

HIPAA and Medical Research Training

ROWAN UNIVERSITY POLICY

Title: *HIPAA and Medical Research Training*

Subject: *Research Integrity*

Policy No: *Res: 2014: 02*

Applies: *University-wide*

Issuing Authority: *Vice President for Research*

Responsible Officer: *RowanSOM Senior Associate Dean for Research*

Adopted: *03-10-14*

Last Revision: *02/04/2015*

Last Reviewed: *10/20/2015*

I. PURPOSE

The purpose of this policy is to articulate the additional new requirements HIPAA adds to research.

II. ACCOUNTABILITY

Under the direction of the Vice President of Research, the RowanSOM Senior Associate Dean for Research shall implement and ensure compliance with this policy.

III. APPLICABILITY

This policy is applicable to all members of RowanSOM workforce who have access to or use PHI, such as to conduct healthcare transactions or clinical research, including students and faculty.

IV. REFERENCES

1. Health Insurance Portability and Accountability Act of 1996 (HIPAA).
2. Health Information Technology for Economic and Clinical Health (HITECH) Act

V. POLICY

1. The HIPAA Privacy Rule
 - a. The HIPAA privacy rule contains comprehensive privacy regulations. The final HIPAA Privacy Rule was issued August 14, 2002 (requiring compliance by April 14, 2003).
 - b. The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.
2. The Privacy Board
 - a. The Privacy Board was founded to help researchers meet the privacy requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These requirements may affect any

research that uses certain protected health data. Under the HIPAA Privacy Rule, any research that involves protected health information, regardless of the source of funding, must be authorized by the individuals whose health data they intend to use or the researcher must obtain a Waiver of Authorization. The Privacy Board was specifically established to review requests for a Waiver of Authorization.

- b. The Privacy Board at RowanSOM is also the Institutional review Board. It is composed of individuals experienced in reviewing a wide variety of clinical research, including research involving confidential and sensitive health information. It is the most efficient and cost-effective resource for any organization engaged in research involving protected health information and data.
- c. While most research is regulated by the Common Rule (45 CFR part 46) and FDA regulations (CFR Parts 50 and 56), since the privacy provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) became effective on April 14, 2003, researchers now need to take precautions to protect the privacy of individually identifiable health information, or "protected health information" ("PHI").

VI. FUNDAMENTAL RULES FOR RESEARCH

1. Patient Authorization

- a. Researchers may request information inside a patient's medical file if the individual has granted written permission for its release to the researcher by means of a signed authorization form.
- b. The Research Authorization required under the HIPAA Privacy Rule is a written patient authorization that must specify:
 - i. Who can use or disclose PHI
 - ii. To whom PHI may be disclosed
 - iii. What PHI may be used or disclosed
 - iv. The purposes of the used or disclosed PHI
 - v. The duration of the authorization (expiration date or event)

2. Preparatory to Research

- a. The Privacy Rule applies to the use of protected health information (PHI) in those activities preparatory to research that are necessary to prepare a research protocol for a grant application or IRB review or for similar purposes.
- b. Preparatory to research activities are defined as:
 - i. the development of research questions;
 - ii. the determination of study feasibility (in terms of the available number and eligibility of potential study participants);
 - iii. the development of eligibility (inclusion and exclusion) criteria; and
 - iv. the determination of eligibility for study participation of individual potential subjects. The Office of Civil Right guidance permits a researcher to identify prospective research participants for purposes of seeking their authorization to use or disclose protected health information (PHI) for a research study. The PHI used to identify prospective research participants could include contact information, diagnosis or condition, and other information necessary to determine study eligibility. Although OCR considers the use and disclosure of PHI to determine study eligibility a preparatory to research activity, the actual process used to recruit subjects remains a research activity and requires IRB approval. A researcher may use PHI for preparatory to research activities, only if before such use, the researcher makes certain representations about the use of PHI by submitting "Preparatory to Research Representation" form. This form and the procedures to follow to obtain permission wherein a researcher uses/reviews PHI for the purpose of developing a research protocol; formulating a research hypothesis; or to screen for study eligibility is available in the following link: <http://www.rowan.edu/som/hsp/guidance/index.html>.

3. IRB or privacy board approval:

A hospital or health plan can allow a researcher access to patient medical information upon receipt of documentation that an Institutional Review Board (IRB), or a privacy board, has granted the researcher a waiver of the requirement to obtain individual authorization. The IRB or Privacy board, a committee formally designated by an institution to review research involving human subjects, can grant a waiver if it determines that the research project cannot proceed without the data, according to HHS.

