component will request a return receipt or other acknowledgment from the individual that he/she has received the transmission.

NPP for Organized Health Care Arrangement (OHCA)

The Emory University Hybrid Covered Entity may utilize a joint NPP that meets the requirements of 45 CFR §164.520(d) with respect to any OHCA in which it is a member. Provision of the joint NPP to an Individual by one member of the OHCA will satisfy the requirement that the NPP be provided with respect to all participants in the OHCA who are covered by the joint NPP.

Record Keeping

Each Emory Covered Component will maintain a copy of its NPP; any revisions to the NPP; and all written acknowledgements from individuals regarding receipt of the NPP or of a good faith effort to provide the NPP. The written acknowledgement of receipt/attempt to provide NPP must be maintained in the individual's medical record, if any.

REFERENCES: 45 CFR §164.520; www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

B.2. RIGHT TO REQUEST RESTRICTIONS ON USE OR DISCLOSURE OF PHI

PURPOSE OF POLICY

The purpose of this policy is to set forth the circumstances under which and the process for an Individual to request restrictions on the use/disclosure of his/her PHI by a Covered Component of the Emory University Hybrid Covered Entity.

NOTE: An individual's rights under HIPAA relating to PHI created/maintained by a unit of the Emory Healthcare Affiliated Covered Entity will be governed by the Emory Healthcare HIPAA Privacy Rule Policies.

POLICY

Circumstances Under which an Individual may Request Restrictions

An Individual may request restrictions regarding the use or disclosure of PHI in the following circumstances:

(a) Uses or disclosures of PHI to carry out Treatment, Payment or Health Care Operations.

(b) Uses and Disclosure of PHI to an Individual's family member, other relative, close personal friend, or any other person identified by the Individual, when:

i. The PHI is relevant to the person's involvement with the Individual's Health Care or Payment for the Individual's Health Care.

ii. The Individual is deceased and the PHI is relevant to the to the person's involvement with the Individual's Health Care or Payment for the Individual's Health Care prior to the Individual's death.

(c) Notification of a family member, personal representative, or other person responsible for care of an Individual about the Individual's location, general condition, or death, and Use and Disclosure of PHI with/to a public or private entity authorized by law/charter to assist in disaster relief efforts for the purpose of coordination regarding such notifications.

Agreement to Restrictions

A Covered Component of the Emory University Hybrid Covered Entity is not required to agree to provide requested restrictions, except as follows:

(a) Disclosures of PHI about the Individual to a Health Plan for purposes of carrying out Payment or Health Care Operations, provided that the Disclosure pertains solely to a Health Care item or service for which the Individual, or someone other than the Health Plan, has paid in full and the Disclosure is not otherwise required by law. Additionally, once an Individual has requested such a restriction, the Covered Component will not be able to terminate it.

Scope of Restrictions: Even if the Covered Component agrees to restrictions, the restrictions are not effective to prevent: (a) Uses and Disclosures to the Secretary of Health and Human Services to investigate or determine the Covered Component's compliance with HIPAA requirements; (b) Uses and Disclosures for facility directories (see *Policy D.5, HIPAA Policy Regarding Use and Disclosure of PHI for Facility Directories*); or (c) Uses and Disclosures for which an Individual is not required to provide an Authorization or to be given an opportunity to agree or object under 45 CFR §164.512.

Emergency Circumstances in which Disclosure of Restricted PHI may be Permissible

If a Covered Component agrees to the restrictions that an Individual has requested on the Disclosure of his/her PHI, then the Covered Component must follow the restrictions, except in the following circumstances:

> If the Individual who requested the restrictions requires emergency Treatment, then the Covered Component may provide the restricted PHI to a Health Care Provider if the PHI is required to provide the Treatment; provided, however, that the Covered Component must ask the Health Care Provider not to make any other Use or Disclosure of the restricted PHI.

Termination of Restrictions

A Covered Component can terminate restrictions when: (a) the Individual agrees to or requests the termination in writing; (b) the Individual agrees to the termination orally, and the oral agreement is documented; or (c) the Covered Component notifies the Individual that it is terminating its agreement to the restriction, provided that the termination will only apply to PHI created or received after the Individual was notified.

PROCEDURE

(a) As stated in the Notice of Privacy Practices, requests for restrictions must be made in writing to the Emory Healthcare Privacy Office, 101 West Ponce de Leon Ave., 2nd Floor, Suite 242, Decatur, GA 30030. The Emory University Hybrid Covered Entity has designated the Emory Healthcare Privacy Office to receive and triage all requests received under the NPP and to refer to the Emory University Privacy Officer those requests that involve the Emory University Hybrid Covered Entity. The written request must include a description of the information that the Individual wants restricted; whether the Individual wants to restrict Use, Disclosure, or both; and to whom the restrictions should be applied.

(b) For requests for restrictions that are referred to the Emory University Privacy Officer, upon receipt, he/she will notify the Privacy Contact Person for each affected Covered Component. With the exception of restrictions on Disclosures to a Health Care Plan, as described above, the Covered Component will determine whether or not to agree to the restrictions and notify the Emory University Privacy Officer of its decision. The Emory University Privacy Officer, in turn, will notify the Individual who requested the restrictions of it's decision either directly or through the Emory Healthcare Privacy Officer.

(c) If a Covered Component wants to terminate the restrictions to which it has agreed, it will notify the University Privacy Officer. The University Privacy Officer will then notify the Individual of the termination either directly or through the Emory Healthcare Privacy Officer.

(d) If the Emory Healthcare Privacy Officer or the Emory University Privacy Officer or a Covered Component receives a communication from an Individual asking that agreed-upon restrictions be terminated, the notification will be shared and the Covered Component will take steps to end the restrictions.

(e) Each Covered Component shall maintain documentation of the following: (a) each request for restrictions received; (b) the decision made by the Covered Component as to whether or not to agree to the requested restriction; (c) any decision of the Covered Component to terminate a restriction; (d) any request of an Individual to terminate requested restrictions and action taken to implement the termination; and (e) any communications with an Individual who requested restrictions. Such records shall be maintained for 6 years from the date of creation, or the date on which the record was last in effect, whichever is later.

REFERENCES: 45 CFR §§ 164.522(a); 164.502(a)(2)(ii); 164.510(a); 164.512; 164.530(j)
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

B.3. CONFIDENTIAL COMMUNICATIONS

PURPOSE OF POLICY

The purpose of this Policy is to describe the process by which an individual can request a Health Care Provider within a Covered Component of the Emory Hybrid Covered Entity to confidentially communicate with them through specified channels or at specified locations.

NOTE: An individual's rights under HIPAA relating to PHI created/maintained by a unit of the Emory Healthcare Affiliated Covered Entity will be governed by the *Emory Healthcare HIPAA Privacy Rule Policies*

POLICY

Communication of PHI

Individuals may request Health Care Providers within a Covered Component of the Emory University Hybrid Covered Entity to communicate PHI to them through alternate means or at alternate locations than those the Covered Component would typically use. For example, an Individual could request the Health Care Provider to contact the Individual at his/her office telephone number with medical test results, as opposed to contacting the Individual at his/her home telephone number. The Covered Component will accommodate all such reasonable requests and will not require the Individual to explain why he/she is made the request.

PROCEDURE

(a) As described in the NPP, to request a specific means for confidential communications of PHI, an Individual must send a written request to the Emory Healthcare Privacy Office, 101 West Ponce de Leon Ave., 2nd Floor, Suite 242, Decatur, GA 30030. The Emory University Hybrid Covered Entity has designated the Emory Healthcare Privacy Office to receive and triage all requests received under the NPP and to refer to the Emory University Privacy Officer those requests that involve the Emory University Hybrid Covered Entity. The request should describe the means by which the Individual wants to

receive communications (e.g., telephone, mail) and the location at which the Individual wants to receive communications (e.g., home, office).

(b) Upon referral of a request for confidential communications, the Emory University Privacy Officer will contact the Covered Component at which the Individual receives services to determine if/how the Covered Component can accommodate the request as well as any conditions that may apply to the provision of a reasonable accommodation including:
    i. Payment for any additional costs incurred to provide the accommodation.
    ii. Specification of a different alternate means of communication or location at to which communications will be directed.

(c) The Covered Component will maintain documentation of the request for confidential communications and how that request was accommodated.

REFERENCES: 45 CFR § 164.522(b).
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

B.4. INDIVIDUAL RIGHT TO ACCESS PHI

PURPOSE OF POLICY

The purpose of this policy is to describe the rights that an Individual has to access his/her PHI under HIPAA that is contained in a Designated Record Set held by a Covered Component of the Emory Hybrid Covered Entity and the process by which those rights may be exercised.

NOTES: (1) An Individual's rights under HIPAA relating to PHI created/maintained by a unit of the Emory Healthcare Affiliated Covered Entity will be governed by the *Emory Healthcare HIPAA Privacy Rule Policies.* (2) An Individual may have additional rights to access his/her PHI under the laws of the State of Georgia. Emory University's Office of the General Counsel should be consulted regarding applicability and provisions of State law.

POLICY

Right of Access

Subject to the exceptions described below, an Individual has a right to inspect and obtain a copy of any PHI about the Individual maintained by a Covered Component of the Emory Hybrid Covered Entity in a Designated Record Set for as long as the PHI is so maintained.

> **Exceptions**: Subject to any applicable laws of the State of Georgia, an individual's right of access under HIPAA does not apply to (a) Psychotherapy Notes; or (b) Information that is compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Designated Record Set: An Individual's right of access under HIPAA is limited to PHI maintained as part of a Designated Record Set. A Designated Record Set is a record or group of

records that contains PHI and that is maintained, collected, used or disseminated by or for the Covered Component or Covered Entity that is:

(a) The medical records and billing records about Individuals maintained by or for a Health Care Provider; or

(b) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a Health Plan; or

(c) Records used in whole or in part by or for the Covered Component/Covered Entity to make decisions about Individuals.

Denial of Request for Access

In the following circumstances, a Covered Component of the Emory Hybrid Covered Entity may deny an Individual access to his/her PHI:

(a) **Unreviewable Grounds for Denial of Access** – If the Emory Covered Component denies an Individual's request to access his/her PHI on any of the following grounds, then the Individual will have no opportunity for any review of that decision:

i. The PHI consists of Psychotherapy Notes.

ii. The PHI consists of information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

iii. The PHI to which access is requested was created or obtained by a Health Care Provider as a part of a Research project, and the Individual agreed that his/her right of access would be suspended during the course of the Research project when he/she consented to participate in the Research. At the conclusion of the Research, however, the Individual will have a right to access the information. [NOTE: Generally, only Research that involves Treatment and collection of Payment through HIPAA-Covered Billing will be considered to be subject to HIPAA and have the possibility of Research records containing PHI that are included in a Designated Record Set.]

iv. The PHI to which access is requested is subject to the requirements of the federal Privacy Act at 5 USC §552(a) and denial of access to the PHI is required under that law.

v. The PHI to which access is requested was obtained from someone other than a Health Care Provider under a promise of confidentiality and the access would be reasonably likely to reveal the source of the information.

(b) **Reviewable Grounds for Denial**: If the Covered Component of the Emory University Hybrid Covered Entity denies an Individual's request to access his/her PHI based on any of the following grounds, it must provide the Individual with a right to have the denial reviewed:

i. Access to PHI may be denied if a licensed Health Care Provider determines in the exercise of his/her professional judgment that:

1. The access requested is reasonably likely to endanger the life or physical safety of the Individual or another person; or

2. The PHI makes reference to another person (other than a Health Care Provider) and the access requested is reasonably likely to cause substantial harm to such other person; or
3. The request for access is made by the Individual's personal representative and provision of access to the personal representative is reasonably likely to cause substantial harm to the Individual or another person.

(c) **Georgia Law**: Georgia law at OCGA § 31-33-2 states that a Health Care Provider having custody of a patient's record must respond to a written request from the patient or a person authorized to have access to the record under an advance directive for health care or durable power of attorney for health care and shall provide a complete and current copy of the record within 30 days of receipt of the request. Mental health records are exempt from the requirements of OCGA § 31-33-2, but all other health records within the custody of a Health Care Provider are subject to this law. Accordingly, OCGA § 31-33-2 applies when a Health Care Provider wants to deny a request for non-mental health records for any of the reasons listed in sections (b)(i)(1)-(3) above. Under OCGA § 31-33-2 a Health Care Provider may only refuse to release a patient's non-mental health records if the provider reasonably determines that disclosure of the records to the patient will be detrimental to the physical or mental health of the patient; provided, however, that upon such a refusal, the record must be provided to any other Health Care Provider designated ty the patient. See the Procedure section below for handling request denials.

PROCEDURE

Process for Requesting Access to Inspect and Copy PHI Maintained in a Designated Record Set

Request: The Individual must submit his/her written request to inspect or copy his/her PHI to the medical records department of the facility in which he/she received Health Care. The medical records department, as necessary, will contact the Health Care Providers who treated the Individual and request them to review the request in order to determine if it should be accepted or denied, based on one of grounds listed above for denial. The request for access must be in writing, and the identity of the requestor should be verified using an identification check or signature comparison before access is granted. Additionally, in accordance with OCGA § 31-33-2, the Covered Component must ask the Personal Representative to provide a signed, written authorization indicating that he/she is authorized to have access to the patient's records in accordance with that code section, as well as a signed Authorization that meets HIPAA requirements. If the requestor directs the Covered Entity/Covered Component to transmit the copy of PHI directly to another person designated by the requestor, the Covered Entity/Component will provide the PHI to the designated person only after the Individual who is the subject of the PHI (or his/her legally authorized representative) provides a signed, written request that clearly identifies the person and location to which the PHI should be sent. If another unit in the Emory Covered Component receives a request for access, it should forward the request to the appropriate medical records department and coordinate with it regarding the response.

Deadlines for Processing of Requests and Providing Access:

(a) **Health Care Providers**: Georgia law provides a stricter timeline by which Health Care Providers must process records requests. Under OCGA §31-33-2, by no later than thirty (30) days after a Health Care Provider within a Covered Component has received a written request for access, it must provide the requested records or let the Individual know that it will deny the request and the grounds for denial.

(b) **Health Plans and Health Care Clearinghouses**: In the case of Health Plans and Health Care Clearinghouses, the HIPAA timelines for response reply. Under the HIPAA timeline, by no later than thirty (30) days after receipt of a written request for access, a Health Plan or Healthcare Clearinghouse must respond to the Individual and state whether it will accept or deny the request, and if it accepts the request, provide the access requested. However, if the information that the Individual requests is only accessible off-site, then the Health Plan or Healthcare Clearinghouse has sixty (60) days in which to send such a response. If the Health Plan or Healthcare Clearinghouse is not able to meet the appropriate deadline, then it may have a one-time extension of thirty (30) days to provide the Individual with its response, but it must give the Individual a letter describing the reasons for the delay and the date by which it will respond. Communications with Individuals in this regard will generally be handled by the appropriate medical records department.

Determining Whether Material is Exempt from the Right of Access: When a request is received, the medical records department, working with the appropriate Health Care Providers, must go through the material requested to determine what, if any, material is properly exempt from the Individual's right of access. There must be a specific regulatory basis within HIPAA (and/or state law) in order to exempt certain information from the right of access. After separating out the exempt information, the medical records department should coordinate with the Individual's Health Care Providers to determine what, if any, information the Health Care Providers wish to deny the Individual access as permitted by HIPAA and/or applicable state law. The Health Care Provider and the medical records department must then consult with the Office of the General Counsel and the University Privacy Officer regarding the applicability of a particular exemption supporting the denial of a request prior to responding to the requestor.

Acceptance of a Request: If a Covered Component of the Emory University Hybrid Covered Entity accepts an Individual's request for access, then it must provide the Individual with access to the information by permitting the Individual to inspect and/or copy the information about him/her that is maintained in a Designated Record Set. Access must be provided within the timeframe set forth above under "Deadlines for Processing of Requests and Providing Access." If the same information is kept in more than one Designated Record Set, then only one copy must be provided.

Method of Access: If the Emory Covered Component accepts the Individual's request for access, then the appropriate medical records department should discuss with the Individual the type of access (e.g., inspection, copy) and/or format in which the Individual would like to receive the information (e.g., hard copy, electronic). Based on this discussion, the medical records department should arrange a mutually convenient time for the Individual to inspect the records or

provide a copy of the PHI. Access will be provided in the form/format that the Individual has requested (including electronic form) if that form/format is readily producible. If the form/format is not readily producible, then the Covered Component will provide the PHI in readable electronic form/format if the information is maintained electronically and the individual requests an electronic copy. Otherwise, a readable hard copy format will be provided.

Summaries: The Emory Covered Component may provide the Individual with a summary of the information that he/she has requested if the Individual agrees in advance to accept a summary. The Individual also must agree in advance to any fees that may be charged for producing a summary. The Individual's agreement to the summary and any charges should be in writing.

Fees: If the Individual requests a copy or summary of the information, then the Covered Component may assess the individual a reasonable cost-based fee. This fee can only include costs for the following services: labor for copying the information in hard copy or electronically; supplies for creating paper copies or for electronic media if the individual requests that the electronic copy be provided on portable media; costs for preparing the summary; postage costs, if the individual requests that the information be mailed. Additionally, for records held in the custody of a Health Care Provider, all fees are subject to the restrictions set forth in OCGA §31-33-3.

Process for Denial of a Request for Access

The Covered Component may only deny a request for access on the grounds specified above under "Denial of Request for Access," and the denial may be issued only after consultation with and approval by the Office of the General Counsel and the University Privacy Officer. If a request for access is denied, then the Emory Covered Component must write to the Individual in plain language stating: (a) the basis for the denial; (b) the Individual's right to a review of the denial, if any; (c) the steps that the Individual must take in order to exercise his/her right to a review of the denial; and (d) a description of how the Individual can register a complaint with the Emory University Hybrid Covered Entity and/or the Secretary for the Department of Health and Human Services, including the name/title, and phone number of the unit designated by the Emory University Hybrid Covered Entity to receive complaints, as listed in the NPP; and (e) in the case of a denial by a Health Care Provider, the option under Georgia law to have non-mental health records provided to another Health Care Provider. The medical records department of the facility at which the Individual received Treatment will be responsible for handling the communication of the denial of access to the Individual.

Access to Other Information: If a request is denied in part, then the Emory Covered Component must provide the Individual access to the information to which access has not been denied.

Information Maintained Elsewhere: If the Emory Covered Component does not have the information that is requested, but it knows where this information is kept, then it must provide the Individual with this location information so that the Individual can know where to properly direct his/her request.

Review of a Denial: If an Individual has a request for access denied based on grounds that are reviewable as described under "Denial of a Request for Access," then the Individual may request that the denial be reviewed. The Emory Covered Component requires that the Individual submit his/her request for review in writing and direct it to the medical records department of the facility at which the Individual received care. After the written request for review is received, a copy of the request should be forwarded to the Emory University Privacy Officer. The medical records department also will forward a copy of the review request to a licensed Health Care Provider who is a member of the workforce of the Covered Component for review. The Health Care Provider will review the denial in a reasonable period of time in order to determine whether or not access to the information was properly denied. The reviewer will inform the medical records department and the University Privacy Officer of the results of his/her review. The medical records department will coordinate with the Health Care Providers regarding communication to the Individual of the results of the review.

REFERENCES: 45 CFR §164.524; OCGA§§ 31-33-2, -3.
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

B.5 RIGHT OF AN INDIVIDUAL TO REQUEST THAT HIS/HER PHI BE AMENDED

PURPOSE OF POLICY

The purpose of this Policy is to describe the process that an Individual must follow in order to request an amendment to his/her PHI contained in a Designated Record Set maintained by a Covered Component of the Emory Hybrid Covered Entity.

NOTE: An individual's rights under HIPAA relating to PHI created/maintained by a unit of the Emory Healthcare Affiliated Covered Entity will be governed by the *Emory Healthcare HIPAA Privacy Rule Policies.*

POLICY

An Individual has a right to request that a Covered Component of the Emory Hybrid Covered Entity amend the PHI that is contained in a Designated Record Set that the Emory Covered Component keeps on the Individual for as long as the Designated Record Set is maintained.

PROCEDURE

Request for an Amendment

The Individual must direct his/her request for an amendment to the medical records department of the facility at which the Individual received care. The request must be in writing and it must provide a reason as to why the amendment should be made. After the request is received, the medical records department will contact the Health Care Providers involved in the treatment of

the Individual and ask them to review the request in order to determine whether or not it should be granted. If the form comes directly to the treatment facility, the facility should forward a copy to the appropriate medical records department and coordinate regarding a response.

Deadlines for Acting on a Request: By no later than sixty (60) days after the request was received, the Covered Component of the Emory University Hybrid Covered Entity at which the Individual received Treatment must either take action to implement the amendment or provide the Individual with a written notice denying the amendment. The Covered Component may have a one-time, thirty day extension by writing to the Individual to let him/her know of the delay and the reasons for the delay. Communication with the Individual will be handled through the medical records department.

Accepting the Amendment

If the Covered Component accepts the amendment, then it must take the following steps: (a) identify the records within the Designated Records Set that are affected by the amendment; (b) add the amendment to those records or provide a cross-reference to the location of the amendment; (c) notify the Individual in writing that the amendment has been accepted; (d) obtain the Individual's written permission to let other persons who have the Individual's PHI or who have relied, or may in the future rely, on the Individual's PHI know of the amendment; (e) notify persons identified by the Individual as having his/her PHI and persons that the Covered Component knows have relied or may in the future rely on the PHI that is the subject of the amendment (e.g., Business Associates). Communications in this regard should generally be coordinated between the unit, Health Care Providers and medical records department.

Denial of the Amendment

If the Covered Component denies a request for an amendment, then it must provide the Individual with a written notice of the denial in plain language. The notification should generally be handled by the medical records department of the facility at which the Individual received care. The notice must state the following: (a) the reason for the denial; (b) the Individual's right to submit a written statement of disagreement with the denial and identity of the person with whom that denial should be filed; (c) a statement that even if the Individual does not file a statement of disagreement, then the Individual may request that the Individual's written request for an amendment and the denial of that request be included along with any Disclosure of the PHI that is affected by the amendment; and (d) a description of how the Individual may file a complaint about the denial with the Emory University Hybrid Covered Entity (including name, title and phone number of contact person, as set forth in the NPP) and/or with the Secretary of the Department of Health and Human Services. In addition, the medical records department and/or the health care providers involved should advise the Emory University Privacy Officer as soon as possible of any determination that a denial will be issued.

Statement of Disagreement: The Individual may give the Emory University Hybrid Covered Entity a written statement of disagreement with all or any part of a denial of a requested amendment. The statement must include the reason for the disagreement. In any further Disclosures of the PHI that are the subject of the requested amendment, the Covered Component must include the requested amendment; the denial; the statement of disagreement; and the statement of rebuttal, if any. If the Disclosure of PHI is part of a billing transaction (i.e., a

standard transaction) such that the aforementioned documents cannot be included in the original transmittal of the information, then they can be separately provided to the recipient of the standard Transaction.

No Statement of Disagreement: If the request for an amendment is denied, but he Individual does not submit a statement of disagreement, then the Individual may request the Covered component to include the request for the amendment and the denial along with any future disclosure of PHI that are affected by the denied amendment.

Statement of Rebuttal: If the Covered Component receives a Statement of Disagreement from the Individual, it may prepare and provide to the Individual a statement of rebuttal to the statement of disagreement.

Record Keeping

Each Covered Component of the Emory University Hybrid Covered Entity is responsible for identifying all of the information in an Individual's Designated Record Set that is affected by the requested amendment and appending that information or linking that information to the Individual's request for an amendment, the denial of the amendment and any statement of disagreement and/or statement of rebuttal.

Amending Records Per Notice From Another Covered Entity

If a Covered Component receives notice from another Covered Component/Entity that an Individual's PHI has been amended, then it must take action to amend its Designated Record Set appropriately.

REFERENCE: 45 CFR §164.526
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

B.6. RIGHT OF AN INDIVIDUAL TO RECEIVE AN ACCOUNTING OF DISCLOSURES OF PHI

PURPOSE OF POLICY

The purpose of this Policy is to describe the circumstances under which, and process whereby, an Individual may request an accounting of Disclosures of his/her PHI made by a Covered Component of the Emory Hybrid Covered Entity.

NOTE: An Individual's rights under HIPAA relating to PHI created/maintained by a unit of the Emory Healthcare Affiliated Covered Entity will be governed by the *Emory Healthcare HIPAA Privacy Rule Policies.*

POLICY

Individual Right to an Accounting of Disclosures

Subject to the exceptions listed below, an Individual has a right to receive from a Covered Component of the Emory University Hybrid Covered Entity an accounting of all Disclosures of his/her PHI that the Covered Component made in the six year period prior to the date on which the request is made; provided, however, that an Individual may request an accounting for a period less than the full six years.

(a) **Exceptions**: The right to an accounting does not apply to the following types of disclosures of PHI:

i. Disclosures made prior to April 14, 2003.
ii. Disclosures made to carry out the Covered Component's Treatment, Payment and Health Care Operations.
iii. Disclosure to the Individual who is the subject of the PHI.
iv. Disclosure made incident to Disclosures that are permitted or required under HIPAA.
v. Disclosure made to a correctional institution or a law enforcement official, or for national security or intelligence purposes, as set forth in *Policy D.10, HIPAA Policy Regarding Use and Disclosure of PHI for Special Government Functions*.
vi. Disclosures made as a part of a limited data set in accordance with *Policy C.5, Limited Data Sets*.
vii. Disclosures made pursuant to an authorization.
viii. Disclosures made for a facility directory in accordance with *Policy D.5, HIPAA Policy on Use and Disclosure of PHI for Facility Directories*.
ix. Disclosures made to persons involved in the Individual's care in accordance with *Policy D.1, Use and Disclosure of PHI to Individuals Involved in a Patient's Care or for Notification Purposes.*

Temporary Suspension of an Individual's Right to an Accounting

An Individual's right to receive an accounting of certain Disclosures of PHI by a Covered Component of the Emory University Hybrid Covered Entity may be temporarily suspended in the following circumstances:

(a) The Disclosures are made to a health oversight agency or a law enforcement official in accordance with *Policy D.8, HIPAA Policy Regarding Disclosure and Use of PHI for Health Oversight Activities* and/or *Policy D.13, HIPAA Policy Regarding Disclosure of PHI for Law Enforcement Purposes* if:

i. The health oversight agency or law enforcement official provides the Covered Component with a written statement that an accounting would be reasonably likely to impede the agency's/official's activities, and specifying a period for the suspension; or
ii. The agency or official makes the request verbally, in which case, the Covered Component must document the request; document the identity of the official/agency making the request; and limit the temporary suspension to thirty (30) days from the date of the request, unless a written statement is received from the agency or official in the interim.

