COLUMBIA UNIVERSITY

INSTITUTIONAL REVIEW BOARD

POLICY ON THE PRIVACY RULE AND THE USE OF HEALTH INFORMATION IN RESEARCH

I. Background

The Health Insurance Portability and Accountability Act of 1996 (as amended from time to time, **HIPAA**) required the creation of regulations for the protection of health information. These regulations, commonly referred to as the "Privacy Rule", became effective in 2003 and are codified in Title 45 of the Code of Federal Regulations, Part 160 and Subparts A and E of Part 164 (the **Privacy Rule**). While the main impact of the Privacy Rule is on uses and disclosures of, and the provision of individual rights with respect to, health information obtained in the provision of clinical health care services, the Rule also affects the use and disclosure of certain health information in connection with research.

There are two categories of health information: (1) **Individually Identifiable Health Information** or **IIHI** and (2) **Protected Health Information** or **PHI,** a subset of IIHI (as such terms and certain other terms used in this Policy are defined in Section III). The Privacy Rule provides that PHI may be Used or Disclosed to others only in certain circumstances or under certain conditions. With certain exceptions, the Privacy Rule applies only to PHI transmitted or maintained by a Covered Entity.

The Privacy Rule permits a Covered Entity that performs both Covered and non-Covered Functions as part of its business operations to elect to be a Hybrid Entity. To become a Hybrid Entity, the Covered Entity must designate and include in its Health Care Component all components that would meet the definition of a Covered Entity or a Business Associate if that component were a separate legal entity. Columbia University (**Columbia** or the **University**) is a Covered Entity that performs both Covered and non-Covered Functions and has elected to be a Hybrid Entity.

Only the Health Care Component of a Hybrid Entity is subject to HIPAA. The University has designated as its Health Care Component (the **Columbia Health Care Component)** CUMC and the other colleges, schools, departments and offices of the University to the extent that they (1) provide treatment or health care services and engage in Covered Transactions electronically or (2) receive PHI to provide a service to, or perform a function for or on behalf of, the Columbia Health Care Component.

Guidance by the U.S. Department of Health and Human Services **(HHS)** with respect to research provides that only those components of a Hybrid Entity that conduct research that involves Covered Transactions must be included in the Health Care Component. By virtue of the

University's designation of the Columbia Health Care Component, most research activities at the University have been excluded from the Columbia Health Care Component and are therefore not subject to HIPAA. This Policy describes the circumstances under which research is subject to the requirements of HIPAA.

II. Policy History

This Policy became effective as of November 1, 2017 and was amended as of January 22, 2017.

This Policy replaces the following University Policy:

- Columbia University Institutional Review Board Policy on Research and the HIPAA Privacy Rule, effective April 28, 2008

and the following CUMC Policies:

- Columbia University Medical Center Institutional Review Board Procedures to Comply with Privacy Laws that Affect Use and Disclosure of Protected Health Information for Research Purposes, dated April 21, 2008.
- Columbia University Medical Center Policy: Research and HIPAA Clinical and Medical Records, dated December 2003, and amended in October 2007 and December 2009.

This Policy does not supersede the Office of HIPAA Compliance's policy entitled "Authorization to Disclose Patient Information—Patient Access—Use and Disclosure of Medical Information", dated May 2008 and amended in September 2013, except for the provisions therein relating to research, which are replaced by this Policy.

III. Definitions

As used in this Policy, certain terms are defined as follows; references to section numbers herein refer to sections of the Privacy Rule:

Business Associate: a person who creates, receives, maintains or transmits PHI on behalf of, or provides services to, a Covered Entity, as more particularly described in Section 160.103.

Columbia or the **University:** as defined in Section I.

Columbia Health Care Component: as defined in Section I.

Columbia Health Care Component Workforce: all members of the University Workforce whose conduct, in the performance of work or study at the University, is under the direct control of the Columbia Health Care Component, whether or not they are paid by the Columbia Health Care Component.

Covered Entity: a (1) health plan, (2) health care clearinghouse or (3) a Covered Health Care Provider, as more particularly described in Section 160.103.

Covered Function: those functions of a Covered Entity the performance of which makes the entity a health plan, a health care clearinghouse or a Covered Health Care Provider.

Covered Health Care Provider: a health care provider that transmits any health information in electronic form in connection with a Covered Transaction.

