Human Subject Research Use and Disclosure of Protected Health Information

1.0 Purpose

The Wright State University (Wright State) Institutional Review Board (hereafter referred to as the "IRB") is responsible for ensuring compliance with the Health Insurance Portability and Accountability Act (hereafter referred to as the "Privacy Rule") when it acts as the privacy board for human subject research involving Wright State's or an external covered entity's (e.g., Premier Health) protected health information (PHI).

The purpose of this policy is to define institutional and investigator Privacy Rule requirements for research involving human subjects, and the procedures the IRB will follow to ensure compliance with those regulatory requirements.

2.0 Scope

This policy applies to all human subject research (exempt and non-exempt) that is conducted by Wright State faculty, staff, and students and for human subject research for which the IRB acts as the IRB of record/privacy board for an external entity (e.g., Premier Health). Many privacy board reviews conducted by the IRB involve non-Wright State PHI. Therefore, investigators must also take steps to identify and to be compliant with any applicable external Privacy Rule policies/procedures prior to initiating a study.

For example, Dayton Veterans Affairs Medical Center (Dayton VAMC) studies reviewed by the IRB must comply with VA Handbook 1200.05 and 1605.01 privacy requirements and are not subject to parts of this policy that are not consistent with VA Handbook and policies.

Wright State will accept Privacy Rule determinations (e.g., full and partial waivers) made by approved external IRBs on a case-by-case basis but reserves the right for the IRB to make independent privacy board determinations for research involving Wright State PHI (see *Collaborative Research and External IRB Review Policy* for more information).

3.0 Definitions

3.1 **HIPAA/Privacy Rule** means the minimum Federal standards (Health Insurance Portability and Accountability Act of 1996, specifically 45 CFR part 160 and subparts A and E of part 164) for safeguarding the privacy of individually identifiable health information. It includes the standards for an individual's privacy rights in order to enable them to understand and control how their protected health information (PHI) is used. Within the Department of Health and Human Services (DHHS), the Office for Civil Rights

(OCR) is authorized to implement and enforce the Privacy Rule.

3.2 **Protected Health Information (PHI)** means individually identifiable health information, including demographic data that is collected from an individual, and meets all of the following criteria:

- Is created or received by a health care provider, health care entity, health plan, public health authority, employer, life insurer, school/university, or health care clearing house; AND
- Relates to past, present, or future physical or mental health or condition of the individual; or the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; AND
- Identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual; AND
- Is transmitted or maintained in any form or medium, whether electronic, paper, or oral (see 45 CFR 160.103).

3.3 **Covered Entity** means a health plan, a health care clearinghouse, or health care provider who transmits health information in electronic form. A covered entity is responsible for implementing Privacy Rule protections of PHI collected, generated, or stored under its auspices.

3.4 **Research** means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge (45 CFR 164.501).

3.5 **Authorization** means permission to gain access to PHI. At Wright State, authorization for use and disclosure of PHI for research purposes is normally provided when a human research subject signs an informed consent document that contains an authorization section. Template authorization language can be found on the IRB website.

3.6 **Workforce Member** means employees, volunteers, trainees, and other persons whose work performance is under the direct control of a covered entity (i.e., Premier Health or Dayton Children's), regardless of whether they are paid by the covered entity.

3.7 **Use** means to employ, apply, utilize, examine, or analyze PHI maintained within the covered entity.

3.8 **Disclosure** means to share PHI with a person or organization outside the covered entity unless the covered entity has designated a recipient as a "Business Associate."

3.9 **Investigator** means the Project Director/Principal Investigator (PD/PI) and any other person, regardless of title or position, who is responsible for the design, conduct, or reporting of research, or proposing of research, including persons who are subcontractors, collaborators, or consultants. At Wright State this definition includes, but is not limited to, the following roles: Principal investigator, co- investigators, research coordinators, research associates, collaborators, and consultants, and may include research assistants and students as identified by the PD/PI depending on their specific roles and responsibilities.

3.10 **VPR (Vice Provost for Research & Innovation) Designee** is the Wright State official who is responsible for the development and implementation of the policies and procedures required to comply with the Privacy Rule as defined by the Code of Federal Regulations, 45 C.F.R. 160, 162 and 164.

4.0 Policy

HIPAA establishes the conditions under which PHI may be used and disclosed by investigators for research purposes. During the conduct of a research study, investigators may obtain, create, use, and/or disclose individually identifiable health information, which includes PHI. HIPAA permits investigators to use or disclose PHI for research only under the following circumstances and conditions:

4.1 The subject has granted specific written permission through an authorization;

4.2 There is documentation that the IRB of record has granted a waiver, partial waiver, or alteration of authorization requirements;

4.3 The review of PHI is solely for the purposes preparatory to research;
4.4 The review of PHI involves only decedents' information;

4.5 The PHI is de-identified in accordance with HIPAA standards, in which case the health information is no longer considered PHI; or

4.6 The PHI is released in the form of a limited data set, with an executed data use agreement including provisions for the use and disclosure of the limited data set as defined below.