Contents of the Accounting

The following details must be included in an accounting of Disclosures that an Emory Covered Component provides to an Individual:

(a) All the Disclosure of PHI that were made by the Emory Covered Component (including Disclosures made to or by Business Associates) for six years prior to the date of the request, with the exception of the Disclosures exempted above. The Individual may request that the accounting cover a lesser period of time.
(b) The date of each Disclosure.
(c) The name of the person or entity who received the Disclosure.
(d) A brief statement of the PHI that was Disclosed.
(e) A brief statement of the purpose of the Disclosure that lets the Individual know what the basis of the Disclosure was, or a copy of a written request for the Disclosure by any official or entity who is permitted to submit such a request under HIPAA.

Special Accounting Situations

(a) **Multiple Disclosure to a Single Entity for the Same Purpose**: If the Emory Covered Component made multiple Disclosures of the same type of PHI to a single entity for a single purpose (e.g., reporting of certain diseases to a public health agency), the Emory Covered Component may account for such Disclosures by providing an Individual with the following information:
    i. Accounting period
    ii. Date of first Disclosure of this type of PHI to this person/entity during the accounting period;
    iii. Name of person/entity who received the Disclosure
    iv. Brief description of the PHI that was Disclosed
    v. Brief Statement of the purpose of the Disclosure or written request for the Disclosure submitted by an official or agency in accordance with HIPAA
    vi. Frequency with which, or number of, Disclosures made for the accounting period.
(b) **Research Protocols**: If the Covered Component made Disclosure of PHI for a particular Research purpose for fifty (50) or more persons during the accounting period, then the Covered Component may account for such disclosures by providing a requesting Individual with the following information:
    i. The name of the protocol or Research activity for which the information was Disclosed.
    ii. A plain language description of the Research activity, including the purpose of the Research and criteria by which records were selected.
    iii. A brief description of the PHI that was Disclosed.
    iv. The date or period of time during which such Disclosures occurred or may have occurred.
    v. The date of the last Disclosure during the accounting period.
    vi. The name, address and telephone number of the entity that sponsored the Research and of the principal investigator to whom the information was disclosed;

vii. A statement that the Individual's PHI may or may not have been disclosed for a particular protocol or Research activity.
viii. If the Individual requests, the Covered Component shall assist the Individual in contacting the Research sponsor and/or the principal investigator.

PROCEDURE

(1) As specified in the NPP, an Individual must send a written request for an accounting to to the Emory Healthcare Privacy Office, 101 West Ponce de Leon Ave., 2nd Floor, Suite 242, Decatur, GA 30030. The Emory University Hybrid Covered Entity has designated the Emory Healthcare Privacy Office to receive and triage all requests received under the NPP and to refer to the Emory University Privacy Officer those requests that involve the Emory University Hybrid Covered Entity. The request must contain the patient's name and the period for which an accounting is requested.
(2) If a Covered Component of the Emory University Hybrid Covered Entity receives a request for an accounting directly, it should immediately provide a copy of the request to the Emory University Privacy Officer. The Emory University Privacy Officer will with work with the Covered Component to respond to the request.
(3) The Emory University Privacy Officer and/or the Emory Healthcare Privacy Officer will handle communications with the Individual regarding the accounting and provide the accounting to the Individual.
(4) Timetable: Within sixty (60) days after receiving an Individual's request for an accounting, the Emory University Privacy Officer must provide that accounting requested or advise the Individual that it requires an additional thirty (30) days to prepare the accounting, along with an explanation of why the extension of time is required. Only one 30-day extension is permitted. In such case, the accounting must be provided to the Individual within sixty (60) days after receiving the Individual's request.
(5) Fees: An Individual may receive one accounting during a 12-month period at no charge. A reasonable, cost-based fee may be assessed if additional accountings are requested during that period provided that the Individual is informed in advance of the fee and is permitted to withdraw or modify the request for an accounting in order to avoid or reduce the fee.
(6) Documentation: The Emory Univeristy Privacy Officer will maintain the following documents: a copy of the request for an accounting; and a copy of the response to the accounting.

REFERENCES: 45 CFR § 164.528
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

B.7. COMPLAINTS BY AN INDIVIDUAL CONCERNING PRIVACY RIGHTS, RESPONSIBILITIES, POLICIES & PROCEDURES

PURPOSE OF POLICY

The purpose of this Policy is to set forth the process by which a patient, an employee of a Covered Component of the Emory University Hybrid Covered Entity, or any other person can make a complaint regarding the Emory University Hybrid Covered Entity's privacy policies or their implementation.

POLICY

The Emory University Hybrid Covered Entity provides a process for all persons (e.g., Individuals, employees) to make complaints concerning the Emory University Hybrid Covered Entity's HIPAA privacy policies and procedures and its compliance with those policies and procedures. Persons who believe that the Emory University Hybrid Covered Entity's HIPAA privacy policies and procedures, or their implementation, are not in conformance with HIPAA regulations are encouraged to bring their complaints to the attention of the Emory University Hybrid Covered Entity by following the procedures below.

PROCEDURE

Reporting of Privacy Complaints/Concerns by Employees of the Emory Hybrid Covered Entity

Any faculty member or staff member who works for a Covered Component of the Emory Hybrid Covered Entity who wishes to report a HIPAA complaint or concern should:

(i) Report the complaint/concern to his/her department chair and/or immediate supervisor;

(ii) Report the complaint/concern in writing to the University Privacy Officer at Ste. 4-105, 1599 Clifton Rd., NE, Atlanta, GA 30322. Phone: (404) 727-2398. FAX (404) 727-2328. Email kwest02@emory.edu.

(iii) Report the complaint/concern through the Emory Trustline by phone at 1-888-550-8850 or online at www.mycomplliancereport.com/EmoryTrustlineOnline (reports may be made anonymously); or

(iv) Report the complaint/concern to the Emory Healthcare Privacy Officer at Ste. 610, Decatur Plaza, 101 W. Ponce de Leon Ave., Decatur, GA 30030. Phone: (404) 778-2186. FAX: (404) 778-2755. Email: anne.adams@emoryhealthcare.org. The Emory Healthcare Privacy Officer will in turn notify the Emory University Privacy Officer.

Faculty and staff also may report concerns and complaints directly to the Secretary of the Department of Health and Human Services. No faculty or staff member shall be retaliated against or penalized in any way for the good faith filing of any complaint or concern.

Reporting Privacy Complaints/Concerns – Individuals and their Family Members

(a) As specified in the NPP, any Individual or family member of an individual who wishes to report a HIPAA complaint or concern should do so by writing to theh Emory Healthcare Privacy Office, 101 West Ponce de Leon Ave., 2nd Floor, Suite 242, Decatur, GA 30030. The Emory University Hybrid Covered Entity has designated the Emory Healthcare Privacy Office to receive and triage all requests received under the NPP and to refer to

the Emory University Privacy Officer those requests that involve the Emory University Hybrid Covered Entity.

(b) An Individual or family member also may directly contact the Emory University Privacy Officer at Ste. 4-105, 1599 Clifton Rd., N.E., Atlanta, GA or by calling (404) 727-2398, or the Indivual or family member may report the complaint/concern through the Emory Trustline by phone at 1-888-550-8850 or online at www.mycomplliancereport.com/EmoryTrustlineOnline (reports may be made anonymously).

(c) Individuals and their family members also may report concerns and complaints directly to the Secretary of the Department of Health and Human Services.

(d) Neither Individuals nor their family members will be penalized for reporting a complaint or concern.

Documentation of Receipt of a Complaint/Concern

(a) The person who receives a complaint under the processes outlined above must document receipt of the complaint/concern. Documentation must include (to the extent it is available): the date on which complaint/concern was received; name of complainant and telephone number; and a description of the nature of the complaint/concern. A copy of this documentation should be immediately forwarded to the Emory University Privacy Officer via secure email to kwest02@emory.edu or telefax to (404) 727-2328.

(b) If the Emory University Privacy Officer initially receives the complaint, then he/she will document the complaint as set forth above.

(c) Documentation of the complaint/concern and any investigation and resolution thereof shall be maintained by the Emory University Privacy Officer for six years after the date on which the complaint or concern was received.

Investigation of a Complaint/Concern and Imposition of Corrective Action/Sanctions

(a) The Emory University Privacy Officer will investigate any complaint/concerns that are received pursuant to this Policy; provided, however, that if the complaint concerns a unit with in the Emory Healthcare Affiliated Covered Entity, then the complaint shall be referred to the Emory Healthcare Privacy Officer for investigation and response. All Emory University units and personnel shall cooperate with the Emory University Privacy Officer and/or the Emory Healthcare Privacy Officer in the conduct of any investigation. The Emory University Privacy Officer and/or the Emory Healthcare Privacy Officer may receive assistance from other appropriate Emory units in conducting the investigation.

(b) Once a complaint has been received by the Emory University Privacy Officer, the appropriate personnel/units will be notified of the matter being investigated, and any necessary interviews and document/material reviews will take place.

(c) After the investigation is completed, the Emory University Hybrid Covered Entity acting through the appropriate department/office will cause appropriate corrective and preventative action to be taken. In addition, in accordance with appropriate unit and University policies, any appropriate disciplinary action and sanctions, up to and including termination, may be imposed against persons found to have violated HIPAA requirements, these Policies, or any other applicable policies and procedures.

REFERENCES: 45 CFR §§164.503(a)(1)(ii) & (d)
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

SECTION C: GENERAL HIPAA POLICIES REGARDING USES AND DISCLOSURES OF PHI

C.1. HIPAA POLICY REGARDING USE AND DISCLOSURE OF PHI FOR TREATMENT, PAYMENT, AND HEALTHCARE OPERATIONS

PURPOSE OF POLICY

The purpose of this Policy is to describe how a Covered Component of the Emory University Hybrid Covered Entity may use an Individual's PHI for Treatment, Payment and Health Care Operations purposes.

POLICY

Disclosures of PHI for Treatment, Payment & Health Care Operations

A Covered Component of the Emory University Hybrid Covered Entity may obtain consent from an Individual to use his/her PHI to carry out Treatment, Payment or Health Care Operations. The Covered Component, however, may Use and Disclose an Individual's PHI for Treatment, Payment and Health Care Operations without first obtaining from the Individual consent or a written Authorization that contains all HIPAA-required elements, provided that the Use or Disclosure falls within one of the categories below:

(a) The Covered Component may Use or Disclose an Individual's PHI for its own Treatment, Payment or Health Care Operations.
(b) The Covered Component may Disclose an Individual's PHI for the Treatment activities of a Health Care Provider.
(c) The Covered Component may disclose an Individual's PHI to another Covered Entity or a Health Care Provider for the Payment activities of the entity that receives the PHI.
(d) The Covered Component may disclose an Individual's PHI to another Covered Entity for the Health Care Operations of the entity that receives the PHI if both the Covered Component and Covered Entity has, or had, a relationship with the Individual; the PHI pertains to the relationship; and the Disclosure is for quality assessment, quality control or peer review purposes, or for the purpose of health care fraud, and abuse detection or compliance.
(e) The Covered Component may disclose PHI about an Individual to other participants in an OHCA in which the Covered Component is a member for any Health Care Operations activities of the OHCA.

Marketing, Psychotherapy Notes, and Sale of Protected Health Information

Notwithstanding the general rule that an Individual's PHI may be used for Treatment, Payment or Health Care Operations without an Authorization, the Covered Component must always obtain an individual's Authorization to Use his/her PHI for Marketing; to Use or Disclose Psychotherapy Notes; and for the sale of PHI. Additionally, applicable laws of the State of Georgia may impose additional authorization requirements with respect to certain categories of information (e.g., communications between a psychologist and a patient).

PROCEDURE

Consent for Treatment

If a Covered Component's utilizes a consent for Treatment, that consent may contain permission for the Use and Disclosure of the Individual's PHI for Treatment, Payment and Health Care Operations purposes and for any other purposes described in the Emory NPP. The Covered Component will maintain a copy of any consent as a part of the Individual's medical records.

APPLICABILITY OF MINIMUM NECESSARY & ACCOUNTRING RULES

Minimum Necessary Rule: The Mininum Necessary Rule does not apply to Disclosures made for Treatment. The Minimum Necessary Rule applies to any other Uses and Disclosures permitted under the Policy that are not made to an Individual or made pursuant to the written Authorization of the Individual.

Accounting Rule: A Covered Component is not required to maintain records of the Disclosure of PHI for Treatment, Payment and Health Care Operations purposes permitted under this Policy, or for Disclosures made to the Individual, or pursuant to the Individual's written Authorization. The Covered Component must maintain records of all other Disclosures permitted under this Policy in order to provide an Individual with an accounting of such Disclosures upon his/her request. The records must be maintained for a period of six years following the date of the Disclosure.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCES: 45 CFR §164.506.
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

C.2. USES AND DISCLOSURES OF PHI THAT REQUIRE: (A) AUTHORIZATION; (B) NO AUTHORIZATION, BUT OPPORTUNITY FOR THE INDIVIDUAL TO AGREE OR OBJECT; AND (C) NO AUTHORIZATION AND NO OPPORTUNITY TO AGREE OR OBJECT

PURPOSE OF POLICY

The purpose of this policy is to set forth the categories of Uses and Disclosures of PHI under HIPAA and their corresponding requirements in terms of Authorization or Opportunity to Object. This policy also contains cross-references to specific Policies that detail the HIPAA requirements for each specific use or disclosure. This Policy also describes the elements that an Authorization must contain and the means by which an Individual must be given an opportunity to agree or object.

POLICY

General Rule Regarding Authorizations

Unless otherwise permitted by a specific HIPAA regulation (as summarized below), a Covered Component of the Emory University Hybrid Covered Entity may not Use or Disclose PHI without a valid written Authorization from the Individual. If the Covered Component receives a written Authorization for its own Use or Disclosure of PHI, then any Use or Disclosure that it makes of such PHI must be consistent with the terms and conditions of the Authorization. The Covered Component must retain any signed Authorization that it receives. To be valid, the Authorization must contain the elements specified below in this policy.

General Rule Regarding Providing an Individual the Opportunity to Agree or Object

In the instances described below, a Covered Component of the Emory University Hybrid Covered Entity may Use or Disclose an Individual's PHI without first obtaining an Authorization, provided that the Individual is given an opportunity to agree or object to the Use/Disclosure. Except as otherwise described below with respect to a specific Use or Disclosure, the Covered Component must inform the Individual in advance of the Use or Disclosure of his/her PHI and permit him/her to agree to, or to prohibit or restrict the Use or Disclosure. The opportunity to agree or object may be in the form of a written document, or it may be done verbally. If done verbally, the Covered Component should document that the Individual was provided with the opportunity, and the Individual's choice also should be documented.

Uses and Disclosures for which an Authorization is Required

(a) Psychotherapy Notes -- A valid Authorization is generally required for the Use or Disclosure of Psychotherapy Notes. *See Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information.*

(b) Marketing – A valid Authorization is generally required to use an Individual's PHI for Marketing. See *Policy D.3, HIPAA Policy Regarding Use and Disclosure of PHI for Marketing Purposes*.

(c) Sale of Protected Health Information – A valid Authorization is generally required for the Sale of an Individual's PHI. See *Policy A.10, Sale of PHI.*

Use and Disclosure for which an Authorization is not Required, but for which the an Individual must have an Opportunity to Agree or Object

The Covered Component may make the following Uses/Disclosures without the necessity for obtaining an Authorization, provided that the Individual is given an opportunity to agree or object as detailed in the specific Emory Policies listed below.

(a) Use and Disclosure of PHI for facility directories. See *Policy D.5, HIPAA Policy Regarding Use and Disclosure of PHI for Facility Directories*.

(b) Use and Disclosure to persons involved in an Individual's care and for notification purposes. See *Policy D.1, Use and Disclosure of PHI to Individuals Involved in an Individual's Care and for Notification Purposes*.

Uses and Disclosures for which Neither an Authorization nor an Opportunity for the Individual to Agree or Object is Required

The Covered Component may make the following Uses/Disclosures of PHI without having an Individual's Authorization or providing the Individual an opportunity to agree or object to the Use/Disclosure. There is a specific Emory policy regarding each of the types of Uses/Disclosures for which an opportunity to agree or object is required. These Policies should be consulted prior to making any such Use/Disclosure.

(a) Uses and Disclosures to carry out a Covered Component's Treatment, Payment or Health Care Operations, except for disclosure of Psychotherapy Notes (see Policy D.15, *Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*) or Disclosure of PHI for Marketing purposes (see *Policy D.3, HIPAA Policy Regarding Use and Disclosure of PHI for Marketing Purposes*).

(b) Uses and Disclosures for public health activities. See *Policy D.6, HIPAA Policy Regarding Use and Disclosure of HI for Public Health Activities and Workplace Surveillance Related Activities and Student Immunizations.*

(c) Disclosures about victims of abuse, neglect, or domestic violence. See *Policy D.7, HIPAA Policy Regarding Use and Disclosure of PHI in Connection with Reporting of child Abuse; Abuse, Neglect or Domestic Violence Converning Adults Who Are Not Elder Persons or Disabled Adults; and Abuse or Neglect of an elder Person or Disabled Adult.*

(d) Uses and Disclosure for health oversight activities. See *Policy D.8, HIPAA Policy Regarding Disclosure and Use of PHI for Health Oversight Activities.*

(e) Disclosures for judicial and administrative purposes. See *Policy D.12, HIPAA Policy Regarding Disclosures of PHI for Judicial and Administrative Proceedings.*

(f) Disclosures for law enforcement purposes. See *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes.*

(g) Uses and disclosures about decedents. See *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAa rules Regarding Coroners, Medical Examiners, Funeral Directors, Tisue/Cadaver Donation, and Research Using Deceased Individual's Information.*

(h) Uses and Disclosures for cadaveric organ, eye or tissue donation purposes. See *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tisue/Cadaver Donation, and Research Using Deceased Individual's Information.*

(i) Uses and Disclosures for Research purposes, provided that the Institutional Review Board (IRB) or Privacy Board has approved an alteration to or a Waiver of an Authorization. See *Policy D.14, HIPAA Policy Regarding the Use and Disclosure of PHI for Research Purposes and the Role of the Institutional Review Board.*

(j) Uses and disclosures to avert a serious threat to health or safety. See *Policy D.9, HIPAA Policy Regarding Use and Disclosure of PHI to Avert a Serious Threat to Health or Safety.*

(k) Uses and Disclosures for specialized government functions. See *Policy D.10, HIPAA Policy Regarding Use and Disclosure of PHI for Special Government Functions.*

(l) Disclosures for workers compensation purposes. See *Policy D.11, HIPAA Policy Regarding Use and Disclosure of PHI for Workers Compensation Purposes.*

Uses/Disclosures of PHI Not Covered Under Any of the Categories Listed Above

If a Use or Disclosure does not fall under any of the categories listed above, then the Covered Component must have a written Authorization from the Individual in order to Use or Disclose his/her PHI.

Required Elements of a Valid Authorization

To be valid, an Authorization must contain the following elements. The Authorization also may contain additional information or elements, provided that they are not inconsistent with the required elements described below:

(a) The Authorization must be written and be in plain language.

(b) The Authorization must state that the Individual will be provided with a copy of the signed document and that the Emory Covered Component also will retain a copy of the document. Verbal authorization is not valid except when the IRB grants an alteration of the Authorization's requirements to permit verbal Authorization for Research. See *Policy D.14, HIPAA Policy Regarding the Use and Disclosure of PHI for Research Purposes and the Role of the Institutional Review Board.*

(c) A description of the PHI to be Used or Disclosed that identifies the information in a specific and meaningful fashion.

(d) The name or other specific identification of the person(s) or class of persons authorized to make the requested Use or Disclosure.

(e) The name or other specific identification of the person(s) or class of persons to whom the Covered Component may make the requested Use or Disclosure.
(f) A description of each purpose of the requested Use or Disclosure. [NOTE: The statement "at the request of the Individual" is a sufficient description of the purpose, if an Individual initiates the Authorization and does not provide a statement of the purpose.]
(g) An expiration date or expiration event that relates to the Individual or to the purpose of the Use or Disclosure. The statement "End of the Research Study," "None" or similar language is sufficient if the Authorization is for a Use or Disclosure or PHI for Research, including the creation or maintenance of a Research database or repository.
(h) The signature of the Individual and date, or if the Authorization is signed by a personal representative of the Individual, the representative's signature, along with a statement of the representative's authority to act for such Individual
(i) A statement of the Individual's right to revoke his/her Authorization in writing, along with a description of the HIPAA-permitted manner in which PHI collected prior to the revocation may be used after revocation.
(j) A statement as to whether or not Treatment, Payment or enrollment for benefits or in Research will or will not be conditioned upon signing the Authorization. [See below regarding conditioning an Authorization.]
(k) A statement of the potential for information Disclosed pursuant to the Authorization to be re-disclosed by the person(s) who receive the PHI, and no longer be protected by HIPAA requirements.
(l) If the Authorization is for Research purposes and the researcher wants to defer the Individual's right to access his/her Research records until the end of the Research study, then a statement to this effect also must be included in the Authorization.
(m) An Authorization for the Disclosure of Psychotherapy Notes cannot be combined with any different type of Authorization.
(n) An Authorization for Marketing that involves financial remuneration must specifically state that such remuneration is involved.
(o) An Authorization for the Sale of PHI must state that Disclosure of the PHI will result in financial remuneration.

Defective Authorizations

An Authorization will be invalid if it contains any of the following defects:

(a) The expiration date has passed or the Covered Component knows that the expiration event has occurred.
(b) The Authorization has not been filled out completely such that one of the mandatory elements is not present.
(c) The Covered Component knows that the Authorization has been revoked.
(d) The Authorization is inappropriately combined with another document or inappropriately conditions Treatment, Payment, enrollment or eligibility on signing the Authorization.
(e) The Covered Component knows that any material information that is contained in the Authorization is false.

Prohibition on Conditioning of Authorizations

An Authorization may not condition Treatment, Payment, enrollment in a Health Plan, or eligibility for benefits on an Individual signing an Authorization, except as follows:

a. For Research-related Treatment, including permitted compound Authorizations.
b. For Health Plan enrollment, eligibility, risk rating or underwriting determinations, provided that the Authorization does not ask for Use or Disclosure of Psychotherapy Notes.
c. For providing Health Care solely for the purpose of creating PHI for Disclosure to a third party (e.g., conducting a physical on behalf an employer for determining fitness related to the performance of a job duty).

Prohibition Against Compound Authorizations

An Authorization may not be combined with any other document except as follows:

(a) An Authorization for a Research project may be combined with the informed consent document that will be used in the Research project; or with another Authorization for the same study; or with an Authorization for the creation or maintenance of a Research database or repository. If one of the Authorizations in a compound Authorization conditions the provision of Research-related treatment on agreeing to the Authorization, then the Authorization must clearly differentiate between the conditioned and unconditioned components. Additionally, the Authorization must provide the individual with an opportunity to opt in to the Research activities described in the unconditioned Authorization.
(b) An Authorization for the use or disclosure of Psychotherapy Notes may only be combined with another Authorization for the use or Disclosure of Psychotherapy Notes.
(c) An Authorization that does not pertain to Psychotherapy Notes and that is not conditioned on anything may be combined with another Authorization.

Revocation of Authorization

An Individual may revoke his/her Authorization by sending a written notice of the Revocation to the person to whom the Authorization was provided or to the person designated in the Notice of Privacy Practices. Revocation will not apply with regard to any action that the Covered Component has taken in reliance on the Authorization, or if the Authorization was a requirement for obtaining insurance.

Consents v. Authorizations

Under HIPAA, a Covered Component may use an Individual's PHI for Treatment, Payment and Health Care Operations without the necessity of having the Individual's Authorization. HIPAA, however, does not prohibit a Covered Component from obtaining an Individual's consent for the Use or Disclosure of PHI for Treatment, Payment and Health Care Operations. Covered Components may ask Individuals to sign a consent for Treatment, which includes provisions regarding the use of PHI for Treatment, Payment and Health Care Operations. This type of consent, however, is not sufficient to permit the Covered Component to make any Use or Disclosure of the PHI for purposes other than Treatment, Payment or Health Care Operations. To make any additional uses of the PHI, an Authorization that meets all of the HIPAA

requirements must be obtained. Additionally, with the exception of consents and Authorizations used for Research projects, an Authorization may not be combined with an informed consent document for Treatment.

PROCEDURE

Forms

Each Covered Component within the Emory University Hybrid Covered Entity should review its forms to ensure that it has appropriate consents and Authorizations. Sample forms will be posted from time to time on the Office of Compliance website at http://compliance.emory.edu/.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule: The type and amount of PHI Disclosed pursuant to an Authorization is governed by the wording of the Authorization. Disclosures pursuant to the HIPAA regulations that require affording the Individual an opportunity to object are limited to the amount and type of information permitted by those requirements, should the Individual not raise an objection. Unless otherwise stated under a specific policy, for all other Disclosures the minimum necessary type and amount PHI should be Disclosed that satisfies the purpose of the Disclosure.

Accounting Rule: The Accounting Rule does not apply to Disclosure made pursuant to an Authorization. Additional exceptions to the Accounting Rule are set forth in Policy B.6, Right of an Individual tor Receive an Accounting of Disclosures of PHI.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCES: 45 CFR §§164.501; 164.506; 164.508; 164.510; 164.512.
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

C.3. HIPAA POLICY REGARDING PERSONAL REPRESENTATIVES

PURPOSE OF POLICY

The purpose of this Policy is to set forth the circumstances under which a Covered Component of the Emory University Hybrid Covered Entity must treat someone as the personal representative of an Individual with regard to the Use and Disclosure of the Individual's PHI. This Policy also sets forth the standards for determining which person shouled be recognized as an Individual's personal representative.

DEFINITIONS

The definitions of the following terms are presented here for convenience. These terms also appear in the Glossary.

"Minor": Under the laws of the State of Georgia, a person who has not yet attained 18 years of age is considered to be a Minor.

"Emancipated Minor": Under the laws of the State of Georgia, an Emancipated Minor is a person who has not yet attained 18 yeas of age, but who is married; in the armed services; or is self-supporting and declared to be emancipated by a court of law. An Emancipated Minor is treated the same as an adult who is 18 years of age or older.

POLICY

General Rule Regarding Personal Representatives

An Individual who is not physically or legally capable of representing himself/herself or an Individual who desires to designate someone to act on his/her behalf, may be represented by a personal representative, provided such representation is in accordance with the laws of the State of Georgia. A personal representative has the Individual's rights and responsibilities under HIPAA that are consistent with the extent of the scope of the person's representation. For example, if an Individual is legally incompetent and has a court-appointed legal guardian who is in charge of all health care decisions for the Individual, then that guardian is recognized as the Individual's personal representative for HIPAA purposes and may have access to all PHI necessary to make Health Care decisions. A Covered Component of the Emory University Hybrid Covered Entity must treat the personal representative of an Individual in the same way that it would treat the Individual for purposes of complying with the HIPAA regulations. In the case of a Minor, the Minor's parent or guardian is treated as his/her personal representative for HIPAA purposes.

