POLICY STATEMENT

Research subjects have the basic right of privacy with respect to their health information. Privacy of health information is protected by both state and federal laws, including HIPAA and state laws governing sensitive health information. In general, the right to privacy requires that subjects sign a HIPAA authorization prior to access to and/or use of their protected health information ("PHI") in research, unless the IRB finds that the conditions for waiver or alteration of HIPAA authorization have been met.

SCOPE

The requirements of this Policy apply to all employees and other individuals involved in research under the jurisdiction of the Einstein IRB and/or using information about individuals who are or have been patients of Montefiore. The Principal Investigator (PI) maintains ultimate responsibility for compliance with HIPAA and the requirements of this Policy. Access, use and disclosure of PHI is also governed by the privacy and security policies of the institutions where the PHI is maintained.

This Policy covers the following research activities:

1. Activities preparatory to research.
2. Research using deidentified data.
3. Research using or creating PHI about living individuals, either with a HIPAA authorization or with waiver of this requirement by the IRB.
4. Recruitment activities.
5. Research on decedents who have been deceased less than 50 years.
6. Research using a limited data set.
7. Databanks and biorepositories.

DEFINITIONS

A. Deidentified Data: Uncoded health information that cannot be linked back to the subject by the researcher, either directly or indirectly. For information to be considered deidentified, all 18 identifiers (defined below) must be removed. PHI may be permanently deidentified, or the code linking identifiers may be maintained by the institution, but may not be provided to the researchers.
B. **Limited Data Set:** A limited data set is a deidentified data set, except that the following data elements are permitted: zip code, city, and state, date of birth and other dates. If a limited data set is to be used a Data Use Agreement is required. See Section J below.

C. **Data Use Agreement:** An agreement by which the covered entity obtains assurances that the recipient of the limited data set will use or disclose the PHI in the data set only for specified purposes. The agreement is to be submitted to the IRB at the time of IRB submission, and it must contain the following:

1. Specific permitted uses and disclosures of the limited data set by the recipient consistent with the purpose for which it was disclosed.
2. Designation of individuals/entities that are permitted to use or receive the limited data set.
3. Statement that the recipient will:
   a. Not use or disclose the information other than permitted by the agreement or otherwise required by law.
   b. Use appropriate safeguards to prevent any use or disclosure of the information except as provided for in the agreement, and report to the covered entity any uses or disclosures in violation of the agreement of which the recipient becomes aware.
   c. Hold any agent of the recipient (including subcontractors) to the standards, restrictions and conditions stated in the data use agreement with respect to the information.
   d. Not attempt to re-identify the information or contact the individuals.

D. **Minimum Necessary Rule:** HIPAA requires that only the minimum necessary PHI should be used unless the use or disclosure is for treatment, or unless the use or disclosure is made subject to a HIPAA authorization. For research subject to a waiver of HIPAA authorization, the minimum necessary standard requires researchers to limit access to only the PHI needed to accomplish the intended purpose of the research as described in the protocol.

E. **Protected Health Information (PHI):** Individually identifiable health information created or received by a HIPAA covered entity. Health information includes any information, whether oral or recorded in any form (including electronic), that 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 of health care to an individual.

PHI is considered individually identifiable if it includes one or more of the following 18 identifiers:

1. Names
2. All geographic subdivisions smaller than a State, including:
   - street address
   - city
   - county
   - precinct
   - zip codes and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly-available data from the Bureau of the Census: (1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

3. Telephone numbers
4. Fax numbers
5. E-mail addresses
6. Social Security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. All elements of dates (except year) for dates related to an individual, including:
    - birth date
    - admission date
    - discharge date
    - date of death
    - 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
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying numbers, characteristics, or codes

PROCEDURES

ALL PROPOSED RESEARCH REQUIRES REVIEW BY THE IRB TO DETERMINE IF RESEARCH IS EXEMPT OR QUALIFIES FOR EXPEDITED OR FULL REVIEW, AND TO DETERMINE WHETHER THE REQUIREMENTS FOR HIPAA AUTHORIZATION MAY BE WAIVED OR ALTERED.