To ensure regulatory compliance and privacy, the IRB expects all investigators utilizing or creating PHI to adhere to the requirements described in this policy and complete the Health Privacy course through the Collaborative Institutional Training Initiative (CITI) website.

Under the Privacy Rule, Wright State is considered a "hybrid" entity. This means that the

University has both covered (health care components subject to HIPAA) and non-covered (not subject to HIPAA) functions. Most on-campus investigators collecting identifiable health information on campus will be doing so via a non-covered function.

For example, a business school research study which recruits students eating at on-campus dining locations that includes a questionnaire which asks about vaccination status, blood pressure, birth date and current medications would not be subject to the Privacy Rule. However, the same survey administered at Miami Valley Hospital by a Wright State School of Medicine faculty member would be subject to the Privacy Rule and the requirements of this policy. Investigators should consult the IRB Office if unsure whether their research involves a covered function/entity.

5.0 **Procedures**

5.1 Uses Preparatory to Research

An investigator may review PHI in medical records or elsewhere without subject authorization to prepare a research protocol (e.g., determining whether a sufficient number or type of records exists to conduct the research prior to IRB application) if the proposed research use meets all of the following provisions:

- The use of disclosure is sought solely to review PHI as necessary to prepare the research protocol or other similar preparatory purposes
- No PHI will be removed from the covered entity during review, and
- The PHI that the investigator seeks to use or disclose is solely necessary for the research purpose.

5.1.2 Preparatory Activities Involving Wright State PHI

To meet the preparatory to research requirements, an investigator must submit an Initial Application using the IRB electronic submission system selecting the "Not Regulated as Research" option **prior** to the planned use. The fully executed form is Wright State's documentation that the use met the "Preparatory to Research" provision. Any investigator who obtains this certification must be able to provide evidence that the use met the three above criteria upon request of Wright State.

5.1.3 Preparatory Activities Involving Non-Wright State PHI

Prior to the preparatory to research access/use of PHI, an investigator must contact the appropriate research or privacy office of the covered entity to determine and then complete the appropriate preparatory to research

requirements for that covered entity.

5.1.4 Minimum Necessary Standard

Uses of PHI for research without authorization (i.e., preparatory to research and via an authorization waiver) are subject to the "minimum necessary" standard - that is, the uses/disclosures must be no more than the minimum required for the described research purpose. Therefore, an investigator must demonstrate in the Initial Application that the PHI to be accessed or used is the minimum necessary for preparing the research protocol and/or identifying potential subjects.

5.2 Subject Recruitment – Partial Waiver of Authorization

Investigators who meet the definition of a Workforce Member can record PHI and contact potential subjects for the purpose of seeking authorization for an IRB-approved study (e.g., WSU psychology professor conducting a study using records from the Wright State Ellis Institute or a Miami Valley research nurse utilizing Miami Valley medical records). However, Non-Workforce investigators and study teams that include Non-Workforce investigators (e.g., WSU psychology professor conducting study using Miami Valley medical records to obtain subject contact information) must obtain a partial waiver of authorization as part of overall study approval from the IRB before contacting potential subjects.

To obtain a partial waiver for recruitment, an investigator must provide sufficient information in the study application to meet the following three criteria:

5.2.1 The use or disclosure of the PHI for screening/recruitment purposes involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:

- An adequate plan to protect PHI identifiers from improper use and disclosure
- 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 such retention is otherwise required by law, and
- 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 study, or for other research for which the use or disclosure of the PHI is permitted by the Privacy Rule

5.2.2 The screening/recruitment could not practicably be conducted without the waiver or alteration, and

5.2.3 The screening/recruitment could not practicably be conducted without access to and use of the PHI.

Note that any subsequent use or disclosure of the same PHI for a separate study requires written authorization or a separate waiver determination.

5.3 Written Authorization

Investigators are required to obtain written authorization from each human subject prior to the use or disclosure of the subject's individual PHI for research purposes unless the IRB, in its privacy board role, has granted a waiver. The purpose of the authorization is to inform an individual how his/her PHI and research information (collected or created) is to be used; who the information will be shared with; and to inform the individual of the right to access information about them that is held by Wright State or by another covered entity.

All written authorizations must include certain elements and statements in order to be valid (45 CFR 164.508). A written authorization must include the following:

- A description of the PHI to be used or disclosed, identifying the information in a specific and meaningful manner (e.g., medication list, problem list). It is not acceptable to state "entire medical record" unless the entire medical record is required to perform the research.

- The names or other specific identification of the person or persons (or class of persons) authorized to make the requested use or disclosure.