Scope of PHI that May be Disclosed to Personal Representative

A Covered Component of the Emory University Hybrid Covered Entity may Use and Disclose with the personal representative PHI that is relevant to and within the scope of the person's representation of the Individual. If the scope of the person's representation is broad (e.g., the person has the authority to make all health care decisions for a person), then the scope of the PHI that may be shared with the personal representative is broad enough to permit the representative

to perform his/her duties. Alternatively, if the scope of the representation is limited (e.g., the person only has the authority to determine if life-sustaining measures should be withdrawn from an individual in a vegetative state), then the PHI that may be shared with the representative will be limited to carrying out the specific, limited purpose of the representation.

Determining Who is Recognized as an Individual's Personal Representative

(1) **Adult or Emancipated Minor**: If the Individual is an adult or Emancipated Minor, the Covered Component must treat as the Individual's personal representative, a person who, under applicable law, has the authority to act on behalf of the Individual in making decisions related to Health Care.

(a) Georgia Law Regarding Persons Who Have Authority to Act on Behalf of an Individual with Respect to Decisions Related to Health Care: In general, Emory Covered Components will look at the laws of the State of Georgia to determine who has the authority to act on behalf of person with respect to health-care related decisions. Under Georgia law, the following persons may consent to lawful surgical or medical Treatment which may be recommended, prescribed or directed by a duly licensed physician:

(i) An adult for him/herself whether by living will, advance directive for health care or otherwise.
(ii) Any person authorized to give consent for an adult under an advance directive for Health Care or durable power of attorney for Health Care. [NOTE: In accordance with OCGA § 31-33-2, if the requestor is a legally authorized representative of the patient, then he/she must provide written authorization indicating that he/she is authorized to have access to the patient's records.]
(iii) Any married person, whether an adult or minor, for him/herself and for his/her spouse.
(iv) Any person temporarily standing in the place of parent, whether formally serving or not, for the Minor under his/her care; and any guardian for his/her ward.
(v) In the absence or unavailability of a living spouse, any parent, whether an adult or a Minor for his/her Minor child.
(vi) Any female, regardless of age or marital status, for herself when given in connection with pregnancy, or the prevention thereof, or childbirth; provided, however, that certain notice requirements pertain to abortion procedures performed on Minors who are not Emancipated Minors.
(vii) In the event that an adult cannot consent for him/herself, and if there is no person to consent under sections (a) to (f) above, then the persons listed below may consent in the following order of priority:

1. Any adult child for his/her parent(s).
2. Any parent for his/her adult child.
3. Any adult for his/her brother or sister.
4. Any grandparent for his/her grandchild.
5. Any adult grandchild for his/her grandparent.

6. Any adult niece, nephew, aunt or uncle of the patient who is related to the patient in the first degree.
7. Upon the inability of any adult to consent for him/herself, and in the absence of any person to consent under this section, an adult friend of the patient.

(b) Minors: In general, the Covered Component will treat a Minor's parent or guardian as the Minor's personal representative for HIPAA purposes. If the Minor does not have a parent or guardian, then the Covered Component will treat another person or entity who is acting in the place of the parent or guardian and who has the authority under applicable law to act on behalf of the Minor to make decisions related to Health Care. There are a few exceptions to this general rule, when the Covered Component will treat the Minor as the person with rights and responsibilities under HIPAA, instead of the Minor's parent, guardian or person acting in place of the parent/guardian. Under the exceptions listed below, the Covered Component will treat the Minor as the person having rights and responsibilities under HIPAA:

(i) Applicable law requires **only** that the Minor consent to obtain a particular Health Care service; the Minor consents (even if another person has also consented); and the Minor has not requested another person to be treated as his/her personal representative.
(ii) Applicable law permits the Minor to obtain a particular health care service without the consent of parent, guardian, or person standing in their place and the Minor, a court, or another person authorized by law consents to the Health Care service.
(iii) A parent, guardian, or person acting in the place of a parent/guardian assents to an agreement of confidentiality between a Health Care Provider and the Minor with respect to a particular Health Care service.

HOWEVER, even when a Minor is treated as the person having the rights and responsibilities under HIPAA, the Covered Componet must follow applicable state law in providing access to PHI to parents/guardians or persons acting in their place. Specifically, in any of the situations outlined in (a) – (c) above, when a parent/guardian or person acting in their place is not treated as the Minor's personal representative, and the parent/guardian or person acting in their place requests access to the Minor's PHI under the rights of access granted by HIPAA (see *Policy B.4, Individual Right to Access PHI*), then:

(i) The Covered Component will/may provide access to the Minor's PHI if there is a state law or other law that permits or requires a Covered Entity to provide access.
(ii) The Covered Component will not provide access to the Minor's PHI if there is a state law or other law that prohibits a Covered Component from providing access.
(iii) The Covered Component will have a licensed Health Care Provider make a decision in the exercise of his/her professional judgment as to whether or not to disclose a Minor's PHI, if there isn't state law or other law that requires,

permits or prohibits disclosure of the Minor's PHI, and this action is consistent with applicable law.

(c) Circumstances Involving Minors under Georgia Law in which the Foregoing HIPAA Rules Apply:

(j) **Abortion:** Georgia law permits a Minor to consent to an abortion, but requires a physician to notify a parent or guardian before performing the abortion. This disclosure of PHI to a parent/guardian is permitted under HIPAA. Additionally, because the Minor can consent to the abortion, she also can sign the HIPAA Authorization for PHI relating to the abortion.
REFERENCE: OCGA §15-11-682

(ii) Treatment for Drug Abuse: Georgia law permits a Minor to consent to medical treatment for drug abuse. A treating physician, member of the medical staff of a hospital or public clinic or licensed physician, may, but is not required to, inform the spouse, parent, custodian or guardian of the Minor as to the treatment given or needed. This disclosure of PHI is permitted under HIPAA. Additionally, because the Minor can consent to the medical treatment for drug abuse, he/she can sign a HIPAA Authorization for PHI related to the treatment for drug abuse.
REFERENCE: OCGA. § 37-7-8

(iii) Treatment for Venereal Disease: Georgia law permits a Minor who professes to be afflicted with a Veneral Disease or at risk for HIV to consent to procedures and therapy related to conditions or illnesses arising out of such Veneral Disease or HIV diagnosis. A treating physician, member of the medical staff of a hospital or public clinic, or a licensed physician, may, but is not required to inform the spouse, parent, custodian or guardian of the Minor as to to the treatment given or needed. Additionally, because the Minor can consent to treatment for Venereal Disease or HIV, he/she can sign a HIPAA Authorization regarding PHI related to the treatment. NOTE: "Venereal disease" is narrowly defined under Georgia law as "syphilis, gonorrhea and chancroid." Accordingly, for treatment of any other type of venereal disease, the Minor's parent/guardian is required to consent to the treatment and would be treated as the Minor's personal representative for HIPAA purposes.
REFERENCE: OCGA. 31-17-1 & H.B. 1058 (2016).

(iv) AIDS Confidential Information: Georgia law permits AIDS confidential information to be disclosed to a Minor, and it also specifies that such information may be disclosed to the parent or guardian of a Minor.
REFERENCE: OCGA. §§ 24-9-7; 31-22-9.12; Georgia H.B. 1058 (2016).

(d) Deceased Individuals: For deceased Individuals whose PHI is subject to HIPAA (see *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individulas and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation, and Research Using Deceased Individual's Information*), the Covered Component will treat an executor, administrator or other person who, under applicable law, has authority to act on behalf of the deceased Individual or his/her estate as the deceased person's personal representative, with respect to PHI relevant to that representation. In this regard,

Georgia law states that the persons, in the order set forth below, may have access to an Individual's PHI contained in his/her patient records:

(i) The executor, administrator, or temporary administrator for the decedent's estate, if such person has been appointed.
(ii) The surviving spouse of the decedent, if an executor, administrator, or temporary administrator for the decedent's estate has not been appointed.
(iii) Any surviving child, if there is no surviving spouse and no executor, administrator, or temporary administrator has been appointed.
(iv) Any parent, if there is no surviving spouse or child and there is no executor, administrator or temporary administrator has been appointed.

REFERENCE: OCGA § 31-33-2

Circumstances Under which a Covered Component may Refuse to Recognize a Personal Representative

Notwithstanding any state law or other HIPAA requirement regarding personal representatives to the contrary, under the circumstances listed below, the Emory Covered Component may refuse to treat as a personal representative a person who would otherwise qualify to be treated as such:

(a) The Emory Covered Component has a reasonable belief that the Individual has been or may be subjected to domestic violence, abuse or neglect by the person who would be the personal representative; or
(b) The Emory Covered Component has a reasonable belief that treating the person as the personal representative could endanger the Individual; or
(c) The Emory Covered Component in the exercise of its professional judgment decides that it is not in the best interest of the Individual to treat the person as the Individual's personal representative.

PROCEDURE

(1) Before recognizing any person as the personal representative of an Individual, the Covered Component will verify that the person has the authority to serve as the Individual's personal representative and that no circumstances apply that would prohibit the Emory Covered Component from recognizing the person as the Individual's personal representative.
(2) In verifying that a person may serve as the personal representative, the Emory Covered Component shall make and retain copies of any identification and/or other documentation establishing that the person is authorized to be the Individual's personal representative (e.g., power of attorney, advance directive, etc.).

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule: HIPAA states that if adults and emancipated Minors have personal representatives who can act on their behalf in making decision regarding Health Care, then PHI that is relevant to the subject matter of the personal representation may be Disclosed to those

representatives. In general, personal representatives may have access to any PHI that may impact their health care decision making.

Accounting Rule: Because the personal representative stands in the place of the Individual under HIPAA and an accounting does not need to be made for Disclosures to the Individual, the accounting rule similarly does not apply to Disclosures made to personal representatives.

REFERENCES: 45 C.F.R. § 164.502(g); OCGA §§ 15-11-201; 15-11-682; 31-9-2; 31-17-1; 31-17-7; 31-33-2; 37-7-8.

RESOURCES: DHHS OCR Guidance "Personal Representatives", revised September 19, 2013 at www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/personalreps.html ;
DHHS OCR Guidance, "HIPAA and Same-sex Marriage: Understanding Spouse, Family Member, and Marriage in the Privacy Rule," Sept. 2014 at www.hhs.gov/ocr/privacy/hipaa/understanding/special/samesexmarriage/index.html.
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2003

C.4. DE-IDENTIFICATION OF PHI

PURPOSE OF POLICY

The purpose of this policy is to specify the process for de-identifying PHI in accordance with HIPAA regulations so that the information will no longer be considered PHI that is subject to HIPAA regulations.

POLICY

Health information is not subject to the HIPAA Privacy Rule if it is de-identified in accordance with HIPAA requirements. No Authorization from an Individual is required to Use or Disclose Health Information that is de-identified. Health Information is considered de-identified if (a) it does not identify an Individual; and (b) there is no reasonable basis to believe it can be used to identify an Individual.

PROCEDURE

Procedures for De-Identification

One of two methods can be used to de-identify Health Information:

(a) Method 1 – Expert Determination

A person with appropriate knowledge and expertise in applying generally accepted statistical and scientific principles and methods for making information not individually identifiable determines that the risk is very small that the information could be used (either by itself or in combination with other available information) by anticipated recipients to identify an Individual. If this

method of de-identification is used, the analytical methods used and results of the analysis must be documented and the documentation must be retained. Persons using the Expert Determination Method to de-identify Health Information should consult the *Guidance on Satisfying the Expert Determination Method* contained in the Department of Health and Human Services, Office of Civil Rights *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* found at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html#guidancedetermination for information about correct implementation of the Expert Determination Method.

(b) Method 2 – Safe Harbor Method

Removal of all of the following identifiers as they pertain to an Individual or to his/her relatives, employers or household members (collectively referred to below as "Individuals"):

- Names
- Addresses (including any email, web URL and postal addresses), except that the names of Individuals' states may be retained along with the first three digits of a zip code if the geographical area that the zip code encompasses has a population of over 20,000 people.
- All parts of a date directly related to Individuals except years (e.g., dates of birth and death, and admission and discharge dates).
- All ages over 89, in which case the Individuals' ages must be categorized as "89 or older."
- Numerical identifiers (including telephone numbers, fax numbers, IP addresses and Social Security numbers; medical record numbers; health plan beneficiary and account numbers; certificate/license numbers; vehicle identification numbers, including license plate numbers, serial numbers and device identifiers.
- Biometric identifiers (including finger and voice prints).
- Full-face photographic images.
- Any other unique identifying number, characteristic or code except any code used by the Covered Component to re-identify the information; provided, however, that such code must not be related in any want to the identifiers that must be removed in order for the information to be de-identified and only the Covered Component can have access to the code and/or use the code for re-identification.

AND

- After removing the identifiers, the Covered Component does not have actual knowledge that the remaining information could be used alone, or in combination with other information available to the recipient, to identify an Individual.

Persons using the Safe Harbor Method to de-identify Health Information should consult the *Guidance on Satisfying the Safe Harbor Method* contained in the Department of Health and Human Services, Office of Civil Rights *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* found at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html#guidancedetermination for information about correct implementation of the Safe Harbor Method.

Data that Does not Need to be Removed to De-Identify Health Information

- Age (except age over 89 years, as specified above)
- Gender
- Race
- Ethnicity
- Marital Status
- State of Residence
- Parts of zip code numbers in certain circumstances, as explained above
- Years

Re-Identification

The Covered Component may use codes or other similar means of marking records so that they can later be re-identified, but only by the Covered Component. Further, the code may not contain information about the Individual and may not be derived from the identifiers removed from the Health Information. For example, a re-identification code may not be derived from Individuals' social security numbers or medical record numbers. In addition, if a re-identification code is use, the Covered Component may not use or disclose the code for any other purpose, nor may it disclose the mechanism for re-identification (e.g., table algorithms, formula or other tools that could be used to link the code with the Individual).

Who may De-Identify Information?

Only workforce members of a Covered Component or a Business Associate with whom the Covered Component has contracted may de-identify Covered Component Health Information. If a third-party Business Associate is used for this purpose, then there must be a Business Associate Agreement in place.

Other De-Identification Standards

The de-identification standard set forth in this Policy sets forth the HIPAA requirements for de-identification, however, other, stricter standards regarding De-identification may apply, e.g., state laws, de-identification standards imposed by sponsors of research, etc. Additionally, although an Individual's Authorization is not required to Use/Disclose de-identified Health Information, in some cases, stricter standards may apply that require obtaining an Individual's consent for the Use/Disclosure of de-identified PHI (e.g., the National Institutes of Health Genomic Data Sharing Policy requires an Individual's informed consent for the Use/Disclosure of certain types of Research data, even though the data has been de-identified in accordance with HIPAA standards). When these stricter standards are applicable, they must be followed.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Because de-identified Health Information is not subject to HIPAA Requirements, the Minimum Necessary and Accounting Rules do not apply.

REFERENCES: 45 CFR § 164.514(a)
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2003

C.5. LIMITED DATA SETS

PURPOSE OF POLICY

The purpose of this policy is to specify the process for removing certain identifying information from PHI in order to create a Limited Data Set that may be Disclosed for Research, public health, or Health Care Operations purposes once the intended recipient of the PHI enters into a Data Use Agreement that restricts the way in which PHI regarding an Individual can be Used/Disclosed.

POLICY

Creation of Limited Data Set

A Covered Component of the Emory University Hybrid Covered Entity may Use or Disclose Health Information for purposes of Research, public health or Health Care Operations if the Health Information has been stripped of the identifiers listed below and the Emory Covered Component obtains a Data Use Agreement from the person/entity to whom the Limited Data Set is to be supplied:

- Names
- Addresses (including any email, web URL and postal addresses), except that the names of Individuals' states may be retained along with the first three digits of a zip code if the geographical area that the zip code encompasses has a population of over 20,000 people.
- All parts of a date directly related to Individuals except years (e.g., dates of birth and death, and admission and discharge dates).
- All ages over 89, in which case the Individuals' ages must be categorized as "89 or older."
- Numerical identifiers (including telephone numbers, fax numbers, IP addresses and Social Security numbers; medical record numbers; health plan beneficiary and account numbers; certificate/license numbers; vehicle identification numbers, including license plate numbers, serial numbers and device identifiers.
- Biometric identifiers (including finger and voice prints).
- Full-face photographic images.
- Any other unique identifying number, characteristic or code except any code used by the Covered Component to re-identify the information; provided, however, that such code must not be related in any want to the identifiers that must be removed in order for the information to be de-identified and only the Covered Component can have access to the code and/or use the code for re-identification.

The Limited Data Set may contain the following data elements: town, city, state and zip code; date of birth; date of death; and admission or discharge dates.

Who May Create a Limited Data Set

Only workforce members of the Emory Covered Component or Business Associates may create a Limited Data Set. If a third-party Business Associate creates a Limited Data Set there must be a Business Associate Agreement in place.

Required Elements of a Data Use Agreement

A Data Use Agreement must contain the following elements:

(a) A description of the permitted Uses and Disclosures of the Limited Data set, which must be limited to and consistent with public health, Research or Health Care Operations purposes;
(b) A description of those persons who are permitted to Use or receive the Limited Data Set;
(c) A statement requiring that the Limited Data Set recipient will:
    i. Not Use or further Disclose the information other than as permitted in the Data Use Agreement or as required by law;
    ii. Use appropriate safeguards to prevent the Use or Disclosure of the information other than as permitted in the Data Use Agreement.
    iii. Report to the Covered Component any Use or Disclosure of the information that is not permitted by the Data Use Agreement of which it becomes aware.
    iv. Ensure that any agents to whom it provides the Limited Data Set agrees to the same restrictions and conditions that apply to the Limited Data Set recipient; and
    v. Not identify the information or contact the Individuals who are the subject of the information.

Non-Compliant Limited Data Set Recipients

If at any time the Emory Covered Component becomes aware that a recipient of a Data Use Agreement has undertaken a pattern of activity or practice that constitutes a material breach or violation of the Data Use Agreement, then the Covered Component must:

(a) Take reasonable steps to cure the breach or end the violation; or
(b) If the breach cannot be cured or the violation ended, then stop Disclosing the Limited Data to the recipient and report the problem to the Secretary of the Department of Health and Human Services.

PROCEDURE

Data Use Agreements for Research Purposes

Researchers who desire to transfer a Limited Data Set to another person/entity for Research purposes should go to the following website: http://compliance.emory.edu/documents/DTA_Instructions.pdf. On the website, the researcher should select and follow the appropriate instructions for the type of data transfer that will take place. In general:

(a) The Emory Office of Sponsored Programs should be contacted regarding incoming or outgoing data transfers that are part of an Emory clinical trial

agreement, sponsored research agreement or contract that governs human subject interaction/intervention by the Emory researcher. The Emory Office of Sponsored Programs will review/provide/negotiate/execute any necessary Data Use Agreement for these types of situations.

(b) The Emory Office of Technology Transfer manages incoming data transfers covering receipt by an Emory investigator of human subject data to be used for Research purposes not involving a clinical trial or human subject intervention by the Emory investigator. The Emory Office of Technology Transfer will review/provide/negotiate/execute any necessary Date Use Agreement for these types of situation.
any necessary Data Use Agreement for these types of situations.

(c) The transfer of data outside of Emory University must be approved by the unit that is the source of the data transferred (e.g., Emory University School of Medicine, Emory Healthcare). To transfer data outside of the University, a researcher must complete an Outgoing Data Transfer Questionnaire located at http://compliance.emory.edu/documents/DTA_Instructions.pdf and submit it somdta@emory.edu. The Questionnaire will be evaluated and the researcher will be advised as to which unit will handle the routing and execution of the associated Data Transfer Agreement.

Other Data Use Agreements

Proposed Data Use Agreements for incoming or outgoing Limited Data Sets for public health or Health Care Operations purposes in association with a sponsored Research project conducted by an Emory University unit should be referred to the Office of Sponsored Programs for review/negotiation/execution. Any other proposed Data Use Agreements not falling into a previously mentioned category should be sent to the Emory University Privacy Officer for evaluation and direction as to appropriate routing/execution.

Execution of Data Use Agreements

Only persons who are authorized to sign agreements on behalf of Emory University under Emory University Policy 1.2, *Contract Approval and Signature Authority* at http://policies.emory.edu/1.2 may sign Data Use Agreements or other agreements governing data transfers.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule: Because a Limited Data Set is by definition limited in the about of PHI included, the Minimum Necessary Rule does not apply.

Accounting Rule: PHI Disclosed as a part of a Limited Data Set is not subject to the Accounting Rule.

REFERENCES: 45 CFR §164.514(e)
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

C.6. VERIFICATION REQUIREMENTS FOR DISCLOSURE OF PHI

PURPOSE OF POLICY

The purpose of this Policy is to establish standards for verifying a person's or entity's identity and authority to have access to an Individual's Protected Health Information before making a EDEisclosure of that Protected Health Information.

POLICY

Verification of Identity

Before making any Disclosure of PHI, a Covered Component of the Emory University Hybrid Covered Entity shall verify the identity of the person/entity requesting the Disclosure and the authority of such person/entity to receive the PHI.

If the HIPAA regulations call for a particular form of verification of identity or Authorization for a particular Disclosure (e.g, written assurance from a researcher in the case of a Disclosure of PHI made Preparatory to Research) then that form is required. In cases in which particular documents, statements or representations are required in order to make the Disclosure, the Covered Component can rely on documents, statements or representations that on their face meet the applicable requirements, if it is reasonable for the Covered Component to do so under the circumstances.

In situations in which a particular form of verification is not prescribed by HIPAA regulations or University policies, the following methods of verification shall be utilized:

> **(a) Verification of Identity When an Individual is Requesting the PHI In-Person**: If the Individual is known to the Covered Component than no further verification procedure need be undertaken. If the Individual is not known to the Covered Component, then the Covered Component shall ask the Individual to provide a picture identification, such as a driver's license, passport or other government-issued identification, or an employment identification. If a picture identification is not available, then the Individual's Social Security card or birth certificate should be requested. A photocopy should be made of the means of identification that is provided and kept with the Individual's records.
> **(b) Verification of Identity When an Individual is Requesting the PHI Over the Telephone**: Prior to Disclosing any PHI over the telephone, including appointment reminders, the Covered Component will make reasonable efforts to verify the identity of the person to whom it is speaking by asking the Individual for his/her name, and requiring him/her to confirm his/her address, phone number and birth date.
> **(c) Verification of the Identity and Authorization of a Personal Representative of an Adult or Emancipated Minor**: The same procedures as are described above will be used to verify the identity of a personal representative. Additionally, the personal representative should be asked for documentation that sets forth the basis for the representation, e.g, Power of Attorney, statement of relationship to Individual, etc. Finally, in the case of a personal representative requesting health records from a Health Care Provider under OCGA § 31-33-2, the Covered Component must ask the personal

representative to provide a signed, written authorization indicating that he/she is authorized to have access to the patient's records in accordance with that code section, as well as a signed Authorization that meets HIPAA requirements.

(d) **Verification of the Identity and Authorization of a Personal Representative of a Minor**: The Covered Component will verify the identity of the personal representative as set forth above. If the personal representative is the child's parent or guardian and is with the child, then no further verification of authorization is required; otherwise a signed, written statement of relationship to the minor will be requested, along with a copy of any supporting documentation (e.g., court appointment as guardian). The Covered Component must record the method of verification used in the Individual's records.

(e) Verification of the Identity and Authorization of Law Enforcement Officials if Request is to Disclose PHI for Certain Law Enforcement Purposes: The Covered Component will ask to see the law enforcement official's official identification and also will request the subpoena, summons, request for records, civil or authorized investigative demand, or similar legal process by which the PHI is being requested. A photocopy of this legal process will be kept in the Individual's records. The Emory University Office of General Counsel should be contacted immediately in the event of a request to Disclose PHI for law enforcement purposes, and if at all possible, review the request before Disclosure is made.

(f) Verification of the Identify of a Public Official: If a public official is making the request for Disclosure in person, the Covered Component will ask to see the person's official governmental identification credentials and document that credentials were reviewed. If the public official is making the request in writing, then verification will be made by checking to make sure the request is on official letterhead. The Emory University Office of General Counsel should be contacted immediately in the event of a request to Disclose PHI for law enforcement purposes, and if at all possible, review the request before Disclosure is made.

(g) Verification of the Identity of a Person Acting on Behalf of a Public Official: The Covered Component will ask for a written statement on official letterhead from the governmental agency for whom the person is acting stating that the person is acting on behalf of the governmental agency. Alternatively, a contract, memorandum of understanding or purchase order that shows the person is acting on behalf of the government agency can be used for verification. The Emory University Office of General Counsel should be contacted immediately in the event of a request to Disclose PHI for law enforcement purposes, and if at all possible, review the request before Disclosure is made.

(h) Verification of the Authority of a Public Official: After verifying the identity of the public official or person acting on behalf of a public official, the Covered Component will request a written statement of the legal authority under which the PHI is being requested. If the request is made per legal process (i.e., a warrant, subpoena, order or other legal process issued by a court, grand jury or administrative tribunal), then such legal process is presumed to constitute legal authority to disclose the PHI. If the Disclosure is not being made pursuant to legal process, and if it is impractical to obtain a written statement of legal authority under the circumstances, then the Covered Component may rely on an oral statement, and it will document the statement. Upon receipt of the documentation of legal authority or legal process, the Covered Component

should forward the same to the Office of the General Counsel for review prior to Disclosure.

(i) Verification Requirements for Disclosures made to Persons Involved in the Individual's Care and Treatment and in Emergency Circumstances: The Covered Component will exercise its professional judgment to determine whether it is in the best interest of the Individual to make a Disclosure of the Individual's PHI to family members, close friends, an adult acting on behalf of a child or others in situations, including emergency situations, in which the Individual is unavailable or unable to give his/her Authorization for Disclosure. The Office of the General Counsel should be contacted to review the matter prior to making such a Disclosure.

(j) Verification Requirements for Disclosure Made to Avert a Serious Threat to Health & Safety: The Covered Component may act on a good faith belief in Disclosing information that it believes would help to avert or substantially lessen a threat to health or safety to a person who is reasonably able to avert or lessen the threat. The Office of the General Counsel should be contacted to review the matter prior to making such a Disclosure.

(k) Verification Requirements for Disclosure Made to Researchers: The Emory Covered Component shall request from the researchers any written assurances that are specified in *Policy D.14, HIPAA Policy Regarding the Use and Disclosure of PHI for Research Purposes and the Role of the Institutional Review Board.*

PROCEDURE

In addition to following the verification procedures described above, a description of the verification procedures that were used should be included in the Individual's records, along with the original or a photocopy of any relevant documents.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

The applicability of the Minimum Necessary and Accounting Rules will depend on the requirements of the particular HIPAA regulation under which a Disclosure is made. Accordingly, the Covered Component should consult the policy for the HIPAA provision under which the Disclosure is sought/being made.