Covered Transaction: an electronic financial or administrative transaction for which HHS has developed standards under the HIPAA Transactions and Code Sets Regulations, as more particularly described in Section 162.

CUMC: Columbia University Medical Center, which is comprised of the College of Physicians and Surgeons, the Mailman School of Public Health, the School of Nursing and the College of Dental Medicine.

CUMC/Hospital OHCA: the OHCA of which CUMC, NewYork-Presbyterian Hospital and Weill Cornell Medical College are members.

Disclosure: with respect to PHI, the release or transfer of PHI to, or the provision of access to such PHI by, a person or entity outside of the entity holding the PHI.

Electronic Health Record: information with respect to the Health Care of an individual that is recorded in an electronic health information system maintained by the Columbia Health Care Component or the CUMC/Hospital OHCA.

Health Care: the care, services or supplies relating to the health of an individual, including, without limitation, (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, and counseling, service, assessment or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body and (2) the sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

HHS: as defined in Section I.

HIPAA: as defined in Section I.

HIPAA Data Use Agreement: a data use agreement relating to a HIPAA Limited Data Set that meets the requirements of Section160.514(e)(4)**.**

HIPAA Limited Data Set: PHI that excludes the following direct identifiers of an individual or his/her relatives, employers or household members:

- Names (including initials);
- Postal address information, other than town or city, state and zip code;
- Telephone numbers;
- Fax numbers;

- Email addresses;
- Social security numbers (including partial social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- URLs;
- IP address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full-face photographic images and any comparable images,

as more particularly described in Section 164.514(e)(2).

HIPAA Rules: the HIPAA Privacy, Security and Breach Notifications and Enforcement Rules (45 CFR Parts 160 and 164), as amended from time to time.

HRPO: the University's Human Research Protection Office.

Hybrid Entity: a single legal entity (1) that is a Covered Entity, (2) whose business activities include both Covered and non-Covered Functions and (3) that designates health care components within the Hybrid Entity, as more particularly described in Section 164.103.

Individually Identifiable Health Information or IIHI: any information (including demographic and genetic information) created or received by the University or a member of the University Workforce that relates to (1) the past, present or future physical or mental health or condition of an individual, (2) the provision of Health Care to an individual or (3) the past, present or future payment for the provision of Health Care to an individual and either (a) identifies the individual or (b) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

IRB: one or more of the University's Institutional Review Boards.

LDS Identifiers: the direct identifiers listed in the definition of HIPAA Limited Data Set.

OHCA: an Organized Health Care Arrangement, which is an arrangement or relationship recognized in the HIPAA Rules that allows two or more Covered Entities that hold themselves out to the public as participating in a joint arrangement and participate in certain joint activities to share PHI for joint health care operations purposes.

Privacy Rule: as defined in Section I.

Protected Health Information or **PHI:** IIHI that is transmitted or maintained by the Columbia Health Care Component in electronic or any other form or medium, **except** (1) as provided in the definition of Protected Health Information in Section 160.103 or (2) RHI.

Research Health Information or RHI: IIHI that (1) is created or received in connection with research that does not involve a Covered Transaction or (2) although previously considered PHI, has been received in connection with research pursuant to a valid HIPAA authorization or IRB waiver of HIPAA authorization.

University Workforce: all faculty and other employees, volunteers, trainees and students of the University whose conduct, in the performance of work or study at the University, is under the direct control of the University, whether or not they are paid by the University.

Use: with respect to PHI, the creation, sharing, employment, application, storage, utilization, examination or analysis of such PHI within an entity that maintains such PHI.

IV. Scope of Policy

This Policy applies Universitywide and to anyone who is a member of the University Workforce. All members of the University Workforce must comply with this Policy to the extent applicable and with the other University policies relating to human subjects research, including the maintenance of privacy and confidentiality of research participants and the security of sensitive data.

V. Categories of Research Data

It is the University's policy, in accordance with HIPAA, that with respect to research data, only such data that are **PHI** are protected by the Privacy Rule. All other health related research data are considered to be **RHI** and are not protected by the Privacy Rule. It is therefore important for researchers to understand the distinction between research data that is PHI and research data that is RHI.