4. De-identified data:

The HIPAA privacy rule allows researchers access to patient health information that has been de-identified through removal of 18 identifiers. Under this condition the IRB (Privacy Board) may approve the use/disclosure of data/information without an individual's authorization if it determines that health information is not individually identifiable. To meet this condition, all of the 18 elements of identifiers must be removed before the data is released to the researcher.

5. Limited data set:

- a. HIPAA's Privacy Rule makes provisions for a "limited data set," authorized only for public health, research, and health care operations purposes. A limited data set could include the following potentially identifying information:
 - i. admission and discharge, and service dates;
 - ii. dates of birth and, if applicable date of death;
 - iii. age, including age 90 or over and
 - iv. five digit zip code or any other geographic subdivision, such as state, county, city, precinct and their equivalent geocodes except street addresses.
- b. The disclosure of the limited data set requires the use of a "data use agreement", which establishes the permitted uses and disclosure of such information consistent with the purposes of research, public health and healthcare operations. It limits who can receive and use data and requires the recipient to not re-identify the data or contact the individuals.

6. Research on protected health information of decedents:

Representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the protected health information of decedents, that the protected health information being sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is being sought. See 45 CFR 164.512(1)(iii).

VII. DIFFERENCES BETWEEN CONSENT AND AUTHORIZATION

1. The Common Rule and FDA regulations require consent to participate in research.
2. The Privacy Rule permits, but does not require, a covered entity voluntarily to obtain patient consent for uses and disclosures of protected health information for treatment, payment, and health care operations. However, the privacy rule requires an "authorization" for uses and disclosures of protected health information not otherwise allowed by the Rule. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization.

VIII. RESEARCH USE WITHOUT AUTHORIZATION

1. Under the Privacy Rule at section 164.512, a covered entity may use or disclose PHI for a research study without Authorization (or with an altered Authorization) from the research participant if the covered entity obtains proper documentation that an IRB or Privacy Board has granted a waiver (or alteration) of the Authorization requirements. Among other requirements under section 164.512, a covered entity must obtain a statement that an IRB or a Privacy Board has determined that the alteration or waiver, in whole or in part, of Authorization satisfies the following three criteria in the Privacy Rule. The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
 - a. An adequate plan to protect the identifiers from improper use and disclosure.
 - b. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law.
 - c. Adequate written assurances that the PHI will not be reused 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 PHI would be permitted by the Privacy Rule.
 - d. The research could not practicably be conducted without the waiver or alteration
 - e. The research could not practicably be conducted without access to and use of the PHI.

2. This provision of the Privacy Rule might be used, for example, to conduct records research, when researchers are unable to use de-identified information, and the research could not practicably be conducted if research participants' authorization were required.

IX. RESEARCH USE/DISCLOSURE WITH INDIVIDUAL AUTHORIZATION

1. A Privacy Rule Authorization is an individual's signed permission to allow a covered entity to use or disclose the individual's protected health information (PHI) that is described in the Authorization for the purpose(s) and to the recipient(s) stated in the Authorization. In contrast, an informed consent document is an individual's agreement to participate in the research study and includes a description of the study, anticipated risks and/or benefits, and how the confidentiality of records will be protected, among other things. An Authorization can be combined with an informed consent document or other permission to participate in research. If a covered entity obtains or receives a valid Authorization for its use or disclosure of PHI for research, it may use or disclose the PHI for the research, but the use or disclosure must be consistent with the Authorization.
2. The Authorization must be written in plain language. A copy of the signed Authorization must be provided to the individual signing it if the covered entity itself is seeking the Authorization. The Privacy Rule specifies core elements and required statements that must be included in an Authorization. An Authorization is not valid unless it contains all the required elements and statements. An Authorization form may also, but is not required to, include additional, optional elements so long as they are not inconsistent with the required elements and statements and are not otherwise contrary to the Authorization requirements of the Privacy Rule.