REFERENCES: 45 CFR §§ 164.510; 164.512(f), (i) & (j); 164.514(h).
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2003

SECTION D: HIPAA POLICIES REGARDING USES AND DISCLOSURES OF PHI FOR SPECIFIC PURPOSES

D.1. USE AND DISCLOSURE OF PHI TO INDIVIDUALS INVOLVED IN AN INDIVIDUAL'S CARE AND FOR NOTIFICATION PURPOSES

PURPOSE OF POLICY

The purpose of this policy is to describe the HIPAA requirements regarding the Use and Disclosure of PHI regarding an Individual to family, friends and other persons involved in the Individual's care and for notification purposes.

POLICY

A Covered Component of the Emory University Hybrid Covered Entity will determine what PHI may be Disclosured to friends, family and other persons involved in the Individual's care, as well as for notification purposes concering the Individual based on whether the Individual is:

(a) Present and has the capacity to consent;
(b) Is not present and/or does not have the capacity to consent; or
(c) Is deceased.

PROCEDURE

(A) Uses and Disclosures if the Individual is Present and has the Capacity to Consent

If the Individual is present for or otherwise available prior to a Use or Disclosure of PHI, has the capacity to make Health Care decisions, and either (i) agrees to the Use or Disclosure after having been provided with an opportunity to object; or (ii) does not express an objection; or (iii) if the Covered Component of the Emory University Hybrid Covered Entity using its professional judgment, can reasonably infer from the circumstances that the Individual does not object to the Disclosure, then the Covered Component may, without written consent or Authorization:

(1) Disclose to a family member, relative, close personal friend or any other person identified by the Individual, PHI that is directly relevant to the Individual's Health Care or Payment for that Health Care.

(B) Uses and Disclosure if the Individual is not Present or does not have the Capacity to Consent

If the Individual is not present, or if there are emergency circumstances, or if the Individual does not have the capacity to agree to or object to the Use or Disclosure, then the Emory Covered Component may, in the exercise of its professional judgment, determine whether the Disclosure is in the best interests of the Individual and if so:

(2) Make the Disclosures specified under (A)(1) above, but only with regard to PHI that is directly relevant to the involvement of the person to whom the Disclosure is made with respect to the Health Care of the Individual, or Payment for that Health Care.

(3) Make Disclosures that are based on reasonable inferences regarding the Individual's best interest in allowing a person to act on behalf of the Individual in picking-up filled prescriptions, medical supplies, x-rays, or Disclosing other similar PHI.

Notwithstanding the foregoing, with respect to PHI that may be considered privileged under the laws of the State of Georgia (e.g., Psychotherapy Notes, communications between a licensed mental health care provider and a patient), the Covered Component should contact the Emory University Office of General Counsel for guidance prior to making a Disclosure of such PHI pursuant to this section.

(C) Uses and Disclosures when the Individual is Deceased

If an Individual is deceased, a Covered Component of the Emory University Hybrid Covered Entity may Disclose to the persons listed below PHI relevant to the involvement of such persons in the Individual's Health Care or Payment for Health Care prior to the Individual's death:

(1) Individual's family member or other relative
(2) Individual's personal representative
(3) Individual's close personal friend
(4) Any other person identified by the Individual who was involved in the Individual's Health Care or Payment for Health Care

Provided, however, that any such Disclosure must not be inconsistent with any prior expressed preference of the Individual known to the Covered Component. Notwithstanding the foregoing, with respect to PHI that may be considered privileged under the laws of the State of Georgia (e.g., Psychotherapy Notes, communications between a licensed mental health care provider and a patient), the Covered Component should contact the Emory University Office of General Counsel for guidance prior to making a Disclosure of such PHI pursuant to this section.

(D) Uses and Disclosures to Notify or Assist in Notifying a Family Member or Personal Representative of an Individual

A Covered Component of the Emory University Hybrid Covered Entity may Use or Disclose PHI to notify, or assist in the notification of (including identifying or locating) an Individual's family member, personal representative, or other person responsible for the Individual's care. The PHI that may be Used or Disclosed is limited to information about the Individual's location, general condition or death. The Use or Disclosure must be conducted in accordance with Sections (A), (B) or (C) above, as applicable.

(E) Uses and Disclosures for Disaster Relief Purposes

In order to assist in disaster relief efforts, a Covered Component of the Emory University Hybrid Covered Entity may make the notification Disclosures set forth above in Section (D) to a public or private entity that is authorized by law or by its charge to assist in disaster relief efforts; provided, however, that the Disclosures must be made in accordance with Sections (A), (B) or (C), as applicable, unless, the Covered Component in the exercise of its professional judgment determines that the requirements of those sections would interfere with the ability to respond in emergency circumstances.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING

Minimum Necessary Rule: The minimum PHI that is necessary to achieve the purpose of the Disclosure should be disclosed; provided, however, that if the Disclosure is being made to a public official, then the Emory Covered Component may rely on the representations of the public

official that the type and amount of PHI requested is the minimum necessary type and amount of PHI.

Accounting Rule: Disclosures made pursuant to this policy are subject to a request for an accounting by an Individual. Accordingly the Emory Covered Component that makes the Disclosure should document the Disclosure and maintain this documentation for six years after the Disclosure.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCES: 45 CFR §§ 164.510; 164.502(f) & (g); 164.512(f)(4); 164.512(g) – (i); OCGA §§ 31-17-1; 31-21-3.
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

D.2. HIPAA POLICY REGARDING USE AND DISCLOSURE OF PHI OF DECEASED INDIVIDUALS AND SPECIAL HIPAA RULES REGARDING CORONERS, MEDICAL EXAMINERS, FUNERAL DIRECTORS, TISSUE/CADAVER DONATION, AND RESEARCH USING DECEASED INDIVIDUAL'S INFORMATION

PURPOSE OF POLICY

The purpose of this policy is twofold: (a) to describe how these Policies apply to the PHI of a Deceased Individual; and (b) to establish standards for how a Deceased Individual's PHI may be used for Research purposes.

POLICY

Applicability of HIPAA to Deceased Individuals

A Covered Component of the Emory University Hybrid Covered Entity will ensure that unless otherwise expressly permitted by HIPAA regulations and these Policies, the PHI of Deceased Individuals is subject to the same standards regarding Use and Disclosure as apply to the PHI of living Individuals for a period of fifty (50) years following the date of the deceased Individual's death. Additionally, special rules regarding the use of the PHI of a deceased Individual apply in the following circumstances: Use and Disclosure of such PHI to coroners, medical examiners and funeral directors; for organ, eye and tissue donation; and for Research purposes.

Disclosures to Coroners and Medical Examiners

The Emory Covered Component may Disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased Individual, determining a cause of death, or other duties authorized by law. If the Covered Component performs any of the duties of a medical examiner or coroner under Georgia law, it may use PHI for the aforesaid purposes. O.C.G.A. Title 45, Chapt. 16 sets forth the duties of coroners/medical examiners in the State of Georgia, and should be consulted in determining what duties are authorized by law. O.C.G.A. § 45-16.10 sets forth the circumstances under which records may be released from a medical facility in the State of Georgia to the coroner of another state with respect to a deceased Individual who was injured in, a resident of, or buried in the county of the out-of-state coroner, or pursuant to a subpoena issued by the out-of-state coroner.

Disclosures to Funeral Directors

Consistent with applicable law, the Covered Component may Disclose PHI regarding a Deceased Individual to funeral directors to carry out their duties with respect to a Deceased Individual. If necessary for the funeral director to carry out its duties, the Covered Component may Disclose PHI prior to, and in reasonable anticipation of an Individual's death. Additionally, the following requirements of OCGA § 31-21-3 shall apply to Deceased Individuals who had certain infectious diseases, and limit the information that may be Disclosed regarding these persons:

> **Georgia Law Regarding PHI Concerning Infectious Disease of a Deceased Individual**: Pursuant to O.C.G.A. § 31-21-3, if a deceased Individual who has infectious hepatitis; tuberculosis; syphilis, gonorrhea or chancroid; or AIDs (all of these diseases singularly and collectively referred to in this Policy as "Infectious or Communicable Disease") dies, and if the attending physician or other person making arrangements for the disposition of the body know of the Infectious or Communicable Disease, then that person is required to prepare a written notice describing the Infectious or Communicable Disease for those involved in the care and disposition of the body. **Notwithstanding anything to the contrary under HIPAA that would permit a broader Disclosure of this information, in Georgia, the information that is contained in this notice is privileged and confidential under Georgia law, and may only be further Disclosed if:**
>
> > (i) The Disclosure is required pursuant to law, but only to the extent required by law.

(ii) The Disclosure is made by a physician in accordance with any law authorizing a physician to Disclose otherwise privileged information.

(iii) The Disclosure involves information about a deceased minor and the Disclosure is made to the parent or guardian of the minor.

(iv) The Disclosure is made to the person who picks up the dead body, or is made in the ordinary course of business to any employee or agent of any person or entity who is authorized or required under Georgia law to receive or report the information contained in the notice.

(v) The Disclosure is for Research purposes and does not reveal the identity of the Deceased Individual, or information that would reveal the identity of the Deceased Individual.

(vi) The Disclosure involves information regarding the sexual assault or sexual exploitation of a deceased minor child and is required to be reported pursuant to any other law requiring the reporting of such assault/exploitation, but only to the extent that such Disclosure is required to be reported.

(vii) Information contained in the notice may not be Disclosed pursuant to discovery proceedings, subpoena or court order.

Disclosure/Use of PHI for Organ, Eye, Tissue of Cadaver Donation Purposes

A Covered Component may Use or Disclose PHI for/to organ procurement organizations or other entities engaged in the procurement, banking, transplantation of cadaveric organs, eyes or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

Disclosure to Law Enforcement Officials

A Covered Component may Disclose a deceased Individual's PHI to a law enforcement official for the purpose of alerting law enforcement of the deceased Individual's death if the Covered Component has a suspicion that the death may have resulted from criminal conduct.

Research Using a Deceased Individual's PHI

The Emory Covered Component may Disclose a deceased Individual's PHI to a researcher for Research purposes if it obtains from the researcher a written assurance that contains the following elements:

(i) A written representation that the Use or Disclosure is sought solely for Research on the PHI of decedents.

(iii) A written representation that the PHI for which Use or Disclosure is sought is necessary for Research purposes.

Additionally, the Emory Covered Component may request documentation of the death of the Individual(s) whose PHI is requested. The Covered Entity or Covered Component from which the PHI is requested may have its own form assurance containing the foregoing representations

that the requestor must complete and sign. A sample assurance is attached to this Policy as **Attachment D.2 -1**.

PROCEDURE

Verification

Prior to releasing a Deceased Individual's PHI to any of the persons/entities specified above for the purposed described in this Policy, the Emory Covered Component shall verify the identity and authority of person/entity to whom the PHI is be released and document that this verification process took place, including the retention of copies of any associated documentation. See Policy C.6, *Verification Requirements for Disclosure of PHI*.

Disclosure of a Deceased Individual's PHI to Personal Representatives

For requirements regarding Disclosure of a deceased Individual's PHI to a Personal Representative see *Policy C.3, HIPAA Policy Regarding Personal Representatives.*

Disclosure to Family Member or Other Persons Involved in the Decedent's Care

For requirements regarding Disclosure of a deceased Individual's PHI to family members who cared for the Deceased Individual see *Policy D.1, Use and Disclosure of PHI to Individuals Involved in an Individual's Care and for Notification Purposes.*

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

(1) Personal Representatives: Only the PHI relevant to the subject of the personal representation should be disclosed to the personal representative of the deceased Individual. As the personal representative stands in the place of the deceased Individual with regard to Disclosures made pursuant to this policy, no accounting needs to be made for such Disclosures.

(2) Disclosures to Coroners, Medical Examiners and Funeral Directors and Disclosures for Organ, Eye and Tissue Donation: Only the minimum necessary PHI required to fulfill the purpose of the Disclosure should be released. The Covered Component is entitled to rely on the representations of public officials and professionals who are members of the Covered Component's workforce that the PHI being requested is the minimum amount necessary to fulfill the purpose of the request. The Covered Component should keep records of Disclosures made for these purposes because a Personal Representative of the deceased Individual may request an accounting of these Disclosures.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following

policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCES: 45 C.F.R. §§164.502(f) & (g); 45 C.F.R. §§164.512(g)-(i); OCGA §§31-17-1 & 31-21-3; OCGA Title 45, Chapt. 16.

RESOURCES:

DHHS Guidance "Health Information of Deceased Individuals", created September 19, 2013
www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/decedents.html

DHHS OCR FAQs "Do the HIPAA Privacy protections apply to the health information of deceased individuals?"
www.hhs.gov/ocr/privacy/hipaa/faq/decedents/1500.html

DATE OF POLICY: April 14, 2003.
REVISED: September 1, 2016

Attachment D.2-1: Assurance Regarding Disclosure of a Decedent's PHI for Research Purposes

Name of Researcher/Title:

Department:

Brief Description of Research:

Name of Research Project for which PHI is Being Requested:

Name of Emory Covered Component Unit from Which PHI is Being Requested:

Names or Descriptions of Specific Decedent(s) or Class of Decedents Whose PHI is Being Requested:

Description of PHI Being Requested:

Description of How the Researcher will Protect the PHI Being Requested, Including When Identifiers will be Destroyed:

Assurance: The undersigned researcher hereby provides his/her assurance that the PHI requested above (a) is the PHI of decedents; (b) is being requested solely for the purpose of research on the PHI of decedents for the Research Project described above; and (c) is necessary for conduct of this Research Project. The undersigned researcher understands and agrees that upon request by the unit of the Emory Covered Component from whom the PHI is sought, he/she will provide documentation establishing that the Individual's(s') whose PHI is/are being requested is/are deceased.

Signature of Researcher:_____Date:_____

For Use by Emory Covered Component:
Researcher requested to provide documentation establishing that PHI requested is that of decedents: ____ Yes ____ No
If requested, description of documentation provided and date provided:_____
PHI Provided to Researcher: ____ No ___Yes Date Provided:_____

D.3. HIPAA POLICY REGARDING USE AND DISCLOSURE OF PHI FOR MARKETING PURPOSES

PURPOSE OF POLICY

This purpose of this Policy is set forth the HIPAA requirements for the use of and disclosure of PHI for Marketing purposes.

POLICY

Authorization Required in Order to Use/Disclose PHI for Marketing

A Covered Component of the Emory University Hybrid Covered Entity will not use PHI for Marketing purposes without first obtaining the Individual's Authorization except in the following circumstances:

(a) A face-to-face communication between the Covered Component and the Individual; or
(b) A promotional gift of nominal value from the Covered Component to the Individual.

The Covered Component will not sell or Disclose PHI to a third party for purposes of Marketing the third party's product without first obtaining an Individual's Authorization; provided, however, that a Covered Component may Disclose PHI to a third party that is conducting Marketing on behalf of the Covered Component in one of the manners described in (a) or (b) above.

Permissible Communications Not Considered Marketing

The Covered Component may make the following communications with an Individual without Authorization, provided that the Covered Component does not receive Financial Remuneration in exchange for making the communication:

(a) A communication by the Covered Component that describes a health-related product or service provided by the Covered Component
(b) A communication concerning Treatment of the Individual (e.g., referral to a specialist by the Individual's Health Care Provider)
(c) A communication for the Individual's case management, coordination of care or to direct or recommend alternative Treatment.

PROCEDURE

Communication

If the Covered Component desires to use PHI to inform Individuals of services or products offered by the Covered Component it must: (i) identify in the communication (including newsletters) that the Emory Covered Component is the entity that is making the communication; and (ii) if a third party is providing direct or indirect Financial Remuneration to the Emory

Covered Component with respect to the communication, then this fact and the name of the third party must be prominently stated in the communication.

Business Associate Agreement

The Emory Covered Component will require any third party that conducts Marketing on its behalf to enter into a Business Associate Agreement.

Authorization Elements

The Authorization for Marketing must meet all HIPAA requirements for a valid Authorization as set forth in *Policy C.2, Uses and Disclosure of PHI that Require: (a) Authorizaiton; (b) No Authorization, but Opportunity for the Individual to Agree or Object; and (c) No Authorizaiton and No Opportunity to Agree or Objec*t. Additionally, if the Marketing communication concerns the description of a third party's product or service, and the Covered Component receives Financial Remuneration from, or on behalf of, the third party, then the Authorization must state that Financial Remuneration is involved.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule: If the Emory Covered Component is making a Disclosure of PHI without an Individual's Authorization, then the Covered Component must only disclose the Minimum Necessary type and amount of PHI that is required to achieve the purpose of the Disclosure.

Accounting Rule: Unless an Individual has authorized a Disclosure, the Disclosure of PHI under this policy is subject to a request for an Accounting by an Individual. The Covered Component that makes the Disclosure will document the Disclosure and maintain this documentation for six (6) years after the Disclosure occurs.

REFERENCES: 45 CFR §§164.501; 164.508(a)(3); 164.508(b).

RESOURCES:
DHHS OCR HIPAA FAQ on Marketing at http://www.hhs.gov/hipaa/for-professionals/faq/marketing

DHHS Guidance -- *The HIPAA Privacy Rule and Refill Reminders and Other Communications about a Drug or Biologic Currently Being Prescribed for the Individual*, created December 19, 2013 at http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/refill-reminders/index.html

DATE OF POLICY: April 14, 2003.
REVISED: September 1, 2016.

D.4. HIPAA POLICY REGARDING THE USE AND DISCLOSURE OF PHI FOR FUNDRAISING

PURPOSE OF POLICY

The purpose of this Policy is to set forth the circumstances under which a Covered Component of the Emory University Hybrid Covered Entity may Use or Disclose an Individual's PHI for fundraising purposes with, or without, the Individual's Authorization.

POLICY

General Rule for Obtaining an Authorization

A Covered Component of the Emory University Hybrid Covered Entity will obtain an Individual's Authorization prior to Using or Disclosing the Individual's PHI for the purpose of fundraising for the benefit of the Covered Component and/or the Emory University Hybrid Covered Entity, except as set forth below.

Exceptions to the General Rule for Obtaining an Authorization

Without the necessity of obtaining the Individual's Authorization, the Covered Component may Use the Individual's PHI described below, or Disclose such PHI to an institutionally-related foundation or Business Associate, for the purpose of raising funds for the benefit of the Covered Component and/or the Emory University Hybrid Covered Entity:

i. Demographic information, including name, address and other contact information, age, gender and date of birth.
ii. Dates of Health Care provided to the Individual
iii. Identification of department that provided service
iv. Treating physician
v. Outcome information
vi. Health insurance status

Fundraising Statement Included in Notice of Privacy Practices

A statement describing how the Emory University Hybrid Covered Entity may use PHI for fundraising purposes is included in the Emory University Hybrid Covered Component's Notice of Privacy Practices that is provided to each Individual in accordance with these Policies.

Individual's Right to Opt Out of Fundraising

In any fundraising materials that are sent to an Individual based on PHI obtained as described above, the Emory University Hybrid Covered Entity will include a statement that informs the Individual how he/she may opt out of receiving any further communications regarding fundraising. The statement must instruct the Individual that he/she should sent his/her written opt-out request to the Development and Alumni Relations Office, Robert W. Woodruff Health Sciences Center, 1440 Clifton Rd., Suite 116, Atlanta, GA 30322 or he/she may call 404-727-7111

The Emory University Hybrid Covered Entity may not make fundraising communications to an Individual under this policy if an Individual has elected not to receive such communications; however, the Individual may be provided with a method to opt back in to receive fundraising communications.

No Conditioning of Treatment or Payment

The Emory University Hybrid Covered Entity may not condition Treatment or Payment on the Individual's choice with respect to receipt of fundraising communications.

PROCEDURE

(a) Institutional advancement personnel shall process all opt-out requests promptly upon receipt.
(b) Records of Individual opt-out requests will be maintained and processed by institutional advancement personnel for the Woodruff Health Sciences Center.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule: Only the specific PHI identified above may be utilized for fundraising without an Individual's Authorization.

Accounting Rule: Unless the Individual has Authorized a specific Disclosure, Disclosure of PHI pursuant to this policy is subject to a request for an Accounting by the Individual. Accordingly, the Emory University Hybrid Covered Entity, or the Covered Component that makes the Disclosure, must document the Disclosure and maintain this documentation for six (6) years after the Disclosure.

REFERENCES: 45 CFR §§164.508; 164.514(f); 164.520(b).

D.5. HIPAA POLICY REGARDING USE AND DISCLOSURE OF PHI FOR FACILITY DIRECTORIES

PURPOSE OF POLICY

The purpose of this policy is to establish standards for the Use and Disclosure of PHI regarding any Individual in a facility directory in those circumstances, if any, in which such facility directories are maintained in facilities directly operated by a Covered Component of the Emory University Hybrid Covered Entity.

POLICY

Emory Healthcare (EHC) Facilities

With regard to any Individual located in or associated with facilities owned or operated by EHC, the EHC policy regarding Use and Disclosure of PHI for the particular facility in question shall govern.

Facilities Owned or Operated by Other Entities

With regard to any Individuals located in or associated with facilities owned or operated by any entity other than a Covered Component of the Emory University Hybrid Covered Entity.(e.g.,

Grady Hospital or Children's Healthcare of Atlanta), the HIPAA policy of the facility's owner or operator regarding the Use and Disclosure of PHI shall govern.

Facilities Operated by Covered Components of the Emory Hybrid Covered Entity that Provide Patient Services

With regard to any Individuals who are located in facilities that provide patient services and that are owned or operated solely by the a Covered Component of the Emory University Hybrid Covered Entity, the requirements below will apply with respect to the Use and Disclosure of PHI in a facility directory that includes patient information, if any, maintained by the facility:

(a) Use of PHI – A Covered Component may use the following PHI to maintain a directory of Individuals located within its facilities:
    1. Individual's name
    2. Individual's location in the facility
    3. Individual's condition described in general terms that does not communicate specific medical information about the Individual; and
    4. Individual's religious affiliation

(b) Disclosure of PHI – With the exception of religious affiliation, a Covered Component may disclose the foregoing information to persons who contact the Emory Covered Component and ask for the Individual by name. In addition to receiving the foregoing information, members of the clergy also may receive information on religious affiliation.

(c) Opportunity to Object – A Covered Component will advise each Individual who comes to its facilities of the PHI that it may include in a directory (if any directory is maintained) and the persons to whom it may Disclose this PHI (including members of the clergy). The Covered Component also shall provide the Individual with the opportunity to restrict or prohibit some or all of these Uses or Disclosures by notifying the Covered Component.

(d) Opportunity to Object in Emergency Circumstances – If the Individual is unable to be offered the foregoing opportunity to object because of his/her incapacity or emergency circumstances, then the Covered Component may make some or all of the Uses or Disclosures of PHI set forth above if such Use or Disclosure is:
    (a) Consistent with any preference of the Individual, if any, that was previously expressed to the Covered Component; and
    (b) In the Individual's best interest, as determined by the Covered Component in its professional judgment.

    The Covered Component must then inform the Individual and provide an opportunity to object to these Uses or Disclosures when it become practicable to do so.

PROCEDURE

The Individual's agreement or objection to/restriction of the Disclosure of PHI pursuant to this Policy must be noted in the Individual's record, and if an objection is registered, then the beginning of the record (or outside cover, if the record is kept in hard copy) should be marked to indicate that there is a restriction regarding the Disclosure of PHI.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary: The more stringent principles regarding the very limited amount of PHI that may be Disclosed for facility directories take precedence over the more general requirements of the Minimum Necessary rule.

Accounting – Disclosures made pursuant to this policy are exempt from any request for an accounting by an Individual.

REFERENCES: 45 C.F.R. §164.510(a)

RESOURCES:
DHHS CMS MEMORANDUM Hospital Patient Privacy and Medical Record Confidentiality, March 2, 2012

DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

D.6. HIPAA POLICY REGARDING USE AND DISCLOSURE OF PHI FOR PUBLIC HEALTH ACTIVITIES AND WORKPLACE SURVEILLANCE RELATED ACTIVITIES, AND STUDENT IMMUNIZATIONS

PURPOSE OF POLICY

The purpose of the Policy is to provide standards for the Covered Component of the Emory Hybrid Covered Entity to Disclose PHI regarding an Individual to governmental or other agencies or authorities for public health purposes or activities, including but not limited to the reporting to the FDA of information regarding FDA-regulated products; Disclosing PHI regarding workplace related illness, injury or surveillance; and Disclosing PHI regarding student immunizations.

POLICY

Public Health Related Uses and Disclosures

A Covered Component of the Emory University Hybrid Covered Entity may Disclose PHI as follows:

(a) To public health authorities that are authorized by law to collect or receive PHI for the purpose of:

(i) preventing/controlling disease, injury, or disability, including, but not limited to the reporting of disease, injury and vital events such as birth or death; and
(ii) conducting public health surveillance, public health investigations and public health interventions.

(b) To foreign government agencies that are acting in collaboration with a Public Health Authority, but only at the direction of the Public Health Authority.

(c)To a public health authorities or other appropriate governmental authorities authorized by law to receive reports of Child Abuse and/or neglect (See *Policy D.7, HIPAA Policy Regarding Use and Disclosure of PHI in Connection with Reporting of Child Abuse; Abuse, Neglect or Domestic Violence Concering Adults Who are not Elder Persons or Disabled Adults; and Abuse or Neglect of an Elder Person or Disabled Adult*.)

(d) To a person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product (e.g., a drug company) or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity including:

i. Collecting or reporting adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations.
ii. Tracking FDA-regulated products.
iii. Conducting product recalls, repairs, or replacements or look-backs (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of look-backs);
iv. Conducting post-marketing surveillance.

(e) To a person who may have been exposed to a communicable disease, or who is at risk of contracting or spreading a disease or condition, if the Covered Component or Public Health Authority is authorized to notify the person in the conduct of a public health intervention/investigation.

Workplace Health Surveillance Related Disclosures

A Health Care Provider who is part of a Covered Component can disclose PHI regarding an employee to the employer of that employee, if:

(a) The Health Care Provider provides Health Care to the Individual at the request of the employer; and

(b) The Health Care Provider is conducting an evaluation relating to the medical surveillance of the employee's workplace, or is evaluating whether the employee has a work-related illness or injury; and

(c) The PHI that is disclosed consists of findings concerning a work-related injury or illness or regarding workplace-related medical surveillance; and

(d) The employer needs the finding in order to comply with its obligation to record the injury or illness or to carry out its workplace medical surveillance obligations under OSHA standards or similar federal or state laws; and

(e) The Health Care Provider provides written notice to the employee stating that the Health Care Provider will be disclosing PHI relating to medical surveillance of the workplace or work-related illnesses and injuries by:

(i) Giving a copy of the notice to the employee at the time the Health Care is provided; or

(ii) By posting the notice in a prominent place at the location at which the Health Care is provided, if provided at the employer's worksite.