For purposes of this Policy, data in a research study are only considered to be **PHI** in the following two circumstances:

(1) When the study for which the data are being collected includes electronic billing to a subject's insurer or other third party payer for any research procedure or intervention described in the IRB protocol relating to such study, such as x rays, clinical tests or hospitalization costs, etc. All such data constitute PHI when created, regardless of whether certain individual data were created or obtained without the subject's insurer or other third party payer having been billed for the procedure.
(2) When data to be used in a research study are accessed, obtained or extracted from a subject's Electronic Health Record maintained by the Columbia Health Care Component.

Although the foregoing data is PHI, such data may no longer be considered to be PHI, but may be considered to be RHI and therefore not subject to HIPPA, if both of the following are true:

- The research data are obtained in compliance with the Privacy Rule (e.g., pursuant to a HIPAA authorization or an IRB waiver of authorization; and
- The research data are maintained in a research record that is separate from the subject's Electronic Health Record or other health record.

As a result, no HIPAA authorization or IRB waiver of authorization is required prior to using or sharing the RHI with any other person, whether or not such person is a member of the Columbia Workforce. In addition, the RHI will not be subject to the requirements of Section VI of this Policy.

Please note that if the costs of all procedures described in the IRB protocol relating to a study are to be covered by the sponsor of the study, whether directly or through the researcher, none of the data obtained in the course of the study are considered to be PHI, so long as they are not extracted from or maintained in the subject's Electronic Health Record or other health record.

As provided in Section VII below, the use, transmission and storage of information in electronic form is subject to the University's Information Security Policies and if such information is deemed to be Sensitive Information, whether or not it constitutes PHI, it must be protected in compliance with such Policies.

If research data are deemed to be PHI, all of the provisions of Section VI of this Policy are applicable to the Use and Disclosure of such data.

In order to assist the research community in understanding the distinction between RHI and PHI, Appendix A to this Policy describes a number of illustrative scenarios.

Please note that the University's Office of HIPAA Compliance, in consultation with the Office of the General Counsel, is responsible for determining whether particular information created, maintained, processed or transmitted by the Columbia Health Care Component constitutes PHI.

VI. Provisions Relating to Research Data That Are PHI

This Section VI only relates to research data that are PHI and not RHI.

The Columbia Health Care Component may Use or Disclose PHI for research under the following circumstances and conditions:

- If the subject of the PHI has granted specific written permission through an Authorization;
- If the Columbia Health Care Component receives appropriate documentation that the IRB has granted a waiver of the Authorization requirement;
- If the Columbia Health Care Component obtains documentation of the IRB's alteration of the Authorization requirement as well as the altered Authorization;
- For reviews preparatory to research, including the Use of PHI by a researcher to identify the Health Care provider at Columbia through whom a patient may be contacted for research participation, provided that (1) certain representations required by this Policy are

obtained from the researcher and (2) such PHI is Used only within the Columbia Health Care Component;

- For research solely on decedents' information with certain representations and, if required, documentation obtained from the researcher that satisfies the provisions of 164.512(i)(1)(ii);
- If the PHI has been de-identified in accordance with the standards required by this Policy;
- If the information is released outside the Columbia Health Care Component in the form of a limited data set, with certain identifiers removed and with a data use agreement between the researcher and the University when a waiver of authorization has not been granted by the IRB; or
- If prior to April 14, 2003, the Columbia Health Care Component received from an individual (1) an authorization or other express legal permission or (2) informed consent of the individual to participate in the research or a waiver of informed consent for the research was granted by the IRB.

As a general rule, when Using or Disclosing PHI or when requesting PHI from another Covered Entity, the Columbia Health Care Component must make reasonable efforts to limit such PHI to the minimum necessary to accomplish the intended purpose of the Use, Disclosure or request.

Each of these circumstances and conditions, and the requirements for the approval of such circumstances and conditions, with respect to the Columbia Health Care Component are described in more detail below.

A. Authorization to Use and Disclose PHI

A researcher may conduct research using an individual's PHI if he/she obtains a written, signed Authorization to Use and/or Disclose such PHI (an **Authorization**) for the purposes and to the recipients described in such Authorization. A valid Authorization must meet the following standards:

- **Content of Authorization.** The content of the Authorization must include the following core elements:
    - A description of the PHI to be Used or Disclosed that identifies the information in a specific and meaningful fashion;
    - The name or other specific identification of the person(s), or class of persons, authorized to perform or make the requested Use or Disclosures;
    - The name or other specific identification of the person(s), or class of persons, to whom the requested Use or Disclosure may be made;
    - A description of each purpose of the requested Use or Disclosure. An Authorization for Use and Disclosure of PHI for future research purposes must adequately describe such purposes such that it would be reasonable for the individual to expect that his/her PHI could be Used or Disclosed for such future research. A description of the PHI to be used for future research may include information collected beyond the time of the original study. Further, since the Authorization requirements allow a "class of

persons" to be described for purposes of identifying the recipients of the PHI, researchers have flexibility in the manner in which they describe the recipients of the PHI for future research, so long as it is reasonable from such description to believe that the individual would expect his/her PHI to be shared with such persons for future research;

  - An expiration date or an expiration event that relates to the individual or the purpose of the Use or Disclosure. The statement "end of research study" or "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 repository; and
  - The signature of the individual and the date of execution of the Authorization. If the Authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

- **Required Statements.** The Authorization must contain statements adequate to place the individual on notice of all of the following:

  - The individual's right to revoke the Authorization in writing, a description of how to revoke and the exceptions to the right to revoke;
  - The ability or inability to condition treatment, payment, eligibility or enrollment for benefits on the authorization, if any; and
  - The potential that the PHI disclosed pursuant to the Authorization may be subject to further disclosure by the recipient and may no longer be protected by the Privacy Rule.

The Authorization, which may be separate from or embedded in an informed consent form, must be written in plain language and a copy must be provided to the individual.

An Authorization for a research study may be combined with any other written permission for the same or another research study, including an informed consent form to participate in the research or for the creation and maintenance of a research database or repository. When the provision of research-related treatment (i.e., in a clinical trial) is conditioned on one of the authorizations in the combined Authorization, the Authorization must clearly differentiate between the conditional and unconditional components (i.e., collection of specimens for a central repository) and provide the individual with an opportunity to opt in to the research activities described in the unconditional Authorization. A combined Authorization may not provide that the individual can "opt out" of the unconditional research activities; the individual must "opt in" to such activities.

At Columbia, an Authorization can be obtained in one of two ways: either by the use of (1) a HIPAA Form A or (2) a Combined Consent and HIPAA Authorization Form.

There are two versions of the HIPAA Form A: one, entitled "Clinical Research Authorization for Sponsored Research", for research that has an external sponsor who will be receiving PHI, and the other, entitled "Clinical Research Authorization for Non-Sponsored Research", for studies without an external sponsor. The HIPAA Form A must be signed by the individual who is

granting the authorization. Rascal includes both English and Spanish versions. Copies of the two HIPAA Forms A (English version only) are attached to this Policy as Annexes 1-A and 1-B. For languages other than English or Spanish, the authorization must be translated. Use of a combined consent and authroizatioin form in such situations will reduce the number of documents to be translated.

Except as provided below, HIPAA Forms A are submitted in Rascal and are reviewed and approved by the HRPO.

An Authorization may (but is not required to) be submitted in a Combined Consent and Authorization Form. Sample authorization language that can be incorporated into consent forms has been posted on the HRPO website at http://research.columbia.edu/irb/.
The IRB must review and approve the Authorization language when it is included in the consent form.

B. Waiver or Alteration of the Authorization Requirement

When it may not be feasible for the researcher to obtain a signed Authorization for all PHI to be used in a research study, the researcher may seek a waiver of Authorization from the IRB. A waiver of authorization may only be approved by the Columbia IRB if the data were created at or by the Columbia Health Care Component, unless Columbia is serving as the single IRB for a multi-site study and has been designated as the Privacy Board for the external site(s).

For research Uses and Disclosures of PHI, the IRB may approve a waiver or an alteration of the Authorization requirement in whole or part. A complete waiver occurs when the IRB determines that no Authorization will be required for PHI to be Used or Disclosed for a particular research project. A partial or "recruitment" waiver of Authorization occurs when the IRB determines that an Authorization is not needed for certain Uses and Disclosures of PHI, such as Use and Disclosure by a researcher to contact a prospective subject with whom the researcher does not have a prior relationship or to conduct screening procedures.

The IRB may approve a waiver of the Authorization requirement, in whole or in part, only if it determines that:

- The proposed use or disclosure of PHI involves no more than minimal risk to the participants' privacy, based on the presence of at least the following elements:
    - An adequate plan to protect identifiers to be used in the research from improper Use and Disclosure; and
    - An adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research (unless there is a health or research justification for retaining the identifiers, or if retention is otherwise required by law);
- Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity except as required by law, for authorized oversight of the research, or for other research for which the Use or Disclosure would be permitted;

- The proposed research could not practicably be conducted without the waiver or alteration; and
- The proposed research could not practicably be conducted without access to and use of the PHI.