A. Activities Preparatory to Research:

1. The PIs or designee may review medical records (written or electronic) in the course of preparation of a research protocol. The following requirements must be met:

   a. Use or disclosure is sought solely to review health information as necessary to prepare a research protocol or for similar purposes preparatory to research. This is limited to the review of data to assist in formulating a hypothesis, determining the feasibility of conducting the study, determining cell size, or other similar uses that precede the development of an actual protocol.

   b. No PHI is to be removed, copied or included in any notes by the researcher in the course of the review. Summary data (e.g., number of individuals with a certain disease) may be written down and removed. PHI may not be used to identify potential research subjects by name or by any other identifier under HIPAA.
c. The health information for which use or access is sought is necessary for the research purposes.

2. The PI is required to provide written assurance to the holder of the PHI that the review of the PHI is necessary to prepare a research protocol and that the PHI will not be removed by the researcher from the entity. No further review or approval is required.

B. Use of Deidentified Data:

Research using data that are deidentified, and for which the research team does not possess any code or other information that would enable reidentification, does not require a HIPAA authorization as long as all 18 identifiers have been removed. The PI is responsible for obtaining a prior written determination from the IRB that the research is “exempt.”

C. Research under a Participant’s HIPAA Authorization

In most research, as determined by the IRB, the PI is required to obtain the subject’s written HIPAA authorization. For adult subjects who lack decision-making capacity and for minor subjects (enrollment of adults who lack capacity and minors must be approved by the IRB in advance), an individual with legal authority to act on behalf of the subject must sign the HIPAA Authorization (see Einstein IRB Policies “Subjects with Diminished Capacity to Consent” and “Enrollment of Minors in Research – Principles and Guidelines.”)

The written authorization must include:

a. A specific description of what PHI will be accessed, used, or disclosed.
b. The names of persons or organizations who may use or disclose PHI.
c. The names of persons or organizations to whom PHI will be disclosed.
d. A description of the purpose of the use/disclosure.
e. A statement of how long the use or disclosure will continue (no expiration date is permitted for research purposes, however this must be specifically stated in the authorization form and justification must be noted in the protocol).
f. A statement that the authorization may be revoked by the subject, and any exception to the right to revoke (i.e. whether previously collected data can be removed once the subject has been enrolled).
g. A statement that the PHI may no longer be protected by HIPAA and may be subject to redisclosure.
h. A notice of the covered entity’s ability or inability to condition treatment (including research-related treatment), payment or enrollment on the authorization.
i. The individual’s signature and date.

Permissible uses and disclosures are limited to those described in the HIPAA Authorization. If a researcher needs to disclose PHI to a person or organization not listed in the HIPAA Authorization, the researcher must obtain another written authorization from the subject or apply to the IRB for a waiver of authorization.
D. **Compound Authorizations**

The informed consent and HIPAA Authorization forms can be combined for the same study, e.g., for a single research purpose, into what is referred to as a “Compound Authorization.” In research involving psychotherapy notes, the authorization may not be combined with any other permission. Although use of a compound authorization is typical, the two documents are not required to be combined and in some cases the IRB may approve the use of two separate documents.

The PI/sponsor may condition the provision of research-related treatment on obtaining the individual’s authorization for the use or disclosure of PHI for such research. Permitting the use of PHI is part of the decision to receive care through a clinical trial, and PIs are able to condition research-related treatment on the individual’s willingness to authorize the use or disclosure of PHI for the research study.

In some circumstances, research may include both treatment as part of a clinical trial and banking of tissue and associated PHI. The patient may be required to sign an authorization for use of his/her PHI as a condition of receiving the research related treatment (a “conditioned authorization”), but is free either to sign or to decide not to sign the tissue and data banking authorization (“unconditioned authorization”). In such circumstances, the compound authorization must differentiate between the “conditioned” and “unconditioned” components, and the individual must have the opportunity to opt into the unconditioned element of research (note that opt out is not permitted). The purpose of this requirement is to ensure that individual understand that they may decline the activity described in the unconditioned authorization, yet still receive the treatment, services or benefits outlined in the conditioned authorization.