Student Immunization Information Disclosures

The Emory Covered Component may Disclose PHI to a school about an Individual who is a student or prospective student of the school if:

a. The PHI Disclosed is limited to proof of immunization;
b. The school is required by law to have such proof of immunization prior to admitting the Individual; and
c. The Covered Component obtains and documents the agreement to the Disclosure from:
    i. The Individual, if the Individual is an adult or emancipated minor; or
    ii. A parent, guardian, or other person acting in the place of a parent of the Individual, if the Individual is an unemancipated minor.

PROCEDURE

Prior to releasing any PHI to public health authorities or regulated persons pursuant to the foregoing policy, the Emory Covered Component shall verify the identity and authority of the Public Health Authority/regulated person. For workplace surveillance related Disclosures, the notice process described above shall be followed. For student immunization Disclosures to a school, the agreement to the Disclsoure shall be documented by the Covered Component and the documentation retained for the appropriate period.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule: The purpose of the Disclosure will govern the type and amount of PHI to be Disclosed; provided, however, that if the Disclosure is being made to a public official, then the Emory Covered Component may rely on the representations of the public official that the type and amount of PHI requested is the minimum necessary type and amount of PHI.

Accounting: Disclosures made pursuant to this policy are subject to a request for an accounting by an Individual. Accordingly, the Covered Component that makes the Disclosure should document the Disclosure and maintain this documentation for six years after the Disclosure.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy*

Notes and Mental Health Information; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCES: 45 CFR §512(b)(v) – (vi).
DATE OF POLICY: April 2003
REVISED: September 1, 2016

D.7 HIPAA POLICY REGARDING USE AND DISCLOSURE OF PHI IN CONNECTION WITH REPORTING OF CHILD ABUSE; ABUSE, NEGLECT OR DOMESTIC VIOLENCE CONCERNING ADULTS WHO ARE NOT ELDER PERSONS OR DISABLEDADULTS; AND ABUSE OR NEGLECT OF AN ELDER PERSON OR DISABLED ADULT

PURPOSE OF POLICY

The purpose of this policy is to provide guidance for a Covered Component of the Emory University Hybrid Covered Entity in its Use and Disclosure of Protected Health Information (PHI) that concerns an Individual who may be a victim of abuse, neglect, or domestic violence. This policy provides specific guidance for Uses and Disclosures of PHI regarding reports of (a) Child Abuse; (b) Abuse, Neglect or Domestic Violence of an Adult who is not an Elder Person or DisabledAdult; and (b) Abuse or Neglect of an Elder Person or Disabled Adult.

DEFINITIONS

The definitions of the following terms are presented here for convenience. These terms also appear in the Glossary. Additional defined terms noted below can be found at the noted sections of the Official Code of Georgia Annotated (OCGA).

"**Abuse of an Elder Person or Disabled Adult**" means the willful infliction of physical pain, physical injury, Sexual Abuse (as that term is defined in OCGA § 30-5-3), mental anguish, unreasonable confinement, or the willful deprivation of Essential Services (as that term is defined in OCGA § 30-5-3) to a Disabled Adult or Elder Person. [OCGA § 30-5-3].

"**Child**" means any person under 18 years of age. [OCGA § 19-7-5].

"**Child Abuse**" means:

(A) Physical injury or death inflicted upon a Child by a parent or caretaker thereof by other than accidental means; provided, however, that physical forms of discipline may be used as long as there is no physical injury to the Child;

(B) Neglect or exploitation of a Child by a parent or caretaker thereof;

(C) Sexual Abuse (as that term is defined in OCGA § 19-7-5) of a Child; or

(D) Sexual Exploitation (as that term is defined in OCGA § 19-7-5) of a Child.

However, no Child who in good faith is being treated solely by spiritual means through prayer in accordance with the tenets and practices of a recognized church or religious denomination by a duly accredited practitioner thereof shall, for that reason alone, be considered to be an "abused" Child. [OCGA § 19-7-5]

"**Disabled Adult**" means a person 18 years of age or older who is not a resident of a long-term care facility, but who:

(A) Is mentally or physically incapacitated;

(B) Has Alzheimer's disease, as defined in OCGA § 31-8-180; or

(C) Has dementia, as defined in OCGA § 16-5-100.

[OCGA § 30-5-3] NOTE: Additional specific rules apply to the reporting of abuse or neglect of residents in long-term care facilities. *See*, OCGA § 31-8-80, *et. seq*.

"**Elder Person**" means a person 65 years of age or older who is not a resident of a long-term care facility. [OCGA § 30-5-3] NOTE: Additional specific rules apply to the reporting of abuse or neglect of residents in long-term care facilities. *See*, OCGA § 31-8-80, *et. seq.*

"**Medical Facility**" includes, facility without being limited to, an ambulatory surgical treatment center as defined in subparagraph (C) of paragraph (4) of OCGA § 31-7-1 and a freestanding imaging center as defined in subparagraph (G) of paragraph (4) of OCGA § 31-7-1. [OCGA § 31-7-9].

"**Neglect of an Elder Person or Disabled Adult**" means the absence or omission of essential services to the degree that it harms or threatens with harm the physical or emotional health of a Disabled Adult or Elder Person. [OCGA § 30-5-3]

"**School**" means any public or private pre-kindergarten, elementary school, secondary school, technical school, vocational school, college, university, or institution of postsecondary education. [OCGA § 19-7-5]

POLICY

(A) Child Abuse

Requirements for the Use and Disclosure of PHI in Conjunction with Child Abuse Reports

As described below, Georgia law mandates that certain persons report Child Abuse to appropriate state authorities ("Mandatory Reporters"), and permits other persons to make such reports ("Permissive Reporters"). HIPAA permits PHI to be Disclosed in conjunction with

Mandatory or Permissive Reports of Child Abuse as follows:

(1) The Covered Component may Disclose PHI about a Child who may be a victim of Child Abuse to a or other government agency that is authorized by law Public Health Authority to receive reports of Child Abuse, if the Covered Component reasonably believes that a Child is the victim of Child Abuse.
(2) The Covered Component is not required to inform the Child or his/her personal representative that such a report has been or will be made.

Mandatory Reporters

Pursuant to Georgia law, it is **mandatory** for the following persons to make a report if they reasonably believe that a Child is the victim of Child Abuse:

(a) Physicians licensed to practice medicine, physician assistants, interns, or residents;
(b) Hospital or medical personnel;
(c) Dentists;
(d) Licensed psychologists and persons participating in internships to obtain licensing pursuant to OCGA Title 43, Chapter 39;
(e) Podiatrists;
(f) Registered professional nurses or licensed practical nurses licensed to OCGA Title 43, Chapter 26 or nurse's aides;
(g) Professional counselors, social workers, or marriage and family therapists licensed pursuant to OCGA Title 43, Chapter 10A;
(h) School teachers;
(i) School administrators;
(j) School guidance counselors, visiting teachers, school social workers, or school psychologists certified pursuant to OCGA Title 20, Chapter 2;
(k) Child Welfare Agency personnel, as that term is defined pursuant to OCGA § 49-5-12;
(l) Child counseling personnel
(m) Child service organization personnel;
(n) Law enforcement personnel; or
(o) Reproductive health care facility or pregnancy resource center personnel and volunteers.

Permissive Reporters

Under Georgia law, any person other than a Mandatory Reporter who has reasonable cause to believe that a Child is a victim of Child Abuse **may** report such Child Abuse.

To Whom Reports of Child Abuse Must be Made

Under Georgia law, a report of Child Abuse must be made to:

(a) A Child Welfare Agency providing protective services, as designated by the Department of Health and Human Services; or, in the absence of such an

agency; or

(b) The appropriate police authority, or

(c) The district attorney's office.

PROCESS

If a workforce member of a Covered Component who is a Mandatory Reporter has reasonable cause to believe that a Child has been a victim of Child Abuse, he/she shall immediately (but in no case more than 24 hours from the time there is reasonable cause to believe a Child has been a victim of Child Abuse) make an oral report to the appropriate Child Welfare Agency, the police or the district attorney's office, as described above. Prior to making any report, the workforce member shall contact the Emory University Office of the General Counsel for guidance in verifying the identity and authority of the official/agency to whom/which the PHI is to be Disclosed. The oral report may be followed by a written report, if requested by the Child Welfare Agency or government authority. Such report must contain the following information:

(1) Name and address of the Child and the Child's parents or caretakers, if known;
(2) Child's age;
(3) Nature and extent of Child's injuries, including evidence of previous injuries;
(4) Any other information that might be helpful in establishing the cause of the injuries and the identity of the perpetrator.

Photographs of the Child's injuries to be used as documentation in support of allegations may be taken without the permission of the Child's parent or guardian and must be made available as soon as possible to the Child Welfare agency and appropriate police authority.

REFERENCE: OCGA §19-7-5

(B) Abuse, Neglect or Domestic Violence Concerning Adults who are not Elder Persons or Disabled Persons

Georgia Law Regarding Reporting of Abuse, Neglect or Domestic Violence with Respect to Adults who are not Elder Persons or Disabled Persons

Georgia law does not have a statute that specifically addresses the reporting of abuse, neglect or domestic violence with respect to adults who are not Elder Persons or Disabled Persons. Georgia, however, does have a law (OCGA § 31-7-9) that requires the reporting by any of the persons listed below of any physical injuries inflicted upon a patient by other than accidental means (hereafter "Non-Accidental Injuries"):

- Any physician;
- Any registered nurse employed by a Medical Facility;
- Any security personnel employed by a Medical Facility;
- Any personnel with patient treatment or care responsibilities employed by a Medical Facility

HIPAA Requirements

HIPAA permits the Use and Disclosure of PHI by a Covered Component in connection with the reporting of abuse, neglect or domestic violence, including the mandatory reporting of Non-Accidental Injuries under OCGA § 31-7-9 as described above, subject to the following limitations:

- The Covered Component reasonably believes that an Individual is a victim of abuse, neglect or domestic violence; **and**
- The Individual agrees to the Disclosure; **OR**
- The Disclosure is required by law and is limited to those items that the law permits to be Disclosed; or
- The Disclosure is authorized by law and the Covered Component believes that the Disclosure is necessary to prevent serious harm to the Individual or other potential victims; or
- The Disclosure is authorized by law; the Individual is unable to agree to the Disclosure because he/she is incapacitated; a law enforcement or public official (e.g., social services agent) that is authorized to receive the report represents that the PHI to be Disclosed won't be used against the Individual; and the Disclosure is necessary for an immediate enforcement activity that would be materially and adversely affected if the law enforcement or public officials had to wait until the Individual was in condition to be able to agree to the Disclosure.
- AND in all of the foregoing cases, the Covered Component promptly informs the Individual, verbally (with documentation) or in writing, that a report has been, or will be, made EXCEPT in the following two circumstances:

  (a) Exception 1: The Covered Component does not have to inform the Individual of the report, if, in the exercise of its professional judgment, it believes that informing the Individual of the report would place the Individual at risk of serious harm; or

  (b) Exception 2: The Covered Component does not have to inform the personal representative of the Individual of the report if the Emory Covered Component (i) reasonably believes that the personal representative is responsible for the abuse, neglect or domestic violence and (ii) the Emory Covered Component determines, in the exercise of its professional judgment, that informing the personal representative would not be in the best interest of the Individual.

PROCEDURE

Report Made Pursuant to OCGA §31-7-9

For a report made under OCGA §31-7-9, the Disclosure of PHI in conjunction with that report would be considered a Disclosure that is required by law under HIPAA. The reporter shall ensure that only those items required to be reported under OCGA §31-7-9 are Disclosed. The reporter first shall make an oral report to the person in charge of the Medical Facility at which he/she works and saw the patient. If the reporter does not know the identity of the person in charge of the Medical Facility, he/she shall contact the Emory University Office of General Counsel for assistance in determining to whom the report should be made. The oral report shall be followed by a written report, if requested by the person in charge of the Medical Facility. The person in charge of the Medical Facility, or his/her designee, shall then notify the

local law enforcement agency having primary jurisdiction in the area in which the medical facility is located. The person in charge of the Medical Facility shall verify with the Emory University Office of the General Counsel the identity of the local law enforcement agency to which the report should be made. The reporter shall provide the law enforcement agency with the following information: name and address of patient; nature and extent of patient's injuries; any information reporter believes might be helpful in establishing the cause of the injuries and the identity of the perpetrator. At the time of the report, or promptly thereafter, the person in charge of the Medical Facility, or his/her designee, shall notify the Individual who is the subject of the report that the report will be/has been made, unless either Exception 1 or Exception 2 under the HIPAA Requirements noted above applies.

Report not made Pursuant to OCGA § 31-7-9

For a report of abuse, neglect or domestic violence with respect to an adult who is not an Elder Person or Disabled Adult and that does not fall within the scope of OCGA **§** 31-7-9, the Covered Component must have the Individual's agreement to the Disclosure pursuant to HIPAA before the Disclosure is made. The agreement should specify the governmental protective agency or law enforcement authority to which the report will be made. This agreement should either be in writing and signed by the Individual, or if verbal, then it should be documented in the appropriate record.

(C) Abuse or Neglect of Elder Persons of Disabled Adults

Georgia Law Regarding Reporting of Abuse, Neglect or Domestic Violence with Elder Persons and Disabled Persons

In accordance with OCGA § 30-5-4, a mandated reporter who is part of the workforce of a Covered Component of the Emory Hybrid Covered Entity **must** make a report regarding a "Disabled Adult" or "Elder Person" (as those terms are defined in OCGA § 30-5-3) when the Mandated Reporter has reasonable cause to believe that the Disabled Adult or Elder Person has been the victim of abuse, other than by accidental means, or has been neglected or exploited.

Mandated Reporters

The following persons are required to report, or cause reports to be made in accordance with OCGA § 30-5-4 when such persons have reasonable cause to believe that a Disabled Adult or Elder Person has been the victim of abuse other than by accidental means, or has been neglected or exploited:

- Physical Therapists and occupational therapists
- Day-care personnel
- Coroners and Medical Examiners
- Emergency medical service personnel (as defined in OCGA § 31-11-49) and any person who has been certified as an emergency medical technician, cardiac technician, paramedic, or first responder pursuant to OCGA Title 31, Chapt. 11
- Employees of a public or private agency engaged in professional health related services to elder persons or disabled adults
- Clergy members
- Physicians, hospital, or medical personnel, including physician assistants, interns or residents
- Dentists

●Psychologists and interns
●Podiatrists
●Registered professional nurses, licensed practical nurses or nurses' aides
●Professional counselors, social workers, marriage and family therapists;
●School (as that term is defined at OCGA §19-7-5) teachers and School administrators
●School counselors, visiting teachers, School social workers or School psychologists certified pursuant to OCGA Title 20, Chapt. 2
●Child Welfare Agency personnel, as such agency is defined at OCGA §49-5-12
●Child-counseling personnel
●Child service organization personnel
●Law enforcement personnel
●Reproductive health care facility or pregnancy resource center personnel and volunteers

HIPAA Requirements

HIPAA permits the Use and Disclosure of PHI by a Covered Component in connection with the reporting of abuse, neglect or domestic violence, including the mandatory reporting of abuse, other than by accidental means, exploitation or neglect of an Elder Person or Disabled Adult under OCGA § 30-50-3 as described above, subject to the following limitations:

● The Covered Component reasonably believes that an Individual is a victim of abuse, neglect or domestic violence; **and**

● The Individual agrees to the Disclosure; OR

● The Disclosure is required by law and is limited to those items that the law permits to be Disclosed; or

● The Disclosure is authorized by law and the Covered Component believes that the Disclosure is necessary to prevent serious harm to the Individual or other potential victims; or

●The Disclosure is authorized by law; the Individual is unable to agree to Disclosure because he/she is incapacitated; a law enforcement or public official (e.g., social services agent) that is authorized to receive the report represents that the PHI to be Disclosed won't be used against the Individual; and the Disclosure is necessary for an immediate enforcement activity that would be materially and adversely affected if the law enforcement or public officials had to wait until the Individual was in condition to be able to agree to the Disclosure.

●AND in all of the foregoing cases, the Covered Component promptly informs the Individual, verbally (with documentation) or in writing, that a report has been, or will be, made EXCEPT in the following two circumstances:

(a) Exception 1: The Covered Component does not have to inform the Individual of the report, if, in the exercise of its professional judgment, it believes that informing the Individual of the report would place the Individual at risk of serious harm; or

(b) Exception 2: The Covered Component does not have to inform the personal representative of the Individual of the report if the Covered Component (i) reasonably believes that the personal representative is responsible for the

abuse, neglect or domestic violence and (ii) the Covered Component determines, in the exercise of its professional judgment, that informing the personal representative would not be in the best interest of the Individual.

PROCEDURE

Reports of Abuse or Neglect of Disabled Adults or Elder Persons Made Pursuant to OCGA § 30-5-4

For a report made under OCGA § 30-5-4, the Disclosure of PHI in conjunction with that report would be considered a Disclosure that is required by law under HIPAA. The Mandated Reporter shall ensure that only those items required to be reported under OCGA § 30-5-4 are Disclosed in the report. The report may be oral or written and shall include the name and address of the Disabled Adult or Elder Person; name and address of the Disabled Adult's or Elder Person's caretaker; age of Disabled Adult or Elder Person; the nature and extent of the Disabled Adult's or Elder Person's injury or condition result from the abuse, exploitation or neglect; and any other pertinent information. If the Mandated Reporter is a member of the staff of a hospital or similar facility, then the report shall be made to the person in charge of the facility. In such case, the Mandated Reporter shall contact the Emory University Office of the General Counsel to verify the identity of the person in charge of the facility. The person in charge of the facility, or any other Mandated Reporter, shall make a report to the following persons/entities per OCGA § 30-5-4:

(a) An adult protection agency providing protective services, AND to the appropriate law enforcement agencies; or

(b) A prosecuting attorney, if an adult protection agency is not available, AND to the appropriate law enforcement agencies.

At the time of the report, or promptly thereafter, the reporter shall notify the Individual who is the subject of the report that the report will be/has been made, unless either Exception 1 or Exception 2 under the HIPAA Requirements noted above applies.

Reports of Abuse or Neglect of Disabled Adults or Elder Persons not Pursuant to OCGA § 30-5-4

For a report of abuse, neglect or domestic violence with respect to an adult who is an Elder Person or Disabled Adult that does not fall within the scope of OCGA § 30-5-4, the Covered Component must have the Individual's agreement to the Disclosure pursuant to HIPAA before the Disclosure is made. The agreement should specify the adult protective agency or prosecuting attorney and law enforcement authority to which the report will be made. This agreement should either be in writing and signed by the Individual, or if verbal, then it should be documented in the appropriate record.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule - The Emory Covered Component should only Disclose the minimum necessary type and amount of PHI that is required to achieve the purpose of the Disclosure. However, if the Disclosure is being made to a public official, then the Covered Component may rely on the representations of the public official that the

amount of information being requested by the official is the minimum necessary type and amount of PHI.

Accounting Rule - Unless the Individual has authorized the Disclosure, Disclosures made pursuant to this policy are subject to a request for an accounting by an Individual. Accordingly, the Emory Covered Component that makes the Disclosure should document the Disclosure and maintain this documentation for six years after the Disclosure.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCES: Listed within policy and: 45 C.F.R. §§164.512(a) & (c); OCGA §§19-7-5, 30-5-4 & 31-7-9
RESOURCES:
DHHS OCR FAQ: *My State law authorizes health care providers to report suspected child abuse to the State Department of Health and Social Services. Does the HIPAA Privacy Rule preempt this State law?* at
www.hhs.gov/ocr/privacy/hipaa/faq/preemption_of_state_law/406.html

DHHS OCR HIPAA Privacy Guidance, *Disclosures for Public Health Activities*, December 3, 2002, revised April 3, 2003 at
www.hhs.gov/ocr/privacy/hipaa/understanding/special/publichealth/publichealth.pdf

DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

D.8. HIPAA POLICY REGARDING DISCLOSURE AND USE OF PHI FOR HEALTH OVERSIGHT ACTIVITIES

PURPOSE OF POLICY

The purpose of this policy is to provide standards governing a Covered Component's Use and Disclosure of an Individual's PHI tto government agencies that are responsible for providing oversight of healthcare activities (i.e., Health Oversight Agencies)..

DEFINITION

The definition of the following term is presented here for convenience. This term also appears in the Glossary.

"Health Oversight Agency" means an agency or authority of the United States, a U.S. state/territory or political subdivision thereof, an Indian tribe, or a person or entity acting under a grant of authority from, or contract with, such agency or authority that is authorized by law to oversee the health care system (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. The term includes employees, agents or contractors of the agency/authority or of the persons/entities to whom it has granted authority. [45 CFR § 164.501].

POLICY

Disclosure for Health Oversight Activities

A Covered Component of the Emory University Hybrid Covered Entity may Disclose PHI to a Health Oversight Agency for health oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil administrative or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

- The health care system;
- Government benefit programs for which Health Information is relevant to beneficiary eligibility
- Entities subject to government regulatory programs for which Health Information is necessary for determining compliance with program standards; or
- Entities subject to civil rights laws for which Health Information is necessary for determining compliance.

Activities that Don't Constitute Health Oversight Activities

A health oversight activity does not include an investigation or other activity in which the Individual is the subject of the investigation or other activity, and such investigation or other activity does not arise out of and is not directly related to:

(a) The receipt of Health Care.
(b) A claim for public benefits related to health.
(c) Qualification for or receipt of public services when the Individual's health is integral to the claim for public benefits or services.

Joint Activities

A joint activity that consists of a health oversight activity that is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits that is not related to health, does not constitute a health oversight activity.

PROCEDURE

The Emory Covered Component shall verify the identity and the authority of the Health Oversight Agency prior to making any Disclosure of PHI to a Health Care Oversight Agency.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule: The minimum necessary PHI that is necessary to achieve the purpose of the Disclosure should be Disclosed; provided, however, that when the Disclosure is being made to a public official, then the Covered Component may rely on representations of the public official that the amount of PHI requested is the minimum necessary type and amount of PHI.

Accounting: Disclosures made pursuant to these policies are subject to a request for an accounting by the Individual. Accordingly, the Covered Component that makes the Disclosure should document the Disclosure and maintain the documentation for six years after the Disclosure.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCE: 45 CFR 164.512(d)
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

D.9. HIPAA POLICY REGARDING USE AND DISCLOSURE OF PHI TO AVERT A SERIOUS THREAT TO HEALTH OR SAFETY

PURPOSE

The purpose of this Policy is to set forth the circumstances under which a Covered Component of the Emory University Hybrid Covered Entity may Use and Disclose PHI concerning an Individual in order to prevent or reduce a serious and immediate threat to the health or safety of a person or the public.

POLICY

Permitted Disclosures:

Prevent or Lessen a Serious Threat to Health or Safety of Person or Public

If the Covered Component in good faith believes that the Use or Disclosure of PHI (a) is necessary to prevent or lessen a serious and imminent threat to the health or safety or a person or the public; and (b) is consistent with applicable law (including, but not limited to, the laws of the State of Georgia) and standards of ethical conduct, then the Covered Component may make a Disclosure of such PHI to a person or persons (including the target[s] of the threat) who is/are reasonably able to prevent or lessen the threat.

Disclosure to Law Enforcement Authorities to Identify or Apprehend an Individual

If the Covered Component in good faith believes that the Use or Disclosure of PHI is necessary for law enforcement authorities to identify or apprehend an Individual as described below:

a. Because of a statement by an Individual admitting that he/she participated in a violent crime that the Covered Component reasonably believes may have caused serious physical harm to the victim; provided, however, that in such event only the Individual's statement and the following PHI may be disclosed: name and address; date and place of birth; Social Security Number; ABO blood type and rh factor; type or injury; date and time or treatment; date and time of death, if applicable; and a description of distinguishing physical characteristics including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars and tattoos.

OR

b. Where it appears from all circumstances that the Individual has escaped from a correctional institution or from lawful custody.

Provided, however, that the Covered Component may not Disclose PHI to law enforcement authorities to identify or apprehend an Individual if the PHI that is to be Disclosed was learned (i) in the course of Treatment to affect the propensity to commit the criminal conduct that is the basis of the Disclosure, or through counseling or therapy; or (ii) through a request by the

Individual to initiate or be referred for treatment, counseling or therapy to treat such propensity. (NOTE: See *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*.)

3. The Covered Component will be presumed to have acted in good faith in making a Disclosure under this Policy with regard to any prerequisite belief that it is required to have before it makes the Disclosure, if the belief is based on the Covered Component's actual knowledge, or in reliance on a credible representation by a person who has apparent knowledge or authority.

PROCEDURE

Prior to making any Disclosure pursuant to this policy, the Covered Component shall contact the Emory University Office of the General Counsel for guidance as to any limitations under State law concerning the Disclosure, including any limitation regarding the type or amount of information that may be Disclosed. Additionally, the Covered Component will verify the identity and authority of any law enforcement official to whom a Disclosure is made pursuant to this policy in accordance with the *Policy C.6, Verification Requirements for Disclosure of PHI*. For any Disclosure made pursuant to this policy, the Covered Component will document the circumstances supporting the Disclosure.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule: In cases in which the specific information that may be Disclosed under a provision of this policy is set forth, then only that information may be Disclosed. In all other cases, only the minimum necessary information requried to accomplish the prupsoe of the Disclosure will be Disclosed.

Accounting Rule: The Covered Component must keep records of any Disclosure made pursuant to this Policy, and an accounting of such Disclosures shall be made to the Individual upon written requrest for an accounting.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy*

Notes and Mental Health Information; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCES: 45 C.F.R. §164.512(j)
DATE OF POLICY: April 14, 2003.
REVISED: September 1, 2016

D.10. HIPAA POLICY REGARDING USE AND DISCLOSURE OF PHI FOR SPECIAL GOVERNMENT FUNCTIONS

PURPOSE OF POLICY

The purpose of this Policy is to set forth the standards per which an Individual's PHI may be Disclosed to certain governmental personnel and agencies in connection with specialized government functions.

POLICY

This policy covers three types of specialized government functions, each of which is individually discussed below. All of the Disclosures covered under this policy make reference to other notices, regulations or laws that impact the circumstances in which these Disclosures should be made. Accordingly, before making any of the Disclosures described in this Policy, **PLEASE CONTACT THE EMORY UNIVERSITY OFFICE OF THE GENERAL COUNSEL** for a review of circumstances and applicable laws to determine whether the Disclosure is appropriate.