For a Use or Disclosure to be permitted based on documentation of approval of a waiver or alteration, the documentation must include all the following:

- The identification of the IRB and the date on which the waiver or alteration of Authorization was approved;
- A statement that the IRB has determined that the waiver or alteration satisfies the criteria set forth above;
- A brief description of the PHI for which Use or access has been determined to be necessary by the IRB; and
- A statement that the waiver or alteration of Authorization has been reviewed and approved by the IRB.

For multi-site studies, the Columbia Health Care Component may reasonably rely upon a researcher to obtain the documentation that a waiver or alteration was properly granted by a single IRB, even if that IRB is not affiliated with the Columbia Health Care Component.

At Columbia, in order for the IRB to review and approve a waiver or alteration of Authorization, the researcher must submit a HIPAA Form B: Application for Waiver of Authorization. The Application requires a description of the nature and scope of the PHI to which access is sought and contains the certifications to be made by the researcher. A copy of Form B is attached to this Policy as Annex 2.

The IRB may also approve a request that removes some, but not all, PHI or alters the requirements for an Authorization. Situations requiring an alteration vary, but most often involve verbal Authorization and use of an information sheet. At Columbia, a HIPAA Form B: Application for Waiver of Authorization, must be submitted to the IRB to request an alteration.

At Columbia, a HIPAA Form C: Requests for Research Recruitment Waiver/Contacting Prospective Study Participants, is used for permission to directly contact potential subjects who are patients without involving the subject's physician or other Health Care provider in the process. It is used only in rare instances when the researcher cannot feasibly involve the physician or health care provider in his/her recruitment efforts (e.g., public health research using PHI of patients with many different providers who cannot all be contacted). The HIPAA Form C requires a description of the nature and scope of the PHI to which access is sought, as well as answers to certain questions and a certification to be completed by the researcher. A copy of the HIPAA Form C is attached to this Policy as Annex 3.

C. Review Preparatory to Research

For activities involved in preparing for research, PHI may be Used by a researcher within the Columbia Health Care Component without an individual's Authorization or a waiver of Authorization. Such activities include determining whether or not there are sufficient potential subjects for a research project or, after development of a protocol, identifying potential subjects. Any preparatory Use or Disclosure of PHI must be prospectively reviewed and approved by the Office of HIPAA Compliance or the HPRO, as indicated in this Policy.

In order for preparatory Use of PHI to be approved, the researcher must represent to the Office of HIPAA Compliance or the HRPO that:

- The Use is requested solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;
- The PHI will not be removed from the Columbia Health Care Component during the review;
- The PHI for which Use is requested is necessary for the research purposes; and
- The PHI that is obtained as part of the request will not be Used in a research study without subsequent Authorization or waiver of Authorization.

At Columbia, a HIPAA Form D: Investigators Certification for Reviews Preparatory to Research is used to determine whether or not there are sufficient potential subjects for a research project. Before doing a search, the researcher must submit a HIPAA Form D in Rascal.

There are two different versions of the HIPAA Form D, one to be attached to a protocol and the other a "stand-alone" version. Generally, the stand-alone version is used when the study is not developed enough to have an IRB protocol and will be approved by the Office of HIPAA Compliance or the HRPO. However, once the researcher has drafted a protocol, the protocol-linked version of HIPAA Form D should be used and must be approved by the HRPO.

Note, however, that it is University policy that, with the exception of the recruitment waiver procedure described in Section C(2) above, a researcher may only contact a potential subject who is a patient through the patient's physician or Health Care provider. Therefore, a HIPAA Form D may only be used when a researcher is not going to use PHI obtained to directly contact the potential subject. The HIPAA Form D requires a description of the nature and scope of the PHI to which, and the purpose for which, access is sought, as well as certain representations to be made by the researcher. Copies of the two HIPAA Forms D are attached to this Policy as Annexes 4-A and 4-B.

D. Research with Decedents' Information

The Columbia Health Care Component must protect the privacy of a decedent's PHI in the same manner and to the same extent that is required for the PHI of living individuals for a period of 50 years following the death of the individual.