The Einstein IRB HIPAA Authorization Form has been designed to incorporate the required language. Investigators need only specify on the form to whom and where PHI will be sent and what type of PHI will be disclosed.

Disclosures of PHI made in connection with research conducted pursuant to a signed authorization do not need to be tracked for purposes of responding to an individual who requests an accounting of disclosures (see Accounting of Disclosures below).

E. **Waiver of the Requirement for a HIPAA Authorization:**

If certain requirements are met, the PI may request, and the IRB may grant, a waiver of the requirement for a HIPAA authorization. A waiver of authorization is permitted only when the following conditions exist:

- a. The research could not be practically conducted without the waiver.
- b. The research could not be practically conducted without access to and use of PHI.
- c. A written assurance is submitted to the IRB stating that the PHI will not be re-used or disclosed except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by HIPAA.
d. Uses and disclosures of PHI will be limited to the minimum necessary standard.
e. Disclosure involves no more than minimal privacy risk to the individuals.

The PI can request a waiver of authorization by completing the appropriate section of the IRB application. The following must be clearly articulated in the protocol and/or application:

a. Why the research could not practicably be conducted without the waiver.
b. Why the research could not be practicably conducted without access to and use of the PHI.
c. A written assurance to the IRB that the PHI will not be re-used or disclosed except as required by law, for authorized oversight of the research, or for other research.
d. A statement regarding what PHI will be used and disclosed and that the PHI is limited to the “minimum necessary” standard.
e. A statement that the disclosure involves no more than minimal privacy risk to the individuals.
f. A description of the plan to protect identifiers (e.g. the records will be secured in a locked file cabinet, identification of the limited number of individuals who will have access to the data, encryption of records, use of codes, etc.).
g. A description of the plan to destroy the identifiers as soon as possible.
h. A description of the plan to track disclosures.

The criteria for waiver are very similar to those for waiving informed consent. Therefore if the research plan includes obtaining informed consent from subjects, it is not likely that a waiver of HIPAA authorization will be granted.

Disclosures of PHI that are made in connection with research conducted pursuant to a waiver of HIPAA Authorization must be tracked in order to respond to individuals who request an accounting of disclosures of their PHI (see Section L below). It will be the responsibility of the PI to track such disclosures.

F. Recruitment Activities:
The rules governing activities preparatory to research also apply to recruitment activities. This provision would allow a PI to identify prospective research subjects for purposes of seeking their authorization to use or disclose PHI for a research study. PIs and providers may discuss the option of enrolling in a study without first obtaining a HIPAA Authorization, and without IRB waiver of the authorization. The IRB must find that the following requirements are documented in the protocol:

a. Use or disclosure is sought solely to review health information as necessary to determine the eligibility of potential subjects.

b. No PHI is to be removed, copied or included in any notes by the researcher in the course of the review. If an outside researcher who is not part of Montefiore or Einstein plans on enrolling subjects, the researcher
may not be granted access to any PHI unless the IRB has granted waiver of the authorization requirement for recruitment purposes only.

c. The health information for which use or access is sought is necessary for the recruitment activities.

The PI is required to provide written assurance to the holder of the PHI that the review of the PHI is necessary for recruitment activities, and that the PHI will not be removed by the researcher from the entity.

In all studies, written IRB approval must be obtained in advance of any subject contact. On a case by case basis, the IRB should consider whether the following additional requirements must be included in the protocol for initial contact of subjects (when the investigator is not part of the treatment team):

1. The PI or designee must contact each subject’s treating physician, explain the study to him/her, and request that he/she assist in the recruitment of the patient into the study.