A. Military and Veterans Activities

1. Armed Forces Personnel:

A Covered Component of the Emory Hybrid Covered Entity may Disclose PHI of Individuals who are members of the armed forces to military authorities for purposes that appropriate military command authorities have deemed necessary to assure proper execution of the military mission IF the military authority has taken the following action prior to seeking the information:

(a) Published a notice in the Federal Register that sets forth (a) the name of the appropriate military command authorities; and (b) the purposes for which the PHI may be used or disclosed.

2. Foreign Military Personnel:

A Covered Component may Use and Disclose the PHI of Individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which Uses and Disclosures are permitted for U.S. Armed Forces personnel under a notice published the Federal Register as described in Section A.1(a) above.

B. Security and Intelligence Activities

1. National Security and Intelligence Activities:

A Covered Component may Disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence and other national security activities authorized by the National Security Act (50 U.S.C. § 401, et. seq.) and implementing authority (e.g., Executive Order 12333).

2. Protective Services for the President and Others:

A Covered Component may Disclose an Individual's PHI to authorized federal officials for the provision of protective services to the President of the United States or other persons authorized by 18 U.S.C. § 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. § 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. §§ 871 and 879.

3. Correctional Institutions and Other Law Enforcement Custodial Situations:

A Covered Component may Disclose an Individual's PHI to a correctional institution or a law enforcement official that has lawful custody of an inmate or other Individual if the correctional institution or law enforcement official represents that such PHI is necessary for: (a) the provision of Health Care to the Individual; (b) the health and safety of such Individual or another inmate; (c) the health and safety of the officers or employees, of or others at the correctional institution; (d) the health and safety of such Individual and officers or other persons responsible for the transporting of inmates or their transfer from one institution facility or setting to another; (e) the administration and maintenance of safety, security and good order of the correctional institution. However, under the foregoing provision, PHI may not be Disclosed regarding Individuals who are released on parole, probation, supervised release or who are otherwise no longer in lawful custody

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule–The Covered Component should only disclose the minimum necessary type and amount of PHI that is required to accomplish the purpose of the Disclosure. The Covered Component may rely on the representations of the governmental official as establishing the minimum necessary PHI to be Disclosed.

Accounting Rule–Unless the Individual specifically authorizes a particular Disclosure or unless the Disclosure is for Treatment, Payment or Health Care Operations purposes, the Covered Component must document any Disclosures of PHI that are made. The Covered Component must keep this documentation for six years after the Disclosure.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following

policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCES: 45 CFR §164.512(k).
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

D.11. HIPAA POLICY REGARDING USE AND DISCLOSURE OF PHI FOR WORKERS COMPENSATION PURPOSES

PURPOSE OF POLICY
The purpose of this policy is to set forth the standards per which an Individual's PHI may be Disclosed by a Covered Component of the Emory University Hybrid Covered Entity for purposes of complying with laws concerning workers' compensation.

POLICY
A Covered Component may Disclose an Individual's PHI without his/her Authorization to workers' compensation and similar programs that are established by law to provide benefits for work-related injuries or illnesses without regard to fault; provided, however, that the extent of the Disclosure is limited to only the type and amount of PHI that must be Disclosed in order to comply with the applicable laws.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule–The Covered Component should only Disclose the type and amount of PHI that is required to be Disclosed per the applicable workers' compensation laws.

Accounting Rule–Unless the Individual specifically authorizes a particular Disclosure or unless the Disclosure is for the Covered Component's Treatment, Payment or Health Care Operations purposes, the Emory Covered Component must document any Disclosures of PHI that are made and the Individual may request an accounting of these Disclosures. The Emory Covered Component must keep this documentation for six years after the Disclosure.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law

enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCE: 45 CFR §164.512(l)
DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

D.12. HIPAA POLICY REGARDING DISCLOSURES OF PHI FOR JUDICIAL AND ADMINISTRATIVE PROCEEDINGS

PURPOSE OF POLICY

The purpose of this policy is to set forth the requirements that must be met under HIPAA and the laws of the State of Georgia, as well as the procedure that must be followed, in order to Disclose PHI in relation to a judicial or administrative proceeding.

DEFINITION

The following definition applies to a term used in this policy. This definition also appears in the Glossary and is provided here for convenience:

"**Confidential Raw Research Data**" means medical information, interview responses, reports, statements, memoranda, or other data relating to the condition, treatment, or characteristics of any person which are gathered by or provided to a researcher:

(c) In support of a Research study approved by an appropriate Research oversight committee (e.g., IRB) of a hospital, health care facility, or educational institution; and
(d) With the objective to develop, study or report aggregate or anonymous information not intended to be used in any way in which the identity of an Individual is material to the results.

The term Confidential Raw Research Data does not include published compliations of the raw Research data created by the researcher or the researcher's published summaries, finding, analyses, or conclusions related to the Research study.

POLICY

A Covered Component of the Emory University Hybrid Covered Entity may Use or Disclose PHI to the extent that such Use or Disclosure is required by law and complies with and is

limited to the relevant requirement of such law. In addition to following the requirements of this policy in making such a Disclosure, the Covered Component also must adhere to the requirements of any of the following policies that are applicable depending on the type of Disclosure to be made: *Policy D.13, HIPAA Policy Regarding Disclosure of PHI for Law Enforcement Purposes* and/or *Policy D.7, HIPAA Policy Regarding Use and Disclosure of PHI in Connection with Reporting of Child Abuse; Abuse, neglect or Domestic Violence Concering Adults who are not Elder Persons or Disabled Adults; and Abuse or Neglect of an Elder Person or Disabled Adult*.

PROCEDURE

A. Permitted Disclosures:

Generally, a Covered Component may Disclose PHI in connection with a judicial or administrative proceeding under circumstances set forth below; **BUT** each situation must be specifically evaluated with respect to the type of PHI requested and any applicable state and federal laws, including, but not limited to state laws regarding appropriate notice to the person whose PHI is requested. Accordingly, if a Covered Component receives any court or administrative order, subpoena, discovery request, or any other legal process seeking the Disclosure of PHI, it must **IMMEDIATELY CONTACT THE EMORY UNIVERSTIY OFFICE OF THE GENERAL COUNSEL** for advice as to how to properly comply **BEFORE** releasing any PHI.

(1) Court/Administrative Orders

A Covered Component may Disclose PHI in response to a court order or the order of an administrative tribunal, provided that only the PHI authorized by the order is Disclosed and provided any requirements of applicable state law are met, including, any requirements regarding notice and opportunity to object. The Office of the General Counsel must be contacted prior to any such Disclosure.

(2) Subpoena, Discovery Request, Lawful Process

A Covered Component may Disclose PHI in response to a subpoena, discovery request or other lawful process that is not accompanied by an order of a court or administrative tribunal if:

a. The Covered Component receives satisfactory assurances (see below "B. Satisfactory Assurances of Notification Attempts") from the party seeking the information that he/she has made reasonable efforts to ensure that the Individual who is the subject of the PHI has been given notice of the request; OR

b. The Emory Covered Component receives assurance (see below "C. Satisfactory Assurances of Attempts to Obtain a Qualified Protective Order") from the party seeking the information that he/she has made reasonable efforts to secure a qualified protective order that meets the following requirements:

(i) The protective order is in the form of an order of a court, administrative tribunal, or a stipulation by the parties to the proceeding;

(ii) The protective order prohibits the parties from Using or Disclosing the PHI for any purpose other than the litigation or proceeding for which the PHI was requested;

(iii) The protective order requires that the PHI (and all copies thereof) be returned to the Covered Component or destroyed at the end of the proceeding; OR

c. The Covered Component itself makes reasonable efforts to seek a protective order or to provide notice to the Individual that meets the specifications set forth in this policy; AND

d. All applicable state law requirements regarding Disclosure pursuant to a subpoena, discovery request and/or lawful process are met, including any requirements regarding notice to the person whose PHI is being sought. In this respect, the Office of the General Counsel must be contacted prior to any Disclosure.

The assurances described below are considered to be satisfactory assurances under HIPAA with regard to a requesting party's attempts to notify the person who is the subject of the PHI requested pursuant to a subpoena, discovery request, etc.; provided, however, that any assurance requirements set forth by state law also must be met. Accordingly, the Covered Component MUST contact the Emory University Office of the General Counsel for advice as to what state law assurances, or other requirements, apply.

(1) Assurances

The Emory Covered Component receives from the requesting party a written statement and accompanying documentation that show that:

a.The party made a good faith attempt to provide written notice to the Individual, or to the Individual's last known address if his/her present location is unknown; and

b.The notice included sufficient information about the proceeding in which the PHI was requested to permit the Individual to file an objection with the court or tribunal; the time for objections to be filed has passed; and either no objections were filed or, if an objection was filed, the court or tribunal has ruled on it and the ruling permits the Disclosure that is being requested; or

c.The Emory Covered Component made reasonable efforts to provide notice to the Individual that meets the above listed specifications.

C. Satisfactory Assurances of Attempts to Obtain a Qualified Protective Order

The following assurances will be considered to be satisfactory assurances under HIPAA with regard to a requesting party's attempts to obtain a qualified protective order; provided, however, that any assurance requirements set forth by state law also must be met.

Accordingly, the Covered Component MUST contact the Emory University Office of the General Counsel for advice as to what state law assurances, or other requirements, apply.

(1) Assurances

The Emory Covered Component receives from the party requesting the PHI a written statement and accompanying documentation demonstrating that:

a. The parties to the proceeding have agreed to a qualified protective order and have presented it to the court or administrative tribunal; or

B. The party requesting the PHI has requested a qualified protective order from the court or administrative tribunal.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES
Only the PHI required per court order, subpoena, discovery or other legal process, as constrained by any qualified protective order, may be Disclosed. PHI Disclosed pursuant to this policy is subject to the Accounting Rule, unless an Individual who is the subject of the PHI has provided Authorization for the Disclosure.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI
In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

D.13. HIPAA POLICY REGARDING DISCLOSURES OF PHI FOR LAW ENFORCEMENT PURPOSES

PURPOSE OF POLICY

The purpose of this policy is to detail those situations in which the Emory Covered Component may make a Disclosure of the Protected Health Information (PHI) of an Individual for law enforcement purposes and the requirements that must be met before such Disclosures may be made.

POLICY

A Covered Component of the Emory University Hybrid Covered Entity may Use or Disclose PHI to the extent that such Use or Disclosure is required by law and complies with and is limited to the relevant requirements of such law. In order to make such a Use or Disclosure as is required by law, the Covered Component must make the Use or Disclosure pursuant to and in conformance with this policy and the following policies, as applicable:

- *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; and/or
- *Policy D.7, HIPAA Policy Regarding Use and Disclosure of PHI in Connection with Reporting of Child Abuse; Abuse, Neglect or Domestic Violence Concerning Adults who are not Elder Persons or Disabled Adults; and Abuse or Neglect of an Elder Person or Disabled Adult.*

Additionally, any Disclosure must be consistent with any laws of the state of Georgia regarding the privileged nature of some or all of the information to be Disclosed (e.g., Psychotherapy Notes), as well as with any Georgia laws governing the Disclosure of medical information in the context of criminal investigations and proceedings against an Individual; and any state laws laws regarding appropriate notice to the person whose PHI is requested. Accordingly, the Covered Component must **CONTACT THE EMORY UNIVERSITY OFFICE OF THE GENERAL COUNSEL** for advice and approval of the Disclosure as indicated below.

Disclosures to Law Enforcement Officials that do Not Require Authorization

The Emory Covered Component may make the following disclosures of PHI to law enforcement officials without obtaining the Authorization of the Individual:

A. Disclosures Made Pursuant to Legal Process and as Otherwise Required by Law

1. Specific Laws Requiring Disclosures: If there is a specific law that requires the Disclosure of PHI to a law enforcement official, such as the reporting of certain types of wounds or injuries, then the Covered Component may make Disclosure of this PHI without the Individual's Authorization; provided, however, that Disclosure of PHI with respect to reports of Child Abuse, or of abuse, neglect or domestic violence concerning adults are governed by the *Policy D.7, HIPAA Policy Regarding Use and Disclosure of PHI in Connection with Reporting of Child Abuse; Abuse, Neglect or Domestic Violence Concerning Adults who are not Elder Persons or Disabled Adults; and Abuse or Neglect of an Elder Person or Disabled Adult*.

2. Disclosures Made Pursuant to Legal Process: The Covered Component may Disclose PHI in response to a court order, court-ordered warrant, subpoena, or summons issued by a judicial officer; a grand jury subpoena; or an administrative request, such as an administrative subpoena or summons, a civil or authorized investigative demand or similar process authorized under law if:

a. The information sought is relevant and material to a legitimate law enforcement inquiry;
b. The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is being sought; and
c. De-identified information could not reasonably be used.
d. The Disclosure is in accordance with any requirements of applicable state law.

Any Disclosure made pursuant to legal process is also subject to the *Policy D.12, HIPAA Policy Regarding Uses and Disclosures for Judicial and Administrative Proceedings*. **The Emory University Office of the General Counsel MUST be contacted prior to making any Disclosure pursuant to legal process.**

B. Disclosures Not Required by Law of Limited Information for Identification and Location Purposes

1 Disclosure Not Required by Law: If a Disclosure of PHI is not required by law, but a law enforcement official has requested the Disclosure of the PHI **solely for the purpose of identifying or locating** a suspect, fugitive, material witness or missing person, then the Covered Component may Disclose only the information listed below: [Note: The Covered Component may not Disclose for identification or location purposes any PHI related to an Individual's DNA, DNA analysis, dental records or typing, samples or analysis of body fluids or tissue.]

a. Name and address;
b. Date and place of birth;
c. Social security number;
d. Type of injury;
e. ABO blood typeand rh factor;
f. Date and time of Treatment;
g. Date and time of death, if applicable; and
h.A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars and tattoos.

Additionally, the Disclosure must be in accordance with the requirements of any applicable state law. In this respect, the Covered Component MUST contact the Emory University Office of the General Counsel prior to making any Disclosure of PHI for the purpose of indentifying or locating a suspect, fugitive, or material witness. Whenever possible, the Emory University Office of the General Counsel also should be contacted prior to making any Disclosure of PHI for the purpose of identifying or locating a missing person.

C. Disclosures not Required by Law Regarding Victims of a Crime:

1. Disclosure of PHI Regarding Victim of a Crime: If a Disclosure is not required by a particular law, but a law enforcement official has requested Disclosure of PHI about an Individual who is thought to be a victim of a crime, other than Child Abuse, or abuse, neglect or domestic violence concerning adults who are not Elder Persons or Disabled Adults, or abuse or neglect of an Elder Person or Disabled Adult (see *Policy D.7, HIPAA Policy Regarding Use and Disclosure of PHI in Connection with Reporting of Child Abuse; Abuse, Neglect or Domestic*

Violence Concerning Adults who are not Elder Persons or Disabled Adults; and Abuse or Neglect of an Elder Person or Disabled Adult), then the Covered Component may make the requested Disclosure if:

a.The Individual agrees to the Disclosure; or

b.The Covered Component is unable to obtain the Individual's agreement because the Individual is incapacitated or because of other emergency circumstances; and

i.The law enforcement official requesting the Disclosure represents that the information is needed to determine whether there has been a violation of law by a person other than the victim, and the information requested is not intended to be used against the victim; and

ii.The law enforcement official represents that immediate law enforcement activities that depend upon the Disclosure would be materially and adversely affected by waiting until the Individual is able to agree; and

iii.The Emory Covered Component, in the exercise of its professional judgment, determines that the Disclosure is in the best interest of the Individual.

The Covered Component MUST contact the Emory University Office of the General Counsel prior to the Disclosure of PHI to law enforcement officials regarding the victim of a crime if the Individual who is the subject of the PHI does not agree to the Disclosure.

D. Disclosures Regarding Decedents

1. Disclosure Regarding Suspicious Death: If a Covered Component has a suspicion that an Individual's death may have resulted from criminal conduct, then the Covered Component may initiate disclosure of PHI about the Individual who has died to a law enforcement official for the purpose of alerting law enforcement to this suspicion. Any request for PHI by a law enforcement official pursuant to legal process related to an Individual's death is subject to Subsections A and B of this Policy, and **the Covered Component MUST contact the Emory University Office of the General Counsel prior to making any Disclosure of PHI pursuant to legal process.**

E. Disclosure Regarding Crime on Premises

A Covered Component may initiate Disclosure to a law enforcement official of PHI that the Covered Component believes in good faith constitutes evidence of criminal conduct that occurred on the Covered Component's premises. Any request for PHI by a law enforcement official pursuant to legal process related to criminal conduct that occurred on the Covered Component's premises is subject to Subsections A and B of this Policy, and the **Covered Component must contact the Emory University Office of the General Counsel prior to making any Disclosure of PHI pursuant to legal process.**

.

F. Disclosures Regarding the Reporting of Crime in Emergencies

1.If a Health Care Provider who is a part of the Covered Component provides emergency Health Care in response to a medical emergency, that Health Care Provider may initiate Disclosure of PHI regarding the medical emergency to law enforcement officials if the Disclosure is necessary to alert law enforcement to:

a.The commission and nature of a crime;
b.The location of such crime or of the victim(s) of the crime; and
c.The identity, description and location of the perpetrator of the crime.
2.Exceptions:

a.This type of Disclosure may not be made with regard to an emergency that occurs on the premises of the Emory Covered Component, but Section E, "Disclosure Regarding Crime on the Premises" may apply in such a situation.
b.This type of Disclosure may not be made with regard to emergency medical care given to an Individual who the Covered Component believes requires this care as a result of abuse, neglect or domestic violence, and in such a case the *Policy D.7, HIPAA Policy Regarding Use and Disclosure of PHI in Connection with Reporting of Child Abuse; Abuse, Neglect or Domestic Violence Concerning Adults who are not Elder Persons or Disabled Adults; and Abuse or Neglect of an Elder Person or Disabled Adult* will apply.

Any request for PHI by a law enforcement official pursuant to legal process related to a medical emergency is subject to Subsections A and B of this policy as well as *Policy D.12, HIPAA Policy Regarding Uses and Disclosures for Judicial and Administrative Proceedings*. **The Covered Component MUST contact the Emory University Office of the General Counsel prior to making any Disclosure of PHI pursuant to legal process.**

PROCEDURE

The Emory Covered Component shall verify the identity of any law enforcement official to whom a permitted disclosure is made pursuant to this policy in accordance with the "Emory University HIPAA Policy Regarding Verification." In addition, as indicated under each type of Disclosure described above, the Covered Component must contact the Emory University Office of the General Counsel for guidance prior to making the Disclosure. Finally, if the Disclosure is made pursuant to legal process, *Policy D.12, HIPAA Policy Regarding Uses and Disclosures for Judicial and Administrative Proceedings* also shall be followed.

APPLICABILITY OF THE MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule: If the Covered Component is permitted to make a Disclosure of PHI in one of the situations described above, the Covered Component will Disclose only the information specified above for that situation. If no specific information is specified for a particular situation, then the Covered Component shall Disclose only the minimum necessary PHI to accomplish the purpose of the Disclosure.

Accounting Rule: The Covered Component shall keep a record of any Disclosures made pursuant to this policy and this information shall be available to any Individual who is the subject of such a Disclosure and who requests an accounting of such a Disclosure. Records regarding such Disclosures shall be kept for at least 6 years after the date of the Disclosure.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCES: 45 C.F.R. §§ 164.512(a) –(c) and (e) –(f).
RESOURCES:
DHHS/DOJ Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: *A Guide for Law Enforcement*, dated September 20, 2013 at http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf

DHHS GUIDANCE: *When does the Privacy Rule allow covered entities to disclose protected health information to law enforcement officials?*, created July 23, 2004, updated August 8, 2005 at http://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/

DATE OF POLICY: April 14, 2003
REVISED: September 1, 2016

D.14. HIPAA POLICY REGARDING THE USE AND DISCLOSURE OF PHI FOR RESEARCH PURPOSES AND THE ROLE OF THE INSTITUTIONAL REVIEW BOARD

PURPOSE OF POLICY

This policy establishes that the Emory University Institutional Review Board (IRB) performs the functions of a Privacy Board for Emory University, or for other institutions upon mutual agreement. Additionally, this policy sets forth the following standards:

(a) Standards for identifying when Research takes place within a Covered Component of the Emory University Hybrid Covered Entity by determining when a Research project includes Treatment for which Payment is collected using HIPAA-Covered Billing OR when Research is taking place in a non-Emory Covered Entity.
(b) Standards regarding the Use and Disclosure of PHI for Research, including standards for Authorizations and Waivers of Authorization.

DEFINITIONS

For convenience, the following terms used in this policy have the definitions listed below. These terms also are listed in the Glossary.

"Authorization" means written permission from a person to Use or Disclose his/her Protected Health Information (PHI), which permission contains all of the required elements specified in 45 CFR § 164.508(b) unless otherwise appropriately altered by an Institutional Review Board (IRB) or Privacy Board.

"**Covered Component"** is a component of a Hybrid Covered Entity that functions as a Covered Entity (e.g., as a Health Plan; Health Care Clearinghouse; or a Health Care Provider who transmits any Health Information in electronic form in connection with a transaction covered under HIPAA regulations, as each of the foregoing capitalized terms is defined at 45 CFR §160.103). [45 CFR § 164.105].

"Covered Entity" 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 under HIPAA regulations as each of the foregoing capitalized terms is defined at 45 CFR §160.103. [45 CFR § 160.103].

"Designated Record Set" means (a) a group of records maintained by or for a Covered Entity or Health Care Covered Component that is: (i) the medical records and billing records about Individuals maintained by or for a covered Health Care Provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a Health Plan; or (iii) used, in whole or part, by or for the Covered Entity to make decisions about Individuals. As used in this definition "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 or a Health Care Covered Component. [45 CFR § 164.501].

"HIPAA-Covered Billing" means transmitting Health Information in electronic form in connection with a transaction covered under HIPAA (i.e. submitting a claim to a health plan electronically).

"Individually Identifiable Health Information" means Health Information, including demographic information collected from an Individual that is: (a) created or received by a Health Care Provider, Health Plan, employer, or Health Care Clearinghouse; and (b) 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 (i) that identifies the Individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual. [45 CFR § 160.103].

"Payment" means activities (a) undertaken by a Health Plan to obtain premiums or determine coverage and provision of benefits; or (b) undertaken by a Health Care Provider or Health Plan to obtain or provide reimbursement for providing Health Care. [45 CFR § 164.501].

"Research" means a systematic investigation, including Research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. [45 CFR § 164.501].

"Treatment" means the provision, coordination, or management of Health Care and related services by one or more Health Care Providers, including the coordination or management of Health Care by a Health Care Provider with a third party; consultation between Health Care Providers relating to a patient; or referral of a patient from one Health Care Provider to another. [45 CFR § 164.501]. Additionally, and solely for purposes of determining whether Research includes Treatment, the definition of Treatment shall also include the administration of a drug, device or procedure to normal, healthy volunteers in the context of a clinical investigation.

"**Waiver of Authorization**" means an alteration to or waiver, in whole or part, of the Individual Authorization required for use of PHI for Research granted by an Institutional Review Board or a privacy board pursuant to the criteria set forth at 45 CFR 164.512(i). [45 CFR 164.512(i)].

POLICY

Role of Emory University IRB:

The Emory IRB is established in accordance with, and meets the membership and other requirements of, 45 CFR Part 46 and 21 CFR Parts 50 and 56, and any other applicable federal regulations. The Emory IRB performs the functions of a Privacy Board pursuant to 45 CFR §164.512(i).

Necessity for Authorization or Waiver of Authorization to Use PHI for Research

A researcher who has a Research protocol that falls under the jurisdiction of the Emory IRB and that seeks to use PHI that belongs to a Covered Component of the Emory University Hybrid Covered Entity, the Emory Healthcare Affiliated Covered Entity, or another Covered Entity/Component must have an Authorization, or a Waiver of Authorization approved by the Emory IRB (or other IRB or Privacy Board designated by Emory) before accessing such PHI unless the access to such PHI is granted as being preparatory to Research pursuant to *Policy D.16, HIPAA Policy Regarding Preparatory to Research Pathway for Accessing PHI*. A Covered Component of the Emory University Hybrid Covered Entity and the Emory Healthcare Affiliated Covered Entity also have the discretion to accept an Authorization or Waiver of Authorization approved by another Institutional Review Board or Privacy Board duly constituted pursuant to the requirements of 45 CFR §164.512(i) (e.g., central IRB, commercial IRB).

Determinations

(1) For each Research protocol that it considers, the Emory IRB will make the following determinations:

a. Whether the protocol includes as Research personnel, researchers who are Workforce members of one of the Emory University Hybrid Covered Entity's Covered Components as listed below; and, if so,

b. Whether the Research includes Treatment for which a Covered Component is collecting Payment using HIPAA-Covered Billing, in which case the Research will be considered to take place within the Covered Component and be subject to HIPAA;

OR, alternatively,

c. Whether the protocol is being conducted in a non-Emory Covered Entity for which the Emory IRB is performing the role of a privacy board.

AND, in all of the foregoing cases

d. Whether an Authorization is required, or whether the Research meets the standards for the grant of a Waiver of Authorization

List of Covered Components: The following is a list of the Covered Components of the Emory University Hybrid Covered Entity:

- Emory University School of Medicine
- Emory University School of Nursing
- Emory University Student Health Service for services not provided to students Oxford College of Emory University Student Health Service for services not provided to students
- Emory University Autism Center
- Emory Psychoanalytic Institute
- Emory Clinical and Translational Research Lab (ECTRL)
- Emory University Health Plan (governed by separate privacy and security policies)

PROCEDURE

IRB Review

Review Process: In reviewing a request for the Use or Disclosure of PHI for Research, the Emory IRB will follow its policies and applicable law in applying appropriate review procedures (e.g., full board or expedited review). An expedited review procedure may be used only if the Research involves no more than minimal risk to the privacy of the Individuals who are the subject of the PHI for which Use or Disclosure is sought. Any expedited review must be carried out by the Chair of the IRB, or one or more members of the IRB designated by the Chair. If a full board review process is used the review will take place at a convened meeting of the IRB that meets the requirements of 45 CFR Part 46 and/or 21 CFR Parts 50 and 56.

Determinations: The IRB will review Research and make the determinations described below.

Determination Regarding Protocol Personnel

The IRB will review the listing of personnel on the eIRB application to determine whether the Research protocol includes as Research personnel researchers who are Workforce members of one of the Emory University Hybrid Covered Entity's Covered Components listed above.