- The names of individuals, organizations, companies, and/or class of individuals to whom Wright State/covered entity officials and investigators (the covered entity) may disclose (share) the PHI, or who may use the subject's PHI in relation to the research study.

- A description of the purpose(s) of the requested use or disclosure.

- A signature block for signing and dating of the authorization by the individual or the individual's legally authorized representative (Note: only one subject signature is required to provide both authorization and consent).

- The authorization expiration date or expiration event that relates to the individual or to the purpose of the use or disclosure.

- A statement of the subject's right to revoke authorization and how to do so, and, if applicable, the exceptions to the right to revoke the authorization.

- A statement explaining whether non-research treatment, payment, enrollment, or eligibility of benefits can be conditioned on authorization. In addition, the authorization must specify whether a subject can still participate in research study if they do not provide authorization, and

- A statement of the potential risk that PHI will be re-disclosed and no longer protected by the Privacy Rule. This may be a general statement that the Privacy Rule may no longer protect health information once it has been disclosed.

The authorization must be written in plain language and included within the research informed consent form. To do this in accordance with Wright State requirements, a section entitled "Authorization to Use and Disclose Your Health Information" must be added as one of the last sections of the consent form, except for Dayton VAMC studies because the VA Handbook requires a separate authorization document.

Investigators must add study-specific information to the Wright State authorization template. The approved authorization template can be found on the IRB website at: https://www.wright.edu/research/research-compliance/templates-check-lists-decision-trees.

FDA and DHHS regulations require that the IRB must review and approve all language included in the consent form. To facilitate this review, investigators should not deviate from currently approved authorization template language as described above, unless unavoidable. Any deviation proposed by the sponsor or study team must be submitted according to the IRB's current study application requirements for review and approval (e.g., submission of a separate copy of consent with all required authorization elements and statements labeled for review).

5.4 Exempt Research

Exempt research that involves PHI requires signed written authorization unless the IRB grants a waiver as described in Section 5.5, even when IRB does not require signed informed consent.

Formal written informed consent is not required for research that is determined to be exempt from IRB review in accordance with 45 CFR 46.101(b). However, the IRB

encourages investigators to provide potential subjects with information about the study (e.g., informational letter) whenever feasible prior to engaging any subject in that research as a way to support their voluntary participation.

5.5 Waiver of Authorization and Required Documentation

Under the Privacy Rule, the IRB may waive or alter, in whole or in part, the Privacy Rule's written authorization requirements for the use and disclosure of PHI in connection with a particular research study. An investigator may seek a complete (full) waiver of the authorization requirements for some types of research.

For example, creating databases or repositories may qualify for a full waiver. However, future use of the data in the database/repository for individual research studies outside of the approved database/repository IRB application will require written authorization or a separate waiver of authorization granted by the IRB.

The IRB may also approve a request that removes some, but not all, required elements of a written authorization (i.e., an alteration). For example, removing the element that describes the purpose of the requested use/disclosure of the PHI in cases where identification of the purpose may affect the results of the study or obtaining verbal authorization without subject signature.

A waiver granted for a study applies only to the use of the PHI for that study, and no other studies. Any subsequent use or disclosure of the PHI obtained for a different research study from the waivered study must have a separate authorization. An exception may apply if the new research meets one of the exceptions criteria under section 45 CFR 164.512(i) (e.g., waiver of authorization) or 45 CFR 164.514(e) (i.e., as a limited data set with a Data Use Agreement), but the IRB must make this determination that exception criteria are met. The investigator is not permitted to make this determination.

To approve a request for waiver or alteration of the requirement to obtain signed authorization, the IRB must determine (via information provided by the investigator in the IRB application) and document that the use meets all of the following three criteria:

5.5.1 The use or disclosure of the PHI involves no more than a minimal risk to the privacy of subjects, based on, at least, the presence of the following elements:

- An adequate plan to protect PHI identifiers from improper use and disclosure
- 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 such retention is otherwise required by law, and

- 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 study, or for other research for which the use or disclosure of the PHI is permitted by the Privacy Rule.

5.5.2 The research could not practicably be conducted without the waiver or alteration, and

5.5.3 The research could not practicably be conducted without access to and use of the PHI.

IRB documentation (i.e., study approval or exemption letter) granting the waiver must include the following information:

- The identity of the approving IRB (i.e., WSU IRB)
- The date on which the waiver or alteration was approved
- A statement that the IRB has determined that all the specified criteria for a waiver or an alteration were met
- A brief description of the PHI for which use, or access has been determined by the IRB to be necessary in connection with the specific research activity, and
- A statement that the waiver or alteration was reviewed and approved under either full board or expedited review procedures (i.e., at least one voting IRB member).