To disclose PHI of a deceased individual for research, the Columbia Health Care Component is not required to obtain an Authorization from the personal representative or next of kin, a waiver or alteration of the Authorization or a data use agreement. However, the Columbia Health Care

Component must obtain from the researcher who is seeking access to decedents' PHI the following:

- Oral or written representations that the Use and Disclosure is sought solely for research on the PHI of decedents; and
- Oral or written representations that the PHI for which Use or Disclosure is sought is necessary for the research purposes.

At Columbia, a HIPAA Form E: Investigators Certificate for Research with Decedents Information, must be submitted in Rascal for review and approval prior to accessing any PHI. There are two different versions of the HIPAA Form E, one to be attached to a protocol when use of decedent information is a component of a protocol that involves other research procedures and the other a stand-alone version that is used when an IRB protocol is not required. The former HIPAA Form E must be approved by the HRPO, while the latter Form must be approved by the Office of HIPAA Compliance. Copies of the two HIPAA Forms E are attached to this Policy as Annexes 5-A and 5-B.

E. Research with a HIPAA Limited Data Set

The Columbia Health Care Component may use PHI included in a HIPAA Limited Data Set without obtaining an Authorization or documentation of a waiver or alteration of Authorization. The Columbia Health Care Component may Use and Disclose a HIPAA Limited Data Set for research activities conducted by itself, another Covered Entity or a researcher who is not a Covered Entity if the disclosing Covered Entity and the HIPAA Limited Data Set recipient enter into a HIPAA Data Use Agreement.

Note that a HIPAA Limited Data Set is not considered to be de-identified data according to HIPAA standards.

A HIPAA Data Use Agreement is the means by which the Columbia Health Care Component can obtain satisfactory assurances that the recipient of the Limited Data Set will Use or Disclose the PHI in the HIPAA Limited Data Set only for specified purposes.

A HIPAA Data Use Agreement must contain the following provisions:

- Specific permitted Uses and Disclosures of the HIPAA Limited Data Set by the recipient consistent with the purpose for which it was disclosed;
- Identification of who is permitted to Use or receive the HIPAA Limited Data Set; and
- Stipulations that the recipient will:
    - Not Use or Disclose the information other than as permitted by the HIPAA Data Use Agreement or otherwise required by law
    - Use appropriate safeguards to prevent the Use or Disclosure of the information, except as provided for in the HIPAA Data Use Agreement, and require the recipient to report to the Columbia Health Care Component any Uses or Disclosures in violation of the HIPAA Data Use Agreement of which the recipient becomes aware;
    - Hold any agent of the recipient to the standards, restrictions and conditions stated in the HIPAA Data Use Agreement with respect to the information; and

- Not identify the information or contact the individuals.

At Columbia, a HIPAA Form F: HIPAA Data Use Agreement for Disclosure of a HIPAA Limited Data Set for Research Purposes or another form of Data Use Agreement must be attached to a protocol and submitted in Rascal for review when (1) the Columbia Health Care Component will be engaged in the research, (2) the Limited Data Set originates from the Columbia Health Care Component, (3) a waiver of authorization has not been granted and (4) the subject did not provide authorization for the proposed use. Use of the template form in the Rascal IRB module is recommended. If the Columbia Health Care Component is only supplying a HIPAA Limited Data Set for research, and the providing Workforce Member is not otherwise involved in the research, a HIPAA Data Use Agreement is required although submission of a protocol to the IRB may not be required. When the HRPO review of the HIPAA Data Use Agreement is completed, the researcher should forward the Agreement to the intended recipient of the HIPAA Limited Data Set for signature, after which it must be provided to Sponsored Projects Administration or the Clinical Trials Office for review and signature on behalf of the University. A copy of the HIPAA Form F is attached to this Policy as Annex 6.

Note that when it is proposed that a Limited Data Set will be Used within the Columbia Health Care Component, it is the practice of the IRB to grant a waiver of authorization if the waiver criteria are met, rather than requiring the use of a HIPAA Data Use Agreement.

F. Research with De-identified Data

The Columbia Health Care Component may Use or Disclose PHI that is de-identified. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify the individual is not PHI.

There are two methods by which health information can be designated as de-identified:

- **Safe Harbor Method:** the LDS Identifiers as well as the following elements (together, the **HIPAA Identifiers**) regarding an individual or his/her relatives, employers or household members are removed from the information;

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

    - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000

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

- Any other unique identifying number, characteristic or code, unless otherwise permitted by this Policy for re-identification (Section 164.514(b)(2)).