Determination as to Whether Research Includes Treatment

For Research conducted by Workforce members of a Covered Component of the Emory University Hybrid Covered Entity, the Emory IRB will make a determination as to whether the Research includes Treatment for which the Covered Component is collecting Payment using HIPAA-Covered Billing. If the IRB determines that the Research includes Treatment for which Payment is collected using HIPAA-Covered Billing, then the Research shall be considered as taking place within the Covered Component and any Identifiable Health Information collected as a part of the Research shall be considered to be PHI, and shall be subject to all HIPAA requirements when held by the Covered Component. If the IRB determines that the Research does not include Treatment for which Payment is collected using HIPAA-Covered Billing, then the Research shall be considered as taking place outside of the Covered Component, and any Identifiable Health Information collected as a part of the Research shall not be considered to be PHI or be subject to HIPAA requirements when held by the Researcher in a separate Research record; provided, however, that if the such Identifiable Health Information in placed by the Researcher in a medical record or other Designated Record Set maintained by a Covered Entity/Component, then that information placed in the Designated Record Set shall be considered to belong to the Covered Entity/Component and shall be subject to HIPAA Requirements when held by the Covered Entity/Component.

Determination of Whether the Protocol is being Conducted in a Non-Emory Covered Entity

When performing the role of a Privacy Board for a non-Emory entity, the Emory IRB will review the list of Research sites along with any reliance arrangements in place for the study to determine if the protocol is being conducted in a non-Emory Covered Entity. If the IRB determines that the Research is being conducted in a Covered Entity then any Identifiable Health Information collected as a part of the Research shall be considered to be PHI, and shall be subject to all HIPAA requirements when held by the Covered Component.

Determination of Whether an Authorization or Waiver of Authorization is Required

If a researcher wants to obtain PHI maintained within a Covered Entity or Covered Component (e.g., collect data from medical records for a retrospective study), then the IRB will require the researcher to have an Authorization from the study participant, or a Waiver of Authorization.

Authorization

Elements of Valid Authorization

If an Authorization is required, the Authorization must meet the requirements for an Authorization set forth in *Policy C.2, Uses and Disclosure of PHI that Require (A) Authorization; (B) No Authorization, but Opportunity for the Individual to Agree or Object; and (C) No Authorization and No Opportunity to Agree or Object* for the Authorization to be valid.

Specifically, the Authorization may be separate or be included as part of the informed consent document, and it must meet the following requirements, unless a waiver or alteration of some or all of the requirements of the Authorization is granted by the IRB:

(a) The form will be written in plain language and a copy of the signed document will be provided to the Individual, as well as maintained by the researcher.

(b) The Authorization will include:

i. A description of the information to be Used or Disclosed written in a specific and meaningful fashion.

ii. The name or other specific identification of the person(s) or class of persons, authorized to make the requested Use or Disclosure.

iii. The name or other specific identification of the person(s), or class of persons, to whom the Covered Component/Covered Entity may make the requested Use or Disclosure.

iv. A description of each purpose of the requested Use or Disclosure. NOTE: The study title, description and explanation that are currently required in the informed consent document are sufficient to meet this requirement.

v. An expiration date or expiration event that relates to the Individual or the purpose of the Use or Disclosure. NOTE: The statement "end of the research study," "none," or similar language is sufficient if the Authorization is for a Use or Disclosure of PHI for Research, including for the creation and maintenance of a Research database or Research repository.

vi. The signature of the Individual and date, or if the Authorization is to be signed by a personal representative of the Individual, the representative's signature along with a statement of the representative's authority to act for such Individual.

vii. A statement of the Individual's right to revoke the Authorization in writing along with a description of how the Individual may revoke the Authorization and the IRB-approved and/or HIPAA permitted exceptions to the right to revoke.

viii. A statement that the Covered Component/Covered Entity Health Care Provider may condition the provision of Research-related Treatment on provision of an Authorization for the Use or Disclosure of PHI for such Research, along with a statement of the consequences to an Individual for refusing to sign an Authorization in such circumstances.

ix. A statement of the potential for information Disclosed pursuant to the Authorization to be re-Disclosed to persons who are not subject to HIPAA and no longer be protected by HIPAA requirements.

Right to Revoke Authorization

A Research participant may withdraw from participation in a Research study in writing, verbally or by failure to further participate. However, under HIPAA, unless the informed consent/Authorization form states otherwise, HIPAA requires a participant to revoke his/her Authorization in writing in order to revoke the subsequent Use or Disclosure of his/her PHI. The Authorization is required to state that Research participant has the right to make a revocation of

the Authorization in writing along with stating any lesser means for revocation that may be permitted (e.g., verbal revocation). [NOTE: Even though an Authorization form may specify that the revocation of Authorization is to be in writing, if a verbal revocation is received, or if the participant verbally withdraws from the study, then the researcher should not access any further PHI of the participant from that point on.]

Use of PHI After Withdrawal from Participation in a Study

Withdrawal by Means Other than Writing. If the Authorization specified that revocation of Authorization was to be in writing, and a subject withdraws from participation in a Research study by any means other than in writing, then, when authorized by the IRB, PHI that has been collected for approved Research purposes may be included in data analysis and study results, unless otherwise stated in the informed consent form/Authorization. [NOTE: The most cautious approach with regard to such data, however, is to refrain from any further Use or Disclosure of the PHI except as is permitted under the "Withdrawal in Writing" section below.]

Withdrawal In Writing: Once a participant withdraws his or her Authorization in writing then no further Use or Disclosure of the participant's PHI is permitted except to the extent that the Covered Component has taken action in reliance on the original Authorization or as is otherwise permitted as an exception to revocation under HIPAA that was set forth in the Authorization. For example, if data was already collected in reliance on the Authorization, enough of the data can be Disclosed to a study sponsor to advise the sponsor of the participant's revocation/withdrawal, and any data that was submitted to the sponsor prior to the revocation does not have to be retrieved. In addition, data that was collected prior to the revocation may be submitted to a study sponsor if the submittal is necessary to preserve the integrity of the study.

Waiver or Alteration of Authorization Requirements

The IRB shall provide procedures by which a researcher may request a waiver or alteration of the requirement that an Authorization (hereinafter collectively referred to as a "Waiver of Authorization") be obtained to use PHI for Research. This procedure shall make clear the criteria that must be met to justify a Waiver of Authorization, and the researcher shall supply information detailing how such criteria are met for the IRB's review. The IRB will not grant a Waiver of Authorization, in whole or in part, unless it determines that the following "Waiver Criteria" have been satisfied:

(a)The Use or Disclosure of PHI involves no more than minimal risk to the privacy of Individuals based on the presence of at least the following elements:

(i) An adequate plan to protect the identifiers from improper Use and Disclosure;

(ii) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the Research, unless there is a health or Research justification for retaining the identifiers, or such retention is otherwise required by law;

(iii) Adequate written assurances that the PHI will not be re-Used or Disclosed to any other person or entity, except as required by law for authorized oversight of the Research, or for other Research for which the Use or Disclosure of PHI is permitted by 45 C.F.R. Part 164, Subpart E.

(b) The Waiver of Authorization will not adversely affect the privacy rights and the welfare of the Individuals;

(c) The Research could not practicably be conducted without the Waiver of Authorization;
(d) The Research could not practicably be conducted without access to and Use of the PHI; and
(e) The privacy risks to Individuals whose PHI is to be Used or Disclosed are reasonable in relation to the anticipated benefits if any to the Individuals, and the importance of the knowledge that may reasonably be expected to result from the Research.

Documentation of Grant of Alteration or Waiver of Authorization

If the IRB determines that a request for a Waiver of Authorization meets the foregoing Waiver Criteria then it may grant the Waiver of Authorization requested by the Researcher, and it shall provide the Researcher with documentation evidencing this grant and describing the nature of the waiver and/or alteration granted. The primary Researcher is responsible for providing a copy of this documentation to the appropriate person in the Covered Entity/Covered Component that is supplying the PHI and for placing a copy of the documentation in the protocol file. The documentation provided by the IRB must include the following elements:

(a)A statement identifying the IRB and the date on which the grant of the Waiver of Authorization occurred;
(b)A statement that the foregoing Waiver Criteria have been satisfied;
(c)A statement identifying whether the request for Waiver of Authorization was reviewed under (1) normal review procedures at a convened meeting of the IRB at which a majority of members were present, including an Unaffiliated Member; or (2) expedited review procedures;
(d) A statement that the IRB followed the regulations at 45 CFR Part 46 and/or 21 CFR Parts 50 and 56 (or other applicable federal regulations governing IRB review).
(e)A statement that briefly describes the PHI for which use or access has been determined to be necessary by the IRB, subject to the Minimum Necessary Rule (see below); and
(e)The signature of the Chair of the IRB, or another individual designated by the Chair.

Researchers who are granted Waivers of Authorization may be asked to provide confidentiality agreements from Research team members who will have access to PHI.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule: In determining the type and scope of the PHI for which the IRB determines Use or Disclosure for Research is necessary, the IRB must limit access to only that PHI which is reasonably necessary to accomplish the purpose for which the request is made. The Covered Component/Covered Entity that is disclosing the PHI may rely on a Researcher's documentation or representations that the information being requested is the minimum necessary, provided that reliance is reasonable under the circumstances.

Accounting Rule: The Covered Component/Covered Entity that discloses the PHI must account for the Disclosure made pursuant to the Waiver of Authorization. Accordingly, records of the Disclosure should be maintained for six years after the Disclosure occurs. Accounting for the Disclosure of PHI for Research Purposes should be made using either the Specific Accounting Method or General Accounting Method described below:

(a) Specific Accounting Method: If the Covered Component/Covered Entity makes a Disclosure of PHI for a particular Research purpose of less than 50 people (e.g., a Disclosure of certain medical information from the records of less than 50 people to a researcher for a retrospective study), then it must keep an individual record showing the specific Research protocol or activity to which an Individual's PHI was Disclosed. The Specific Accounting Method also may be used for Disclosures of PHI for a particular Research purpose of 50 of more people, OR the General Accounting Method may be used for such Disclosures.

(b) General Accounting Method: The General Accounting Method may be used for Disclosures of PHI for Research purposes involving 50 or more people. Under this method, the Covered Component/Covered Entity must keep a record of: (1) the name of the Research protocol or other Research activity for which the Disclosure was made; (2) a description, in plain language, of the Research protocol or activity, including the purpose of the protocol and the criteria for selecting certain records; (3) a description of the PHI that was Disclosed; (4) the period when the Disclosures were made, including the date of the last Disclosure made within the period; (5) the name, address and telephone number of the entity that sponsored the Research and or the researcher to whom the information was disclosed; and (6) a statement that the PHI of the Individual who is requesting the accounting may or may not have been Disclosed for a particular protocol or Research activity.

(c) Provision of List of Protocols Upon Request: If the General Accounting Method is employed, then each Individual who requests an accounting of the Disclosure of his/her PHI in accordance with applicable HIPAA regulations and Emory University HIPAA policies shall be provided with a list of all Research protocols at Emory for which the PHI of 50 or more people was disclosed. This list shall contain all of the elements set forth under the description of the General Accounting Method. In addition to providing this list of protocols (if any), the Covered Component also shall provide the Individual making the request with an accounting of any other non-Research related disclosures of that Individual's PHI or Research disclosures for fewer than 50 people, as required by applicable HIPAA regulations.

(d) Additional Assistance: If a Covered Component provides a General Accounting of Research Disclosures, then if it is reasonably likely that the Individual's PHI was Disclosed to a particular protocol or activity, the Covered Component must, upon the Individual's request, assist the Individual in contacting the Research sponsor and researcher involved in the protocol.

Transition Period Provisions

PHI that was created or received before or after HIPAA's compliance effective date of April 14, 2003 may be used for the Research purposes for which it was obtained, if the PHI was obtained pursuant to one of the following means, and then, only to the extent allowed by the means by which it was obtained:

(a) An Authorization or other express legal permission from an Individual to Use or Disclose PHI for the Research.

(b) The informed consent of the Individual to participate in the Research.

(c) A waiver by the IRB of informed consent for the Research; provided, however, that if informed consent is sought from an Individual after the HIPAA effective compliance date, then an Authorization must be sought and obtained as well.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCES: 34 C.F.R. §§ 164.502, .508, .512, .528.
DATE OF POLICY: April 14, 2003.
REVISED: September 1, 2016

D.15. POLICY REGARDING USE AND DISCLOSURE OF PSYCHOTHERAPY NOTES AND MENTAL HEALTH INFORMATION

DEFINITIONS

"**Psychotherapy**" means the employment of Psychotherapeutic Techniques. [OCGA §24-5-501].

"**Psychotherapeutic Techniques**" means those specific techniques involving the in-depth exploration and treatment of interpersonal and intrapersonal dynamics by professionals who are licensed to administer such techniques under the laws of the State of Georgia (i.e., licensed psychiatrists, psychologists, clinical social worker, clinical nurse specialist in psychiatry/mental health, marriage and family therapist or professional counselor). [OCGA §§ 24-5-501 & 43-10A-3].

"**Psychotherapy Notes**" means 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 Individual's medical records. 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. [45 CFR §164.501].

"**Licensed Mental Health Professional**" means a licensed psychiatrist, psychologist, clinical social worker, clinical nurse specialist in psychiatry/mental health, marriage and family therapist or professional counselor. [OCGA § 24-5-501]

PURPOSE OF POLICY

The purpose of this policy is to set forth the special requirements under HIPAA and the laws of the State of Georgia as concerns Psychotherapy Notes and PHI contained in certain mental health treatment records.

POLICY

HIPAA and State Law

HIPPA has special rules governing the Disclosure of Psychotherapy Notes. Additionally, the laws of the State of Georgia consider communications between a patient and a Licensed Mental Health Professional who is providing, or has provided, Psychotherapy to a patient to be privileged. In cases concerning the Disclosure of Psychotherapy Notes or records of communications between a patient and Licensed Mental Health Professional who is providing, or has provided, Psychotherapy to the patient, the laws of the State of Georgia shall apply in instances in which those laws afford more rights to Individuals than do HIPAA regulations.

Authorization Required for Disclosure to Third Parties of Psychotherapy Notes or Communications between a Patient and a Licensed Mental Health Provider

Notwithstanding anything to the contrary set forth in these Policies, before a Covered Component of the Emory University Hybrid Covered Entity can Disclose to a third party PHI that consists of Psychotherapy Notes or communications between an Individual and a Licensed Mental Health Provider who is providing (or has provided) Psychotherapy to the Individual, the Covered Component must have the written Authorization of the Individual who is the subject of the Psychotherapy Notes or who had such communications. The foregoing applies to adult and minor Individuals. Additionally, the Disclosure to a third party of Psychotherapy notes concerning a deceased Individual and/or communications between such Individual and a Licensed Mental Health Provider is prohibited.

In order to ensure compliance with the laws of the State of Georgia, the Covered Component MUST contact the Emory University Office of the General Counsel before making any such Disclosure to third parties of Psychotherapy Notes or communications between an Individual and a Licensed Mental Health Provider without having written Authorization from the Individual, including any Disclosure contemplated in the following circumstances, even though such Disclosures may be permitted under the HIPAA Regulations:

(a) To the extent that a Use or Disclosure is required by law regarding victims of abuse, neglect or domestic violence, and the Use or Disclosure complies with and is limited to the requirements of the law. See *Policy D.7, HIPAA Policy Regarding Use and*

Disclosure of PHI in Connection with Reporting of Child Abuse; Abuse Neglect or Domestic Violence Concering Adults who are not Elder Persons or Disabled Adults; and Abuse or Neglect of an Elder Person or Disabled Adult.

(b) To the extent the Use or Disclosure is required by law for judicial and/or administrative proceedings, and the Use or Disclosure complies with and is limited to the requirements of the law. See *Policy D.12, HIPAA Policy Regarding Disclosures of PHI for Judicial and Administrative Proceedings.*

(c) To the extent the Use or Disclosure is required for law enforcement purposes, and the Use or Disclosure complies with and is limited to the requirements of the law. See *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes.*

(d) To a Health Oversight Agency to conduct oversight of the author of the Psychotherapy Notes pursuant to *Policy D.8, HIPAA Policy Regarding Disclosure and Use of PHI for Health Oversight Activities.*

(e) To a medical examiner or coroner pursuant to *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information.*

(f) To avert a serious threat to health or safety pursuant to *Policy D.9, HIPAA Policy Regarding Use and Disclosure of PHI to Avert A Serious Threat to Health or Safety.*

(g) Use or Disclosure by the Covered Component or the Hybrid Covered Entity to defend itself in a legal action or other proceeding brought by the Individual.

Disclosure of Psychotherapy Notes to the Individual who is the Subject of the Notes

The laws of the State of Georgia requiring Disclosure of health records to Individuals do not apply to psychiatric, psychological or other mental health records. HIPAA regulations, however, afford additional rights to Individuals regarding access to their PHI, and thus HIPAA regulations will typically apply in situations in which an Individual requests access to his/her records regarding mental health Treatment. Accordingly, with the exception of Psychotherapy Notes, *Policy B.4 Individual Right to Access PHI* will apply with respect to the Disclosure to an Individual of his/her PHI regarding Treatment for mental health. With respect to the Disclosure of Psychotherapy Notes to an Individual, the following process applies.

(a) A Covered Component may Disclose Psychotherapy Notes concerning an Individual to the Individual at his/her request; provided, however that Disclosure to the Individual is permissible, but not mandatory (see below). The Covered Component may deny the Individual the right to access Psychotherapy Notes without any opportunity for the Individual to review the denial pursuant to *Policy B.4, Individual Right to Access PHI.*

(b) A Covered Component may Disclose Psychotherapy Notes to an Individual who is the subject of those Notes and who requests an accounting of Disclosures of his/her PHI, but only to the extent required to provide the Accounting pursuant to *Policy B.6, Right of an Individual to Receive an Accounting of Disclosures of PHI.*

(c) If a Provider receives a request from an Individual for his/her Psychotherapy Notes, the Provider must decide if he/she will permit the Individual access to the Psychotherapy Notes. If the Provider determines the he/she wants to deny the Individual access to the Psychotherapy Notes, the Provider must contact the the Office of the General Counsel for review of the denial under applicable HIPAA regulations and state laws.

Type of Authorization Required to Use/Disclose Psychotherapy Notes under HIPAA

An Authorization for the Use and Disclosure of Psychotherapy Notes must contain all of the elements required for an Authorization under *Policy C.2, Uses and Disclosures of PHI that Require (A) Authorization; (B) No Authorization, but Opportunity for the Individual to Agree or Object; and (C) No Authorization and No Opportunity to Agree or Object*. Additionally, the Authorization may not be combined with any other Authorization, except for another Authorization for the Use and Disclosure of Psychotherapy Notes.

Minimum Necessary Rule: If a Covered Component is making a Disclosure of Psychotherapy Notes without an Individual's Authorization, as approved by the Office of the General Counsel, then the Covered Component must only disclose the Minimum Necessary type and amount of PHI that is required to achieve the purpose of the Disclosure.

Accounting Rule: Unless an Individual has authorized a Disclosure of Psychotherapy Notes, their Disclosure under this Policy is subject to a request for an Accounting by an Individual. The Emory Covered Component that makes the Disclosure should document the Disclosure and maintain this documentation for six (6) years after the Disclosure occurs.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCES: 45 CFR §§164.508(a)(2) & (b); 164.502(a)(2)(ii); 164.512(a) & (d); 164.512(g)(1); 164.512(j)(1)(i); O.C.G.A. §§ 24-5-501, 31-33-4, 43-10A-3 & 43-39-16.
DATE OF POLICY: April 14, 2003.
REVISED: September 1, 2016

D.16. PREPARATORY TO RESEARCH PATHWAY FOR ACCESSING PHI

PURPOSE OF POLICY

The purpose of this policy is to describe how a researcher in a Covered Component may gain access to an Individual's PHI to conduct a Use Preparatory to Research.

POLICY

A Covered Component of the Emory University Hybrid Covered Entity, or another Covered Component or Covered Entity, may permit a researcher access to an Individual's PHI for a Use Preparatory to Research without having the Individual's Authorization or providing the Individual an opportunity to agree or object, provided that the researcher follows the procedures outlined below.

PROCEDURE

Representations

For each Use Preparatory to Research, the researcher must provide to the Covered Component or the Covered Entity from which PHI is sought signed, written representations as follows:

(a) That the Use or Disclosure of PHI is sought solely to review the PHI as necessary to prepare a Research protocol or for similar purposes preparatory to Research;
(b) That the researcher will not remove PHI from the Emory University Hybrid Covered Entity or a Covered Component thereof, or from any other Covered Entity or Covered Component from which PHI is sought during the course of the review; and
(c) That the PHI for which Use or Disclosure is sought is necessary for the Research purposes.

Covered Component or Covered Entity Options to Provide PHI for Use Preparatory to Research

A Covered Entity or Covered Component, may, but is not required to, permit a researcher who makes the foregoing representations access to PHI held by the Covered Entity or Covered Component for a Use Preparatory to Research. Each Covered Entity or Covered Component is free to adopt its own internal policies for determining whether/when and to which researchers it will permit Use Preparatory to Research of PHI held by the Covered Entity or Covered Component. A Covered Entity or Covered Component must document when it permits a researcher Use Preparatory to Research. In this regard, the Covered Entity Covered Component is free to adopt its own internal forms that document the above representations that must be made prior to a Use Preparatory to Research and the granting of a Use Preparatory to Research.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimun Necessary Rule: In determining the type and scope of the PHI for which the IRB determines Use or Disclosure for Research is necessary, the Covered Entity/Covered Component that received a request for a Use Preparatory to Research must limit access to only that PHI which is reasonably necessary to accomplish the purpose for which the request is made. The Covered Component/Covered Entity that is disclosing the PHI may rely on a Researcher's documentation or representations that the information being requested is the minimum necessary, provided that reliance is reasonable under the circumstances.

Accounting Rule: The Covered Component/Covered Entity that discloses the PHI pursuant to a Use Preparatory to Research should follow the same process for accounting that applies to Disclosures made pursuant to a Waiver of Authorization as described in *Policy D.14, HIPAA Policy Regarding the Use and Disclosure of PHI for Research Purposes and the Role of the Institutional Review Board.* Records of the Disclosure should be maintained for six years after the Disclosure occurs.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCE: 45 CFR §§164.512(i)(1)(ii); 164.528.
DATE OF POLICY: April 14, 2003.
REVISED: September 1, 2016

D.17. SPECIAL RULE REGARDING THE CONFIDENTIALITY OF RAW RESEARCH DATA

The State of Georgia affords special protections to Confidential Raw Research Data with respect to subpoenas, legal discovery, or admissibility as evidence in any judicial or administrative proceeding. Accordingly, in addition to the foregoing requirements set forth above in Sections A-C, the following requirements apply to Confidential Raw Research Data. Any Disclosure of Confidential Raw Research Data that is authorized or required by the law of the State of Georgia,

or any other law, however, will not destroy the confidential nature of the data except for the purpose for which the Disclosure is made.

Confidential Raw Research Data in a researcher's possession in the State of Georgia is not subject to subpoena, otherwise discoverable, or deemed admissible as evidence in any judicial or administrative proceeding in any court in the State of Georgia except as otherwise provided below:

(a) Confidential Raw Research Data related to a person may be Disclosed to that person or another person on such person's behalf when specifically authorized by law.
(b) Confidential Raw Research Data related to a person may be Disclosed to an entity who is designated in writing by the Research participant (or by a person authorized by law to act on his/her behalf) to receive that information.

(c) Confidential Raw Research Data related to a person may be Disclosed to any agency or department of the federal government, the State of Georgia (or any of its political subdivisions), if such data are required by law or regulation to be reported to such agency or department.

(d) Confidential Raw Research Data may be Disclosed in any legal proceeding in which a party was a participant, researcher, or sponsor in the underlying Research study, including, but not limited to, any judicial or administrative proceeding in which a Research participant places his or her care, treatment, injuries, insurance coverage, or benefit plan coverage at issue; provided, however, that the identity of any Research participant, other than the party to the judicial or administrative proceeding, shall not be Disclosed, unless the researcher or sponsor is a defendant in such proceeding.

(e) Confidential Raw Research Data may be Disclosed in any judicial or administrative proceeding in which the researcher has either volunteered to testify or has been hired to testify as an expert to one of the parties to the proceeding.

(f) In a criminal proceeding, a court shall order the production of Confidential Raw Research Data if the data are relevant to any issue in the proceeding, and the Court shall impose appropriate safeguards against the unauthorized Disclosure of the data and admit the data into evidence if the data are material to the defense or prosecution.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule: No information other than that which is requested in the subpoena, discovery request or other legal process should be provided.

Accounting Rule: Disclosures made pursuant to legal process should be tracked and are subject to a request for an accounting from an Individual. Records of Disclosure should be kept for at least 6 years after the Disclosure is made.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI

In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCES: 45 CFR §§64.512(a) & (e); O.C.G.A. §24-12-2

RESOURCES: DHHS OCR FAQs Judicial and Administrative Proceedings, www.hhs.gov/ocr/privacy/hipaa/faq/judicial_and_administrative_proceedings

DATE OF POLICY: April 14, 2003

REVISED: September 1, 2016

SECTION E. MISCELLANEOUS HIPAA POLICIES

E.1. HIPAA POLICIES REGARDING EMAILING AND TELEFAXING PHI

PURPOSE OF POLICY

These Policies set forth general requirements for protecting the privacy of Individual's protected health information (PHI) when emailing or telefaxing. These policies seek to minimize the risk of unauthorized access to of modification of PHI during and after electronic transmission.

POLICY

A Covered Component of the Emory University Hybrid Covered Entity has the responsibility to verify the identity and authorization of persons/entities to whom telefaxes and emails are sent, and to follow the procedures below in transmitting such telefaxed and emails.

PROCEDURE

Telefaxing via a Standalone Telefax Unit

Prior to telefaxing any PHI via a standalone telefax unit, the Covered Component should perform the following verifications: (a) verify that the PHI in the telefax is being Disclosed to the receipient pursuant to a specific HIPAA regulation or policy (e.g., transmission to another Healthcare Provider for Treatment purposes) or pursuant to an Authorization; and (b) verify the

receiving telefax number by calling the intended recipient, and, if necessary, sending a test telefax. Numbers that are used frequently may be pre-programmed into the telefax unit to avoid incorrect dialing; however, such pre-programmed numbers must periodically be re-verified. Each telefax should have a be accompanied by a cover sheet that includes data and time of transmission; sender's name, title, address and telephone and telefax numbers; number of pages being sent (including the cover sheet); and a confidentiality statement, such as the following: "The information contained in this telefax is privileged and confidential information intended only for the use of the addressee listed above. If you are neither the intended recipient, nor the employee or agent responsible for delivering this telefax to the intended recipient, you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this information is strictly prohibited. If you have received this telefax in error, please notify the sender immediately."

Receiving Telefaxes

Telefax machines should be located in secure areas away from visitors and the public. Telefaxes should be removed from the machines as promptly as possible. If the Covered Component receives regular telefaxes from particular senders, it must keep those senders apprised of any changes in telefax numbers.