2. The initial recruitment contact with the subject must be made by a member of the subject’s treatment team and not by the PI or a member of the research team. If the subject’s physician is not available, contact shall be made by the Chairman or Chief of Service of that department or his/her designee.

3. If the patient’s treating physician agrees to assist in the recruitment process, the protocol submission to the IRB must include a proposed recruitment letter for review and approval by the IRB that will be signed by the potential subject’s physician.

4. The PI may send the letter (signed by the subject’s physician and approved by the IRB) to the potential subject seeking his/her participation in the study. Information on the envelope should be limited to the name of the institution and should not include reference to the department.

5. The letter to potential subjects must contain the following elements: (i) the nature of the research; (ii) the fact that participation is voluntary; (iii) the patient’s medical care will not be affected if he/she decides not to participate; (iv) a description of who will contact the potential subject and how contact will be made (e.g. by phone, letter, etc); (v) a phone number the potential subject should call, or a postcard to be returned, if he/she is not interested and does not want to be contacted; (vi) disclosure that the patient’s medical information is known to the researcher.

6. The letter to the potential subjects may not contain the following information: (i) the patient’s diagnosis; (ii) the disease category of the study; (iii) any information from which the reader could learn any health information about the potential subject.
Research on Decedents:

1. The health information of individuals who have been deceased for more than 50 years is not subject to the HIPAA requirements.

2. HIPAA requires that researchers who wish to access PHI of decedents who have been deceased less than 50 years for research purposes first make certain representations to the holder of the PHI. For subjects who have been deceased less than 50 years, the PI must first represent that the use or disclosure of PHI is solely for research on the PHI of decedents. The PI may not use the PHI of the decedent to obtain information about a decedent’s living relative(s). A PI may request a decedent’s medical history for an outcome study relating to treatment previously administered to the decedent. The PI must also provide written assurances that the PHI is necessary for the research. The holder of the PHI has a right to require documentation of death of the individuals about whom information is being sought.

G. Review of PHI Maintained in Electronic Medical records: With respect to access to electronic PHI, the research team must follow the requirements of the institution that maintains the PHI electronically.

H. Access to or Disclosure of Health Information in Connection with Quality Assurance / Quality Improvement Activities:

Access to or disclosure of health information in connection with bona fide quality assurance and/or quality improvement activities of the institution is not subject to IRB oversight. Approval must be obtained from the institution’s or department’s Quality Improvement process.

I. Limited Data Sets

Some studies may need some limited identifiers and thus not meet the definition of “de-identified data” but nonetheless hold only minimal potential for identifying participants based on the data set. In such circumstances, HIPAA permits use of a “limited data set” for research purposes. A limited data set is PHI that excludes “direct identifiers” of the individual, relatives of the individual, employers, or household members.

A limited data set must exclude:

<table>
<thead>
<tr>
<th>1. Names</th>
<th>8. Account Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Street Addresses</td>
<td>9. Certificate/Licenses Numbers</td>
</tr>
<tr>
<td>3. Phone and Fax Numbers</td>
<td>10. Vehicle Identifiers/license Plates</td>
</tr>
<tr>
<td>4. Email Addresses</td>
<td>11. Device Identifiers</td>
</tr>
<tr>
<td>5. Social Security Numbers</td>
<td>12. Web URLS</td>
</tr>
<tr>
<td>6. Medical Record Numbers</td>
<td>13. Internet Protocols (IP)</td>
</tr>
<tr>
<td>7. Health Plan Numbers</td>
<td>14. Full Face Photo</td>
</tr>
</tbody>
</table>

A limited data set may include one or more of the following:

1. Town
2. City
3. State
4. Zip Code and their equivalent geocodes. (Note the zip code cannot be used if the area composing the zip code has less than 20,000 citizens.)
5. Dates including birth and death
6. Other unique identifying numbers, characteristics, or codes that are not expressly excluded. (Medical record numbers and pathology numbers are excluded.)
7. Relevant medical information

A limited data set may only be used for purposes of research, public health, or health care operations. It may only be used if the covered entity providing the data and the recipient of the data first enter into a Data Use Agreement. The PI, the holder of the PHI and their respective institutions must sign the Data Use Agreement, for access to a limited data set or for the release of a limited data set. The Data Use Agreement must, among other things, establish the permitted uses and disclosures of the information included in the limited data set and must provide that the recipient of the limited data set will not identify the information or use it to contact individuals. The standard data Use Agreement is attached. Any proposed changes must be reviewed by legal counsel for the institution.