X. CORE ELEMENTS OF AUTHORIZATION

1. Description of PHI to be used or disclosed
2. The name(s) of persons or other specific identification of person(s) class of persons authorized to make the requested use or disclosure.
3. The name(s) or other specific identification of the person(s) or class of persons who may use the PHI or to whom the covered entity may make the requested disclosure.
4. Description of each purpose of the requested use or disclosure. Researchers should note that this element must be research study specific, not for future unspecified research.
5. Authorization expiration date or event that relates to the individual or to the purpose of the use or disclosure (the terms "end of the research study" or "none" may be used for research, including for the creation and maintenance of a research database or repository).
6. Signature of the individual and date. If the Authorization is signed by an individual's personal representative, a description of the representative's authority to act for the individual

XI. REQUIRED STATEMENTS IN THE RESEARCH AUTHORIZATION AGREEMENT

1. The individual's right to revoke Authorization in writing and either (1) the exceptions to the right to revoke and a description of how the individual may revoke Authorization or (2) reference to the corresponding section(s) of the covered entity's Notice of Privacy Practices. *Note:* A research subject may revoke Authorization at any time. However, a covered entity may continue to use and disclose PHI that was obtained before the individual revoked Authorization to the extent that the entity has taken action in reliance on the Authorization. In cases where the research is conducted by the covered entity, this would permit the covered entity to continue using or disclosing the PHI as necessary to maintain the integrity of the research.
2. Notice of the covered entity's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the Authorization, including research-related treatment, and, if applicable, consequences of refusing to sign the Authorization.
3. The potential for the PHI to be re-disclosed by the recipient and no longer protected by the Privacy Rule. This statement does not require an analysis of risk for re-disclosure but may be a general statement that the Privacy Rule may no longer protect health information.

XII. TRACKING AND ACCOUNTING FOR RESEARCH DISCLOSURES OF PHI

1. The HIPAA Privacy Rule gives a person the right to request a written record ("an accounting") when a covered entity has made certain disclosures of that person's protected health information ("PHI"). The accounting must include all covered disclosures in the six years prior to the date of the person's request, but no further back than April 14, 2003. The principal investigator of an IRB-approved research project or a project for which the IRB has granted exempt status is responsible for compliance with the following two HIPAA accounting requirements:
 - a. Tracking certain disclosures of an individual subject's PHI, or of all subjects' PHI, that are made by any member of the study team; and
 - b. Providing the disclosure tracking information to the HIPAA Office or to Medical Records (as explained below)
2. The HIPAA compliance Office at RowanSOM responds to patient requests for accountings and uses the information provided by the principal investigator and by Medical Records for this purpose. For research, the investigator should maintain a record of all disclosures (as described above) made by the research team that are subject to the HIPAA tracking requirement.
3. This accounting must include disclosures of protected health information that occurred during the six years prior to the individual's request for an accounting, or since the applicable compliance date (whichever is sooner), 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. See 45 CFR 164.528(b)(3). Among the types of disclosures that are exempt from this accounting requirement are:
 - a. research disclosures made pursuant to an individual's authorization and
 - b. disclosures of the limited data set to researchers with a data use agreement under 45 CFR 164.514(e).
4. In addition, for disclosures of protected health information for research purposes without the individual's authorization pursuant to 45 CFR 164.512, and that involve at least 50 records, the Privacy Rule 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 under 45 CFR 164.512, as well as the researcher's name and contact information. Other requirements related to this simplified accounting provision are found in 45 CFR 164.528(b)(4).

XIII. TRANSITION PROVISIONS

1. The Privacy Rule contains a transition provision that, under certain conditions, allows covered entities to continue to use or disclose PHI without an Authorization, or waiver or alteration of the Authorization requirement, in connection with ongoing research, including research involving repositories or databases. For many such uses and disclosures of PHI in connection with ongoing research, a covered entity may rely on any one of the following that was obtained prior to the compliance date:
 - a. an Authorization or other express legal permission from an individual to use or disclose PHI for research;
 - b. the informed consent of the individual to participate in the research and
 - c. a waiver by an IRB of informed consent in accordance with applicable laws and regulations governing informed consent, unless informed consent is sought after the compliance date
2. If the transition provisions do not apply and the information is not de-identified, subsequent uses and disclosures of PHI from databases and repositories held by covered entities generally require an individual's Authorization unless otherwise permitted by the Privacy Rule (e.g., with a waiver of Authorization or as a limited data set).
3. In addition, if the database or repository, which is held or maintained by a covered entity, contains only de-identified health information (which may include a re-identification code) meeting the Privacy Rule's requirements at section 164.514(a)-(c), the Privacy Rule does not apply.

XIV. ATTACHMENTS

1. Attachment 1, HIPAA and Medical Research – Frequently Asked Questions

ATTACHMENT 1

FREQUENTLY ASKED QUESTIONS

1. **What is HIPAA?**

HIPAA is the Health Insurance Portability and Accountability Act of 1996. HIPAA requires many things, including the standardization of electronic patient health, administrative and financial data. It also establishes security and privacy standards for the use and disclosure of "protected health information" (PHI).