Misdirected Telefaxes

If the Covered Component discover that a telefax containing PHI was sent to an incorrect number, the Covered Component should take steps to locate the misdirected telefax or confirm that the number to which the telefax was sent is not a working telefax line. If possible, the incorrect recipient of the telefax should be contacted and requested to destroy or return the misdirected telefax. Any other steps that are necessary to mitigate the potential of any harm to the Individual(s) whose PHI was in the telefax should be be taken. In general, telefaxes that are misdirected internally to a Covered Component or Emory Healthcare Covered Entity are not considered to be a Breach. In the event of a telefax that is misdirected externally, the sender should promptly contact the Emory University or Emory Healthcare Privacy Officer.

Telefaxes Sent Via Computer Telefax Applications

The procedures set forth above also apply to telefaxes sent via computer telefax applications. In addition, the Emory University and Emory Healthcare HIPAA Security Policy entitled "Transmission Security Policy" also applies.

Emailing Information that Contains PHI

To protect electronic PHI that is transmitted via email over a network, the Covered Component must follow the Emory University and Emory Healthcare HIPAA Security Policy entitled "Transmission Security Policy." This Policy can be found at https://hipaa.emory.edu/home/Policies/emory_security_policies.html An Emory ID and password is required to access this policy.

Specific Verification Requirements

In addition to the verification steps set forth herein, any applicable verification requirements specified in *Policy C.6, Verification Requirements for Disclosure of PHI* also should be taken.

APPLICABILITY OF MINIMUM NECESSARY AND ACCOUNTING RULES

Minimum Necessary Rule: The minimum PHI that is necessary to achieve the purpose of Disclosure should be disclosed.

Accounting Rule: Depending on the purpose of the Disclosure and whether or not it is made pursuant to an authorization, a Disclosure made pursuat to this policy may be subject to a request for an accounting by an Individual. Accordingly the Emory Covered Component that makes the Disclosure should document the Disclosure and maintain this documentation for six years after the Disclosure.

REFERENCES: 45 CFR §514(h)
DATE OF POLICY: April 2003
REVISED: September 1, 2016

E.2 BREACH NOTIFICATION

PURPOSE OF POLICY

The purpose of this policy is to set forth the process that should be followed in determining whether or not a "Breach," as defined in the Health Information Technology for Economic and Clinical Health Act (HITECH) has occurred when there is an unauthorized Use or Disclosure of PHI in/by a Covered Component of the Emory University Hybrid Covered Entity, and, if so, what process must be followed with respect to notification of affected Individuals, mitigation of any damage and reporting to government agencies.

DEFINITIONS

The definitions below are provided here for convenience. These defined terms also appear in the Glossary.

"Access" means the ability to read, write, modify, or communicate data/information.

"Breach" is the acquisition, Access, Use, or Disclosure of Protected Health Information (PHI) in a manner that is not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the PHI.

1. Breach excludes:
    d. Any unintentional Access or Use of PHI by a Covered Component of the Emory University Hybrid Covered Entity, including a Business associate, if such Access or Use was made in good faith and within the scope of work and does not result in further inappropriate Use or disclosure.
    e. Any inadvertent Disclosure by a person who is authorized to access PHI controlled by a Covered Component of the Emory University Hybrid Covered Entity to another person also authorized to access PHI controlled by a Covered Component, as long as the information received as a result of such Disclosure

does not result in further inappropriate Use or disclosure.

f. A Disclosure of PHI where an employee of a Covered Component of the Emory University Hybrid Covered Entity has a good faith belief that an unauthorized person who received the information would not reasonably be able to retain such information.

3. An acquisition, Access, Use, or Disclosure of Protected Health Information is presumed to be a Breach unless the Emory University Hybrid Covered Entity, or applicable Business Associate, can demonstrate that there is a low probability that the Protected Health Information has been compromised based on a risk assessment of at least the following factors:
    a. The nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification,
    b. The unauthorized person who used the Protected Health Information or to whom the Disclosure was made,
    c. Whether the Protected Health Information was actually acquired or viewed,
    d. The extent to which the risk to the Protected Health Information has been mitigated, including the extent and efficacy of mitigation, and
    e. Other mitigating factors considered by the Emory University Hybrid Covered Entity that are relevant to the risk assessment.

POLICY

In the event of a potential Breach, the Emory University Hybrid Covered Entity will follow the procedure described below to determine whether a Breach occurred, and then, as necessary, provide written notification to the affected Individuals, the Department of Health and Human Services and media. Such notification will be carried out in compliance with the Health Information Technology for Economic and Clinical Health Act (HITECH), as well as any other applicable federal or state notification law.

PROCEDURE

Steps to be Following in the Event of a Potential Breach

In the event of a potential Breach of PHI by a Covered Component of the Emory University Hybrid Covered Entity (or upon notification or discovery of a potential Breach by a Business Associate (BA)), Workforce members of the affected Covered Component will follow the procedures noted below.

Step One: Alert Supervisor, Privacy Officer or Security Officer. Employees and BAs should notify thir supervisor and the Emory University Privacy Officer and Security Officer immediately if a potential Breach of PHI is discovered or believed to have occurred. Notification can also be made via the Emory Trust Line at 1-888-550-8850, 24 hours a day and 7 days a week.

The Breach Notification Form (**Attachment E.2 – 1**) can be used in the event of a potential Breach to record details of the incident. Employees are encouraged to use the form to record details of a privacy incident, though the form is not required to be used to report a concern. If

the Breach Notification Form is used, it should be forwarded to the Emory University Privacy Officer and the Security Officer. The Emory University Privacy Officer will, in turn, notify the Emory Healthcare Privacy Officer if PHI belonging to Emory Healthcare is involved.

Step Two: Alert Administration. The unit responsible for the potential Breach, or the unit that has the agreement with the BA responsible for the potential Breach, must alert the following offices as soon as possible if a Breach is reasonably believed to have occurred:

- Unit leadership
- Risk Management
- Information Technology, if the potential Breach involves electronic PHI (ePHI)
- Police and/or Security Personnel if physical theft has taken place

Step Three: Investigation of Potential Breach. The Privacy Officer/Security Officer or designee will conduct the investigation of the potential Breach. The investigation conducted should include the following (as applicable):

1. Interviews of employees and/or BAs with knowledge of the incident, including those responsible for the incident.
2. Forensic examination of any computer hardware, software, etc. involved in the incident, as determined by the Security Officer. This examination will focus on determining the extent of the potential Breach and specific information that was affected. If applicable. BAs will be asked to perform similar forensic examinations of their own computer hardware and software.
3. Communication with police officers to file theft or other reports and/or to review the police report(s).

Step Four: See attached Flow Chart - Attachment E.2 - 2
See attached Risk Assessment Form - Attachment E.2 - 3

Once the initial investigation has concluded, the Emory University/Emory Healthcare Breach Risk Assessment Team will assess the situation using the below questions as a guide to making a determination of whether a Breach of PHI has occurred that requires notification.

1. **Was there an acquisition, access, use, or disclosure of PHI?**
   If yes, proceed to 2. If no, proceed to Step 5.

2. **Was the PHI at issue "Unsecure PHI?"**
   If yes, proceed to 3. If no, proceed to Step 5.

3. **Did the acquisition, Access, Use, or Disclosure of PHI result in a violation of the HIPAA Privacy Rule?**
   If yes, proceed to 4. If no, proceed to Step 5.

4. **Did the potential Breach compromise the security or privacy of the PHI? (See mitigating factors to consider in Attachment E.2 - 2; Complete Attachment E.2 - 3.)**
   If yes, proceed to 5. If no, proceed to Step 5.

5. **Is there an exception that applies to the definition of Breach?** ***(See exceptions in definition of Breach at the beginning of this Policy.)***
    a. *If no, skip Step 5 and proceed to Steps 6-11 for procedures regarding provision of notice. If yes, proceed to Step 5 because no notice is required under HIPAA.*

Step Five: When Notice is not required**.** If "no" was answered to any of the Questions 1-5 above, or if a Breach exception applies as noted in Question 5, then notice is not required.

Although there may not have been a Breach requiring notification, the Breach Risk Assessment Team in consulation with management may determine that notice is advisable under the circumstances or is required under other federal or State laws that may be applicable.

Step Six: Notification to the Individuals whose PHI Has Been Breached.
In the event of a confirmed Breach, the responsible unit will notify each Individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, Used, or Disclosed as a result of such Breach.

If the Breach was made by a BA, the Emory University Privacy Officer (or designee) will coordinate with the BA regarding which party will actually send the notice.

Notification: If notification is required, it should be provided without unreasonable delay and no later than 60 calendar days after discovery of the Breach, unless the Law Enforcement Exception noted below applies.

- If a law enforcement official states to the Emory University Hybrid Covered Entity or the BA (if applicable) that a notification would impede a criminal investigation or cause damage to national security, the Emory University Hybrid Covered Entity or the BA may, (a) delay such notification for the time period specified by the official if the statement is in writing and specifies the time for which a delay is required, or (b) document the statement, including the identity of the official making the statement if the statement is made orally, and delay the notification temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in (a) is submitted during that time.

Breaches Treated as Discovered: A Breach should be treated as discovered by the Emory University Hybrid Covered Entity as of the first day on which such Breach is known, or by exercising reasonable diligence, would have known. The Emory University Hybrid Covered Entity is considered to have knowledge of a Breach if such Breach is known by an employee of a Covered Component, a BA acting as a Covered Component's agent, or any individual other than the person who committed the Breach.

Required Contents of Notification: The Individual notification should be written in plain language and should include, to the extent possible, the following elements:

1. A brief description of what happened, including the date of the Breach, and the date of the discovery of the Breach, if known;

2. A description of the types of unsecured PHI that were involved in the Breach (such as full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;
4. A brief description of what the Emory University Hybrid Covered Entity is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches; and
5. Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

Although, the elements above and other actions noted in this policy, are the steps required by HIPAA, the Privacy Officer or Security Officer, in conjunction with Emory University leadership, may consider offering additional assistance or information to affected Individuals, such as complimentary credit monitoring, identity theft insurance, and fraud alerts for approximately one year from the date of the Breach.

Method of Individual Notification: The Individual notification required should be provided in the following form:

- *Written Notice.* Notice should be provided via written notification by first-class mail to the Individual at the last known address of the Individual, or if the Individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

- If the Emory University Hybrid Covered Entity knows the Individual is deceased and has the address of the next of kin or personal representative, written notification by first class mail should be sent to either the next of kin or personal representative of the Individual. Substitute notice (as noted below) need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or Personal Representative of the deceased Individual.

- *Substitute Notice*. In the case in which there is insufficient or out-of-date contact information that prevents written notification to the Individual, a substitute form of notice reasonably believed to reach the Individual should be provided. The names or other PHI of Individuals should not be Disclosed in such notice.

- *Insufficient or Out-of-Date Contact Info for < 10 Individuals.* In the case in which there is insufficient or out-of-date contact information for fewer than ten Individuals, then substitute notice may be provided by an alternative form such as written notice, telephone, or other means.

- *Insufficient or Out-of-Date Contact Info for ≥ 10 Individuals.* In the case in which there is insufficient or out-of-date contact information for ten or more Individuals, then such substitute notice shall:

1. Be in the form of either a conspicuous posting for a period of 90 calendar days on the home page of the website of Emory University, or conspicuous notice in major print or broadcast media in geographic areas where the Individuals affected by the Breach likely reside; and
2. Include a toll-free phone number that remains active for at least 90 calendar days where an Individual can learn whether the individual's PHI may be included in the Breach.

Additional Notice in Urgent Situations. In any case deemed by the Emory University Privacy Officer or the Security Officer as an urgent situation because of possible imminent misuse of PHI, the Emory Hybrid Covered Entity may provide information to Individuals by telephone or other means as appropriate in addition to written notification.

Step Seven: Notification to Media of Breaches involving 500+ Individuals: For a Breach of PHI involving more than 500 residents of a state or jurisdiction, the Emory University Hybrid Covered Entity will notify prominent media outlets serving the state or jurisdiction.

Timeliness of notification. Media notification should be made without unreasonable delay and not later than 60 calendar days after discovery of a Breach.

Content of notification. The media notification required by this section shall meet the same content requirements of the Individual notice. The names or other PHI of affected Individuals should not be Disclosed in such notice.

Step Eight: Notification of HHS**.** The Emory University Hybrid Covered entity will notify the Secretary of HHS using the electronic forms located on the HHS OCR website.

Breaches Involving 500 or More Individuals. For Breaches of PHI involving 500 or more Individuals, the Privacy Officer (or designee), shall provide the notification at the same time as the Individual notice and in the manner specified on the HHS OCR website.

Breaches Involving Less Than 500 Individuals. For Breaches of PHI involving less than 500 Individuals, the Privacy Officer (or designee) shall maintain a log or other documentation of such Breaches and, not later than 60 days after the end of each calendar year, shall provide notification of Breaches occurring during the preceding calendar year, in the manner specified on the HHS OCR website.

Step Nine: Documentation**.** The Emory Hybrid Covered Entity will retain files on and/or a log of all Breaches of Unsecured PHI regardless of the number of Individuals affected.

Step Ten: Accounting. The Emory Hybrid Covered Entity will account for unauthorized Disclosures of PHI as required by *Policy B.6, Right of an Individual to Receive an Accounting of Disclosures of PHI.*

Step Eleven: Sanctions. Human Resources in consultation with the Privacy and Security Officers and Emory University Hybrid Covered Entity leadership will determine whether

sanctions against any employee involved in a Breach are warranted. In the case of a Breach occurring with a BA, the Office of General Counsel, leadership of the involved Unit, and the Privacy and Security Officer will consult to determine whether sanctions of the BA are warranted, up to and including possible termination of the BA agreement.

Encrypted PHI

Notification is not required if PHI is secure via encryption; provided, however, that encryption keys keys must be kept on a separate device from the data they encrypt or decrypt.

Nothing in this policy is meant to require a Covered Component to provide information to the Individual that is privileged under the attorney-client privilege, licensed mental health professional or other privilege laws. Further, the Emory Univeristy Hybrid Covered Entity will not disclose in the notification to the Individual the names of any employees or other Individuals involved in the Breach or any specific sanctions taken against such employees.

Unit Responsibility

The unit responsible for the potential Breach/Breach, or that has the BA agreement with the BA where the potential Breach/Breach occurred, will be responsible for compliance with any necessary notification to affected Individuals and any and all costs required to comply to carry out such notification and/or otherwise comply with this policy and the HITECH Act Breach Notification Requirements. The Emory University Privacy Officer retains the ability to direct Breach notification activities as necessary to comply with the requirements of the HITECH Act.

ATTACHMENTS: **Attachment E.2 - 1**: Breach Reporting Form
Attachment E.2 – 2: Breach Algorithm
Attachment E.2 – 3: Breach Risk Assessment

REFERENCES: 45 CFR §§ 164.400 - .414.
DATE OF POLICY: September 1, 2016

Attachment E.2 -1: Potential HIPAA Privacy Breach Reporting Form

This form may be completed in the event of a potential breach of HIPAA. Please provide detailed and complete answers to all of the following questions.
When finished, please forward the form by secure email to the Emory University Privacy Officer at **kwest02@emory.edu** or send by telefax to (404) 727-2328

Name and title of the person completing the reporting form:
_____

Date of Completed Report: _____/_____/_____

Date and time of incident:
_____

Provide a description of the incident, including details on what happened, how the incident occurred, all relevant facts, and information on any actions taken to date (attach an additional sheet if necessary):
_____
_____
_____
_____
_____
_____

List staff members involved:
_____
_____

The name of the unauthorized person/entity who received the PHI, including contact information:
_____
_____
_____

PHI involved in the breach (what information was involved? SSN, MRN, etc.):
_____
_____

Attachment E2-2: Breach Algorithm

Was there an acquisition, access, use, or disclosure of PHI?

NO → No HIPAA notice required.
Although there may not have been a Breach requiring HIPAA notification, the Privacy Officer in consultation with the Security Office and leadership may determine whether notice is advisable under the circumstances or is required under other federal or State laws that may be applicable.

YES

Was the PHI at issue "Unsecure PHI?" Note: If the PHI was encrypted or destroyed using NIST standards noted in the HHS Breach Notification Guidance, then it was secure.

YES

Did the acquisition, access, use, or disclosure of PHI result in a violation of the HIPAA Privacy Rule?

YES

Did the potential Breach compromise the PHI In a manner that was not mitigated by the following?

- The nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the Protected Health Information or to whom the disclosure was made;
- Whether the Protected Health Information was actually acquired or viewed;
- The extent to which the risk to the Protected Health Information has been mitigated;
- Other mitigating factors considered by EHC that are relevant to the risk assessment.

Attachment E.2 - 3 can be used to document consideration of each mitigating factor.

YES → HIPAA Notice Required.

See Policy E.2 procedures for providing such notice.

NO

Does one of the following exceptions to the definition of "Breach" apply?
Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule;
Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; OR
A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Attachment E2-3: Potential Breach Risk Assessment

Risk Assessment	Incident Date:
	Report Date:

Purpose of this Document: This document is intended for internal use. It is designed to provide a summary of key risk factors related to this incident and provide sufficient background information to enable an institutional decision to be made on whether a breach notification is warranted.

Incident Background

What happened?

Please provide names of individuals and organizations involved.

When did the incident occur?

Risk Assessment

Has there been an unauthorized acquisition, access, use, or disclosure of unsecured sensitive data?

What is the nature and extent of the Protected Health Information involved? What types of identifiers were included?

Who was the unauthorized party that received the Protected Health Information?

Was the Protected Health Information actually acquired or viewed by the receiving party?

Have any actions been taken to mitigate any risk to the patients involved, such as, has the receiving party confirmed the paperwork has been destroyed?

Please provide details on any other relevant mitigating factors.

How many patients are believed to be involved in the incident?

Is there any indication that the data was targeted? If yes, is the primary motivation of the attacker known?

<u>Notification Recommendations: Based on the potentially harmful and mitigating factors above, please answer the following.</u>

Has a breach legally requiring notification actually occurred?

Should Emory notify potentially affected parties? If so, should Emory offer identity theft protection services?

E.3 AIDS CONFIDENTIAL INFORMATION

PURPOSE OF POLICY

The purpose of this policy is to describe the special protections under the laws of the State of Georgia that apply to the Disclosure of PHI that is also AIDS Confidential Information.

DEFINITION

The definition of the following term is provided here for convenience. This term also appears in the Glossary.

"**AIDS Confidential Information**" means information which discloses that a person: (a) has been diagnosed as having AIDS; (b) has been or is being treated for AIDS; (c) has been determined to be infected with HIV; (d) has submitted to an HIV test; (e) has had a positive or negative result from an HIV test; (f) has sought and received counseling regarding AIDS; or (g) has been determined to be a person ar risk of being infected with AIDS; and which permits the identification of that person. [OCGA §31-22-9.1].

POLICY

The laws of the State of Georgia provide additional protections above and beyond those set forth in HIPAA regarding the Use and Disclosure of PHI that also constitutes AIDS Confidential Information. Accordingly, in the case of PHI that also constitutes AIDS Confidential Information, a Covered Component of the Emory University Hybrid Covered Entity shall not make any Use or Disclosure of such PHI that also constitutes AIDS Confidential Information unless that Use or Disclosure is permitted both by HIPAA and applicable Georgia law. A summary of the parameters of Georgia law regarding permissible Use and Disclosure of PHI that also constitutes AIDS Confidential Information are set forth below under Procedure.

PROCEDURE

General Rule Under Georgia Law Regarding Use and Dislcosure of AIDS Confidential Information

A person or entity that receives AIDs Confidential Information pursuant to OCGA §24-12-21 or that is responsible for recording, reporting or maintaining AIDS Confidential Information shall not:

(a) Intentionally or knowingly Disclose the AIDS Confidential Information to another person or entity except as permitted under OCGA §24-12-21;
(b) Be compelled by subpoena, court order or other judicial process to Disclose AIDS Confidential Information to another person or legal entity; and
(c) Intentionally or knowingly re-Disclose, or be compelled by subpoena, court order or other judicial process to re-Disclose, to any person or

entity AIDS Confidential Information received in violation of paragraphs (a) and (b) above.

Summary of Permissible Uses and Disclosures of AIDS Confidential Information under OCGA §24-12-21

The following is a summary of the Uses and Disclosures of PHI that also Constitutes AIDS Confidential Information that are permitted under OCGA §24-12-21. **The Emory University Office of the General Counsel must be contacted for specific information regarding the scope and applicability of these provisions, as well as guidance regarding the any specific manner in which the Disclosure must/may be made/received pursuant to OCGA §24-12-21**:

Disclosure to Person Identified by the AIDS Confidential Information: AIDS Confidential Information shall be Disclosed to the person identified by that Information. If the person so identified is incompetent, then the Information shall be disclosed to that person's legal guardian. The Information also may be Disclosed to a minor's parent or legal guardian.

Disclosure Pursuant to Written Authorization: AIDs Confidential Information shall be Disclosed to any person or legal entity designated in an Authorization signed by the person who is identified by the Information, or legal guardian if the person is incompetent, or legal guardian or parent if the person is a minor and the laws of the State of Georgia do not otherwise permit the minor to authorize a Disclosure. In this respect, a Covered Component must contact the Emory University Office of the General Counsel prior to permitting a Minor to sign an Authorization for the Disclosure of AIDS Confidential Information.

Disclosure to a Government Agency: AIDS Confidential Information shall be Disclosed to any agency or department of the federal government, the State of Georgia, or any political subdivision of the State of Georgia if the Information is authorized or required by law to be reported to that agency or department and all requirements of any HIPAA regulations or policies pertaining to such disclosure are met. See, e.g., *Policy D.6, HIPAA Policy Regarding Use and Disclosure of PHI for Public Health Activities and Workplace Surveillance Related Activities, and Student Immunizations.*

Disclosure of HIV Test Results: The results of an HIV test shall be Disclosed to the person who is the subject of the test, or that person's designated representative who ordered such test of the body fluids or tissue of another person.

Disclosure to Spouse, Sexual Partner or Child: If a physician determines that his/her patient is infected with HIV and the physician reasonably believes that the spouse, sexual partner or child of the patient, spouse, or sexual partner is a person at risk of being infected with HIV by that patient, the physician may Disclose to that spouse, sexual partner or child that the patient has been determined to be infected with HIV, after first attempting to notify that patient that such a Disclosure will be made and provided that the Disclosure also complies with *Policy D.6, HIPAA Policy Regarding Use and Disclosure*

of PHI for Public Health Activities and Workplace Surveillance Related Activities, and Student Immunizations.

Disclosure to a Department of Public Health: An administrator of a licensed hospital or a physician that has a patient who has been determined to be infected with HIV may Disclose to the Georgia Department of Public Health (a) the name and address of the patient; and (b) that the patient has been determined to be infected with HIV; and (c) the name and address of any other person whom the Disclosing physician or hospital administrator reasonably believes to be a person at risk of being infected with HIV by that patient; provided, that such Disclosure also complies with *Policy D.6, HIPAA Policy Regarding Use and Disclosure of PHI for Public Health Activities and Workplace Surveillance Related Activities, and Student Immunizations.* Additionally, a Health Care Provider or facility shall report to the Georgia Department of Public Health the name and address of a person determined by a HIV test to be infected with HIV pursuant to any regulation for mandatory reporting adopted by the Department; provided, however, that such Disclosure also complies with the aforesaid *Policy D.6.* Reports of positive HIV tests provided by anonymous HIV test sites operated by or on behalf of the Department of Public Health need not be reported.

Disclosure to Health Care Provider or Health Care Facility: A Health Care Provider who is authorized to order an HIV test may Disclose AID Confidential Information regarding a patient who is the subject of the test to a Health Care Provider or Health Care facility that has provided, is providing, or will provide any Health Care service to that patient and as a result of the provision of service, the Health Care Provider or facility (a) has personnel or patients who may be persons at risk for being infected with HIV by that patient, if the patient is HIV infected and the Disclosure is reasonably necessary to protect the personnel or patients who are are at risk; or (b) the Health Care Provider or facility have a legitimate need for the information in order to provide Health Care service to the patient. Provided, however, that any such Disclosure must also comply with *Policy D.6, HIPAA Policy Regarding Use and Disclosure of PHI for Public Health Activities and Workplace Surveillance Related Activities, and Student Immunizations* and/or *Policy C.1, HIPAA Policy Regarding Use and Disclosure of PHI for Treatment, Payment and Healthcare Operations.*

Other Disclosures Permitted Pursuant to OCGA §24-12-1: OCGA §24-12-1(s) sets forth additional circumstances in which AIDs Confidential Information may be Disclosed without Authorization from the person who is the subject of the Information (e.g., Disclosure pursuant to a court order, as authorized or required by law, in connection with a claim filed by an Individual, etc.). **A Covered Component MUST consult the Emory University Office of the General Counsel prior to making any such Disclosure without Authorization to ensure that the Disclosure complies with both the requirements of OCGA §24-12-1 and any applicable HIPAA provisions**.

APPLICABILITY OF MINIMUN NECESSARY RULE AND ACCOUNTING RULE

Minimum Necessary Rule: If a Disclosure is made pursuant to law and without Authorization, only the type and amount of PHI permitted by the applicable law may be Disclosed. In cases in which the applicable law does not specify the type or amount of PHI to be Disclosed, only the type and amount of PHI necessary to carry out the purpose of the Disclosure may be Disclosed.

Accounting Rule: The Covered Component shall keep a record of any Disclosures made pursuant to this policy except for those made pursuant to Authorization or for Treatment purposes. This information shall be available to any Individual who is the subject of such a Disclosure and who requests an accounting of such a Disclosure. Records regarding such Disclosures shall be kept for at least 6 years after the date of the Disclosure.

SPECIAL GEORGIA STATE LAW REQUIREMENTS REGARDING CERTAIN TYPES OF PHI
In some instances, the laws of the State of Georgia afford additional confidentiality protections regarding the Use and Disclosure of certain types of of PHI. These types of PHI include communications with licensed mental health care providers, confidential raw research data, information concerning HIV/AIDs status, or certain Disclosures to funeral directors, law enforcement officials or for judicial/administrative proceeding. If the PHI being Disclosed or the type of Disclosure falls into any of the foregoing catetogies, please consult the following policies as appropriate: *Policy D.2, HIPAA Policy Regarding Use and Disclosure of PHI of Deceased Individuals and Special HIPAA Rules Regarding Coroners, Medical Examiners, Funeral Directors, Tissue/Cadaver Donation and Research Using Deceased Individual's Information*; *Policy D.12, HIPAA Policy Regarding Disclosure of PHI for Judicial and Administrative Proceedings*; *Policy D.13, HIPAA Policy Regarding Disclosures of PHI for Law Enforcement Purposes*; *Policy D.15, Policy Regarding Use and Disclosure of Psychotherapy Notes and Mental Health Information*; *Policy D.17, Special Rule Regarding Confidentiality of Raw Research Data*; and *Policy E.3, AIDS Confidential Information.*

REFERENCES: OCGA §§24-12-21, 31-22-9.1
DATE OF POLICY: April 2003
REVISED: September 1, 2016