As with research conducted pursuant to a HIPAA Authorization, disclosures of PHI that is part of a limited data set need not be tracked for purposes of providing an accounting to the individual.

The use of a limited data set should be specified in the protocol and must be approved by the IRB, subject to execution of the Data Use Agreement.

**J. Databanks and Biorepositories**

The collection or maintenance of PHI in databanks or repositories for future research purposes requires an IRB-approved protocol. Likewise, research utilizing data from databanks and repositories must be conducted under a protocol approved by the IRB.

The PI must obtain a HIPAA Authorization from the subject about whom information is stored or a HIPAA waiver of authorization approved by the IRB for the collection of PHI and prior to conducting subsequent studies utilizing the PHI. The authorization 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.

The HIPAA Authorization may be combined with the informed consent for the creation or maintenance of a research database or repository. The combined HIPAA Authorization and informed consent form for participation in the database or repository, i.e., for future use of samples or PHI, must provide the option for the subject to opt in and provide separate authorization for the database or repository. Example: the subject is given the option to provide permission for sharing information for purposes related to the trial AND in a separate statement, the subject provides a “second” permission to bank the biologic material for use in future research studies. If selecting this option, investigators are reminded to retain the signed combined form for the full duration that the banked data or biologic sample will be retained for future research purposes.

**K. Accounting of Disclosures**

T:\Procedural Manual\Policies\PHI-in-research.doc
Administratively Revised 6/28/2012, Revised and JEC approved 5/9/14
In general, HIPAA requires that, upon request, patients be provided with a listing of individuals external to the covered entity who have had access to or been provided a copy of their records for reasons other than treatment, payment, healthcare operations or with the patient’s authorization. This accounting must include disclosures of protected health information that occurred during the six years prior to the individual's request for an accounting, and must include specified information regarding each disclosure. A more general accounting is permitted for subsequent multiple disclosures to the same person or entity for a single purpose.

Among the types of disclosures that are exempt from this accounting requirement are:

- Research disclosures made pursuant to an individual's authorization .
- Disclosures of the limited data set to researchers with a data use agreement.

In addition, for disclosures of PHI for research purposes without the individual's authorization (i.e. when the IRB has approved waiver of the authorization requirement), and that involve at least 50 records, HIPAA allows for a simplified accounting of such disclosures by covered entities. Under this simplified accounting provision, covered entities may provide individuals with a list of all protocols for which the patient's protected health information may have been disclosed, as well as the researcher's name and contact information.

L. Reporting and Sanctions

Call your institution’s Privacy Officer if you suspect that PHI might have been lost, stolen, or improperly accessed or disclosed. For Montefiore, call (718) 920-8239 or email Montefiore’s Privacy Officer at privacyofficer@montefiore.org. For Einstein, ___________. For NBHN, ____________

Improper access to or disclosure of patient information may result in the loss of access to electronic clinical information and may result in disciplinary action, up to and including termination and/or revocation of clinical privileges and faculty appointment.

M. Resignations of Investigators or Research Staff

In the event that a PI or research staff member leaves the institution and wishes to copy or remove research data created or acquired by/at the institution, he or she must request permission from his or her department chair and the Privacy Officer. All data remains the property of the employing institution. Upon termination or resignation of research staff who had been granted access to electronic medical records, the PI must notify the institution’s IT department immediately to ensure termination of access.

N. Case Reports

Refer to Einstein IRB Policy, “Case Report Policy” for requirements for obtaining HIPAA Authorization prior to publishing a case report.