2. **What is PHI?**

HIPAA's privacy provisions are limited to use and disclosure of Protected Health Information, or PHI. PHI is defined as individually identifiable health information that is created or received by a HIPAA covered entity. Health information includes any information, whether oral or recorded in any form, 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.

3. **What are covered entities?**

Covered entities are health plans, health care clearinghouses and health care providers that transmit health information related to insurance coverage electronically. At Rowan University, all transactions occurring at RowanSOM is considered as part of the covered entity.

4. **Does HIPAA rule hinder research?**

There is no reason to believe that the Privacy Rule will hinder medical research. Indeed, patients and health plan members should be more willing to authorize disclosures of their information for research and to participate in research when they know their information is protected. The Privacy Rule both permits important research and, at the same time, it encourages patients to participate in research by providing much needed assurances about the privacy of their health information.

5. **What is the definition of a researcher under HIPAA?**

A researcher is a covered health care provider if he or she furnishes health care services to individuals, including the subjects of research, and transmits any health information in electronic form in connection with a transaction covered by the Transactions Rule. See 45 CFR 160.102, 160.103. For example, a researcher who conducts a clinical trial that involves the delivery of routine health care and transmits health information in electronic form to a third party payer for payment would be a covered health care provider under the Privacy Rule. Researchers who provide health care to the subjects of research or other individuals would be covered health care providers even if they do not themselves electronically transmit information in connection with a HIPAA transaction, but have other entities, such as a hospital or billing service, conduct such electronic transactions on their behalf. For further assistance in determining covered entity status, see the "decision tool" at www.hhs.gov/ocr/hipaa.

6. **What impact does HIPAA has on research protocols?**

Besides the impact of Common Rule on research, HIPAA adds certain additional new requirements to research. Under HIPAA, the use and disclosure of PHI for research purposes requires an authorization from the research subject unless some exception applies. HIPAA also applies to research related activities which were not covered under the Common Rule such as research on decedents. HIPAA introduces a concept known as the "minimum necessary" standard. In general, HIPAA requires that only the minimum necessary PHI should be used unless the PHI is used for treatment, or unless the use or disclosure is made subject to a written authorization (including a research authorization). Thus, the minimum necessary standard requires researchers who are engaging in research not pursuant to an authorization to limit their access of PHI to only that needed to accomplish the research initiative and the intended purpose of the use and disclosure of PHI.

7. **What research activities are covered under HIPAA?**

The Privacy Rule applies to the following types of research activities when they involve PHI:

- a. research using or creating PHI about living individuals;
- b. activities that are preparatory to research;
- c. research on decedents who have been deceased less than 50 years;
- d. recruitment and
- e. research using a limited data set

8. **What research activities are not covered under HIPAA?**

- a. Research using de-identified data
- b. Research conducted by an individual who is not part of a covered entity and that does not require access to information held by a HIPAA covered entity

- c. Research on individuals who have been deceased more than 50 years

9. ***What are the conditions for using or creating PHI for research on living individuals?***

PHI may not be used unless the following conditions are met:

- a. subject has provided IRB-approved authorization for research;
- b. IRB has approved waiver of authorization;
- c. the study involves IRB-approved use of de-identified data or limited data set;
- d. researchers may continue to use or disclose PHI obtained or created before April 14, 2003 pursuant to the informed consent document for that research study and
- e. an authorization form or request for a waiver is not required if subjects have executed an informed consent to participate prior to April 14, 2003.

10. ***What are some of the elements that must be included in the authorization***

HIPAA generally requires a written authorization from the subject permitting a researcher to use or disclose the subject's PHI for research purposes. The researcher is required to get written authorization from the research participants via a signed Research Authorization Form. The written authorization must articulate:

- a. a specific description of what PHI will be used/disclosed;
- b. the names of persons or organizations that may use or disclose PHI;
- c. the names of persons or organizations to which PHI will be disclosed;
- d. a statement 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. A statement regarding the potential for re-disclosure to others not subject to the Privacy Rule;
- g. a notice that the covered entity may or may not condition treatment or payment on the individual's signature and
- h. the individual's signature and date.

11. ***What is a waiver of authorization?***

An IRB may grant a waiver of authorization if the following conditions are met:

- a. the research could not be practicably conducted without the waiver;
- b. the research could not be practicably conducted without access and use of 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 study, or for other research for which the use or disclosure of protected health information would be permitted by the Privacy Rule;
- d. uses and disclosures of PHI will be limited to the minimum necessary standard; disclosure involves no more than minimal privacy risk to the individuals and
- e. reviewed by the IRB with specific approval regarding access to the PHI.