- **Expert Determination Method:** a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable (1) determines that the risk is "very small" that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information and (2) documents such methods and results of the analysis that justify the determination.

De-identified health information created following either of these methods is no longer subject to this Policy because it does not fall within the definition of PHI.

The Columbia Health Care Component may assign to, and retain with the PHI, a code or other means of record re-identification if that code is not derived from or related to information about the individual and is not otherwise able to be translated to identify the individual. For example, an encrypted social security number would not meet the conditions for use as a re-identification code because it is derived from individually identifiable information (see 67 FR 53233 (8/14/01)). In addition, the Columbia Health Care Component may not (1) Use or Disclose the code or other means of record identification for any purpose other than as a means of re-identifying the de-identified data or (2) disclose its method of re-identifying the information (Section 164.514(c)).

At Columbia, in order to Use de-identified data, HIPAA Form G: Certification for Research with De-identified Data must be attached to the protocol and approved by the HRPO. If the data are determined not to be de-identified, the Form G will be returned and the HIPAA form that relates to the applicable permissible method of obtaining PHI (e.g., Authorization, waiver or alteration of Authorization or use of a HIPAA Limited Data Set) that will be requested. The HIPAA Form G requires a certification by the researcher that the data will not include any of the HIPAA Identifiers. A copy of the HIPAA Form G is attached to this Policy as Annex 7.

G. Accounting for Research Disclosures

In general, the Privacy Rule gives individuals the right to receive an account of certain disclosures of PHI made by a covered entity. See 45 CFR 164.528. This accounting must include disclosures of PHI that occurred during the six years prior to the individual's request for an accounting. Exempt from the accounting requirement are research disclosures made pursuant to an individual's authorization and disclosures of a limited data set to researchers with a data use agreement that is compliant with 45 CFR 164.514(e). Disclosures for research purposes that are subject to the accounting requirement include PHI disclosed under an approved waiver of authorization.

When a researcher or his or her designee, as a representative of the Columbia Health Care Component, abstracts PHI directly from the Electronic Health Record, under a waiver of authorization approved by the IRB, he or she must document the PHI that is subsequently

entered as RHI into the research record, in order to be able to respond to any request for an accounting of disclosures.

H. Research Databases and Repositories

There are two separate activities to consider with respect to research databases and repositories: (1) the Use or Disclosure of PHI for creating the database or repository and (2) the subsequent Use or Disclosure of PHI in the database or repository for a particular research protocol.

The Columbia Health Care Component's Use or Disclosure of PHI to create a research database or repository and Use or Disclosure of PHI from the database or repository are each considered a separate research activity. In general, an Authorization is required for each activity, unless, for example, the IRB waives or alters the Authorization requirement. Documentation of a waiver or an alteration of Authorization to use PHI to create a database or repository requires, among other things, a statement that the IRB has determined that the researcher has provided adequate written assurances that data in the database or repository will not be further Used or Disclosed except as described in the waiver request. The use of any permissible method of obtaining PHI (e.g., Authorization, waiver or alteration of Authorization of use of a HIPAA Limited Data Set) results in the data in the database or repository no longer constituting PHI. Depending on the content of the data, the data may be RHI or de-identified data. Subsequent Use or Disclosure of such data obtained for research purposes from a database or repository is not subject to HIPAA.

Note that requests to Use individual patient or electronic health record data from NewYork-Presbyterian Hospital (NYPH), CUMC or Weill Cornel Medical College (WCMC) data storage systems, when a researcher needs assistance to query a system, must be reviewed by the Tripartite Request Assessment Committee (TRAC) of NYPH, CUMC and WCMC prior to its Use. See https:///webapps.nyp.org/trac/.

VII. Information Security

The use, transmission and storage of information in electronic form, including PHI and RHI, is subject to the University's Information Security Charter (http://policylibrary.columbia.edu/information-security-charter) and the information security policies adopted by the University thereunder.

Appendix A

PHI vs. RHI: Illustrative Scenarios

Example One:

Facts: The research consists solely of the analysis of identifiable data obtained from the Columbia or NewYork-Presbyterian Hospital (NYP) Electronic Health Record (EHR) (i.e., identifiers will be maintained in the research record). A waiver of authorization may be requested by the researcher, if the waiver criteria are met, and must be approved by the IRB. There will be no billing for any study procedure described in the protocol.