Researchers can request a waiver of authorization by completing the appropriate section of the eIRB application by answering all of the questions on the application form and submitting to the IRB for approval. The criteria for waiver are very similar to those for waiving informed consent. Investigators will receive from the IRB an authorized Approval/Denial of Waiver of HIPAA Authorization.

12. ***What activities may be conducted under preparatory to research?***

- a. PHI may be accessed in activities that are "preparatory to research." This type of access is limited to a 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. While an investigator may review PHI during the course of a review of preparatory to research, he or she may not remove copy or include any PHI in notes. As such, a researcher who is an employee or a member of the covered entity's workforce could use protected health information to contact prospective research subjects. The preparatory to research provision would allow such a researcher to identify prospective research participants for purposes of seeking their authorization to use or disclose protected health information for a research study. In addition, the Rule permits a covered entity to disclose protected health information to the individual who is the subject of the information. See 45 CFR 164.502(a)(1). Therefore, covered health care providers

and patients may continue to discuss the option of enrolling in a clinical trial without patient authorization, and without an Institutional Review Board (IRB) or Privacy Board waiver of the authorization.

- c. However, a researcher who is not a part of the covered entity may not use the preparatory to research provision to contact prospective research subjects. Rather, the outside researcher could obtain contact information through a partial waiver of individual authorization by an IRB or Privacy Board as permitted at 45 CFR164.512(1).

13. *What researchers need to do if research involves decedents health information?*

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. The Health information of individuals who have been deceased for more than 50 years is not subject to the HIPAA requirements. The researcher must first represent that the use or disclosure of PHI is solely for research on the PHI of decedents. Please contact the Privacy Compliance Office for further information or to request a decedent's medical history.

14. *Using de-identified for research, what should be done?*

De-identified data are data that contains none of the 18 identifiers listed earlier. If all of the identifiers are removed, the information is considered to be no longer individually identifiable, no longer PHI, and no longer subject to HIPAA's requirements. A de-identified data set may be coded with a unique identifier that cannot be traced back to the individual for the purpose of being re-identified by the recipient at a later date. It is important to remember that re-identification will subject the information to HIPAA's requirements.

15. *What is limited data set?*

- a. Some studies may need some limited identifiers and thus not meet the strict 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.
- b. A data set may also be considered de-identified if an expert in statistical and scientific methods determines and documents that the methods used to de-identify or code the data presents a very small risk that the information can be used alone or in combination with other reasonably available information to identify an individual.
- c. A limited data set could include the following potentially identifying information: (1) Admission and discharge, and service dates; (2) dates of birth and, if applicable date of death; (3) age, including age 90 or over and (4) five digit zip code or any other geographic subdivision, such as state, county, city, precinct and their equivalent geocodes except street addresses.
- d. The disclosure of the limited data set requires the use of a "data use agreement", which establishes the permitted uses and disclosure of such information consistent with the purposes of research, public health and healthcare operations, limits who can receive and use data and requires the recipient to not re-identify the data or contact the individuals.

16. *How do HIPAA regulations cover databanks and repositories?*

First collection or maintenance of PHI in databanks and utilizing data from repositories requires IRB approval. The HIPAA Privacy Rule requires an authorization from the subject about whom information is stored or a HIPAA Waiver of Authorization approved by an IRB for the collection of PHI and prior to conducting subsequent studies.

17. *Is exempt review of a research project allowed?*

Yes, so long as the study does not involve PHI. If the study does not involve risk to subjects, no identifiers are used and PHI is not involved, the study may be approved without the waiver of authorization. If the study involves, review of medical charts, tissue samples, medical and diagnostic images even though identifiers are not present but involves PHI, a waiver of authorization approved by the chair or a member of the IRB is required.