Conclusion: The waiver of authorization is required to access the data (PHI) in the EHR and copy it for research purposes. The resultant research data (RHI) do not constitute PHI because of the waiver of authorization, provided that the research data are stored separately from the EHR from which the data were copied and other PHI.

A Notice of Privacy Practice does not have to be provided to subjects. The data that are being used already exist in the EHR. The patient would have been given a Notice of Privacy Practice at the time of the first service delivery.

Example Two:

Study procedures consist of the administration of a survey by a CUMC researcher. Identifiable health information is collected through survey responses and researchers have access to the email addresses of respondents. The survey is not directed to patients and patient information is not being used to administer the survey. There will be no billing for any study procedure described in the protocol.

Conclusion: The research dataset does not constitute PHI, provided that the research data (RHI) are stored separately from Columbia/NYP medical records and other PHI. No HIPAA processes/forms are necessary, because no HIPAA Covered Transactions are involved and no PHI is being accessed.

A Notice of Privacy Practice does not have to, and should not, be provided to subjects.

Example Three:

A clinical trial involves no billing to participants because the sponsor is paying for all study procedures. The EHR is not being accessed. Patient information is not being used for recruitment or enrollment.

Conclusion: The research dataset from the clinical trial would not constitute PHI, provided that the research data (RHI) are stored separately from Columbia/NYP EHR and other PHI, because no HIPAA Covered Transactions are involved and no PHI is being accessed. No HIPAA forms are required.

A Notice of Privacy Practice does not have to, and should not, be provided to subjects.

Example Four:

A clinical trial involves billing to participants' health insurance providers or other third party payers for standard of care (SOC) procedures. Costs of procedures that are for research purposes only, i.e., beyond SOC, are covered by the sponsor.

Conclusion: The research involves PHI as a result of the SOC procedures, i.e., those study procedures that subjects would undergo even if they were not enrolled in the study. This is PHI because the subjects' insurers or other third party payers will be billed for the costs of the SOC procedures and thus the research involves a HIPAA Covered Transaction. Subjects will provide authorization, which will allow a copy of the SOC data in the EHR to be used for research. The resultant research data (RHI) do not constitute PHI because of the authorization, provided that the research data are stored separately from the EHR from which the data were copied and other PHI.

A Notice of Privacy Practice must be provided to subjects, if this is the first service delivery to the participant.

Example Five:

Study procedures include extraction of existing data from the CUMC/NYP EHR, various physical exams, and collection of data from protocol required tests such as CT and MRI scans that are ordered for research purposes only and not for SOC purposes. The study is NIH-funded and the costs of all study procedures are covered by the grant.

Conclusion: Subjects will provide authorization, which will allow a copy of the data in the EHR to be used for research. The resultant research data (RHI) do not constitute PHI because of the authorization, provided that the research data are stored separately from the EHR from which the data were copied and other PHI. Data obtained as a result of the tests that are administered solely for research are not PHI because no HIPAA Covered Transaction is involved in creation of those data; billing to a sponsor is not considered to be a HIPAA Covered Transaction. If the test results are routinely entered into the EHR, and must be retrieved from the EHR for research use, the authorization will cover use of the test results.

A Notice of Privacy Practice does not have to be provided to participants. Because the participants have existing patient records in the CUMC/NYP EHR, they would have received a Notice of Privacy Practice at the time of the first service delivery.

Example Six:

Study procedures include extraction of existing data from the CUMC/NYP EHR. The criteria for waiver of authorization are not met, and obtaining authorization is not feasible. Extraction and use of a Limited Data Set (LDS) is an option.

Conclusion: HIPAA allows use of a LDS under certain circumstances, and neither authorization nor a waiver of authorization is required. When a LDS is extracted from an EHR and used or disclosed for research purposes, a Data Use Agreement (DUA) is required. The DUA must be executed between the covered entity whose PHI is being used/disclosed, i.e., the Columbia Health Care Component in this example, and the researcher who is the recipient of the data. The data in a LDS are not considered to be de-identified and therefore constitute PHI, until the data are received by the researcher and stored separately from the EHR, in which case the data are considered to be RHI. However, even if the data are RHI, the data remain subject to the terms of the DUA.

A Notice of Privacy Practice does not have to be provided to participants. Because the participants have existing patient records in the CUMC/NYP EHR, they would have received a Notice of Privacy Practice at the time of the first service delivery.