18. *Is expedited review of a research project permitted?*

The Common Rule applies if PHI is not included, involves minimal risk and identifiers are included. Such studies require participant's consent. If PHI is included, involves minimal risk, involves healthy or non-healthy participants, identifiers are included subjects consent and authorization is required. A special request for waiver of consent and authorization can be made so long as the criteria under this FAQ #9 have met. In both cases described above, IRB review and approval is required

19. ***What rights participants have to access research records or results?***

With few exceptions, the Privacy Rule gives patients the right to inspect and obtain a copy of health information about themselves that is maintained by a covered entity or its business associate in a "designated record set." It is unlikely that a researcher would be maintaining a designated record set, any research records or results that are actually maintained by the covered entity as part of a designated record set would be accessible to research participants unless one of the Privacy Rule's permitted exceptions applies. One of the exceptions of the privacy rule permits the individual's access rights in these cases to be suspended while the clinical trial is in progress, provided the research participant agreed to this denial of access when consenting to participate in the clinical trial. In addition, the health care provider/researcher must inform the research participant that the right to access protected health information will be reinstated at the conclusion of the clinical trial.

20. ***Are the HIPAA Privacy Rule's requirements regarding patient access in harmony with the Clinical Laboratory Improvements Amendments of 1988 (CLIA)?***

Yes. The Privacy Rule does not require clinical laboratories that are also covered health care providers to provide an individual access to information if CLIA prohibits them from doing so. CLIA permits clinical laboratories to provide clinical laboratory test records and reports only to "authorized persons," as defined primarily by State law. In addition, for certain research laboratories that are exempt from the CLIA regulations, the Privacy Rule does not require such research laboratories, if they are also a covered health care provider, to provide individuals with access to protected health information because doing so may result in the research laboratory losing its CLIA exemption.

21. ***If a research subject revokes his or her authorization to have protected health information used or disclosed for research, can the researcher continue using the protected health information already obtained prior to the time the individual revoked his or her authorization?***

Covered entities may continue to use and disclose protected health information that was obtained prior to the time the individual revoked his or her authorization, as necessary to maintain the integrity of the research study.

22. ***Can the researcher continue to disclose adverse event reports that contain protected health information to the Department of Health and Human Services (HHS) Office for Human Research Protections?***

Yes. The Office for Human Research Protections is a public health authority under the HIPAA Privacy Rule. Therefore, covered entities can continue to disclose protected health information to report adverse events to the Office for Human Research Protections either with patient authorization as provided at 45 CFR 164.508, or without patient authorization for public health activities as permitted at 45 CFR 164.512 (b).

23. ***Are there restrictions for recruiting study participants under HIPAA?***

Under HIPAA, the use of PHI to recruit an individual to participate in a research study must comply with HIPAA's general requirement that the use must be pursuant to an authorization or some exception, such as a waiver of HIPAA authorization. Although recruitment procedures usually only require access to a limited amount of health information, recruitment nonetheless is considered to be accessing PHI and therefore must comply with HIPAA requirements. Treating providers may not disclose PHI to a third party (including a "researcher" within the same covered entity) for purposes of recruitment in a research study without first obtaining authorization from the individual.

24. ***What should researchers do, if there is a breach of PHI?***

Research subjects have a right to be notified in cases where their PHI has been inappropriately accessed, used or disclosed in violation of the Privacy Rule. Potential breaches include lost paper records, lost smartphones or laptops containing PHI, misdirected mail, email or faxes etc. Notify the Privacy Officer immediately of all events that might have potential breaches.

25. ***How long should record be maintained?***

HIPAA related documentation must be maintained in accordance with record retention policy of the university. This requirement applies to accounting for disclosures records, authorizations, data use agreements and any other HIPAA forms. In some cases, FDA regulations for record keeping must be followed in accordance to agreement with the sponsor.

26. ***What privacy and security measures should be followed?***

HIPAA requires that we maintain the privacy of PHI by limiting its uses and disclosures and that we take reasonable steps to ensure that the PHI is secure. Most often, breaches in privacy can be traced to lax security so the two issues are intimately related.

- a. Everyone must complete RowanSOMs privacy training.
- b. If you are a researcher, you must also complete privacy training to specific HIPAA and medical research.
- c. Everyone must use "strong" passwords and must comply with Rowan IT's password security standards
- d. Must immediately report incidents that may involve the loss of, improper disclosure of, or improper access to PHI or ePHI (for example, the loss or theft of paper PHI; the loss or theft of computer, smartphone, or thumb drive storing ePHI; or an electronic intrusion into a computer storing ePHI). Reports should be made to the HIPAA Privacy Officer.
- e. Must not create, store, access, transmit or receive ePHI on personally owned computers. Faculty and staff who require remote access to on campus workstations or systems (e.g., IDX) that hold ePHI must use a University-provided, fully managed and encrypted device.
- f. Destroy or delete paper PHI or ePHI when no longer needed or when retiring computers, smartphones or other mobile devices such as thumb drives.

Draft HIPAA and Medical Research – 3-10-14