Generally, if a research protocol qualifies for a waiver of informed consent from the IRB, the research protocol may be eligible for a waiver of authorization under the Privacy Rule. However, the IRB must make the determination whether waiver of authorization is appropriate. Investigators remain accountable, and have responsibility, for any PHI disclosed under a waiver of authorization (see Section 5.6).

Investigators who conduct medical record reviews and secondary data analyses should be aware that the “not practicable without a waiver” standard requires substantive justification. For example, it may be practicable to get written authorization from 30 subjects who are current patients of the investigator. In contrast, it may not be practicable to obtain written authorization from 500 stroke patients seen at Premier Health during the past ten years.

5.6 Accounting of Research Disclosures

The Privacy Rule gives individuals the right to receive an accounting of certain disclosures of PHI made by Wright State, the 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, or since the effective date of HIPAA (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)).

To meet the accounting requirements, it is important to understand the difference between a use and a disclosure. Disclosures occur whenever PHI is shared with a person or organization outside the covered entity (e.g., Wright State or local hospital), unless the covered entity has designated a recipient as a "workforce member." During the conduct of research PHI is commonly "disclosed" to non-workforce members such as research sponsors, external collaborators, contract research organizations, and sample testing laboratories. "Use" means to employ, apply, utilize, examine, or analyze PHI maintained within the covered entity.

Accounting is required for certain "disclosures, not for "use" of PHI.

5.6.1 Applicable Research Disclosures

Investigators must account for all disclosures of PHI under a waiver (partial and full) of authorization granted by the IRB or disclosures of decedent PHI for research where no authorization on behalf of the individual has been obtained.

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

- Research disclosures made pursuant to an individual's written authorization;
- Disclosures of the limited data set to researchers with a data use agreement under 45 CFR 164.514(e).

PHI that has been obtained through a review preparatory to research (as defined in the regulations) is not to be removed from the covered entity (i.e., disclosed) by the investigator in the course of the review. Therefore, it is also not subject to the accounting requirements.

5.6.2 Single Disclosure Per Individual for Research Involving Less Than 50 Subjects

As a general rule, the following information must be maintained and provided to an individual or their authorized representative upon request:

- The date of the disclosure;

- The name of the entity or person who received the protected health information and, if known, the address of such entity or person;
- A brief description of the protected health information disclosed; and
- A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of the applicable written request for a disclosure, if any.

5.6.3 Multiple Disclosures Per Individual for Research Involving Less Than 50 Subjects

If there have been multiple disclosures to the same person or entity (such as multiple disclosures of that person's information to a researcher or sponsor) during the "accounting period" the person is requesting, the following information may be provided:

- The information required above for the first disclosure during the accounting period;
- The frequency, periodicity, or number of the disclosures made during the accounting period; and
- The date of the last disclosure during the accounting period.

5.6.4 Disclosures for Research Involving 50 or More Subjects

In addition, for research disclosures of PHI without the individual's authorization pursuant to 45 CFR164.512(i), and that involve at least 50 individuals (such as with research databases), the Privacy Rule allows for a simplified accounting of such disclosures. Under this simplified accounting provision, covered entities may provide individuals with the following for disclosures where the PHI about the individual was (or may have been) included:

- The name of the protocol or other research activity;
- A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;
- A brief description of the type of PHI that was disclosed;
- The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
- The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

- A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

5.6.5 Required Logging of Research Disclosures

Investigators are responsible for logging disclosures described above using the electronic "Research Accounting of Disclosures" form found on the IRB website.

A copy of the required log information (Section 5.62-5.64) must be maintained for audit purposes by the investigator for at least six years and securely stored to protect confidentiality.

5.6.6 Individual Requests for Accounting of Disclosures

All individual requests for an accounting of disclosures will be directed to the VPR Designee. This official will be responsible for providing the required information in accordance with all applicable Wright State policies and requirements. If an individual requests additional information about disclosure of their PHI for research purposes after receiving their initial accounting, the applicable investigator will be responsible for providing as much additional information about the disclosure as available to the VPR Designee.

The documentation of disclosures and related information must be maintained for at least six years from the completion of the research involving the disclosure of PHI.

5.7 De-Identified Data

Health information that meets the Privacy Rule definition of "de-identified" is not considered PHI and therefore is not subject to the Privacy Rule or the requirements (e.g., written authorization) in this policy. However, the definition of "de-identified" is very specific under the Privacy Rule. Therefore, investigators must understand that data that may be considered "de-identified" under DHHS and FDA regulation may not be considered "de-identified" under the Privacy Rule. For example, under DHHS regulations (45 CFR 46.101(b) (4)) an investigator can record data such that the subjects "cannot be identified, directly or" indirectly "through identifiers linked to the subjects." Under this scenario, individual subject data collected by the investigator containing a zip code could be considered "de-identified," but not de-identified under the Privacy Rule.

Using improperly de-identified data for research can constitute non-compliance. Therefore, investigators who plan to conduct research involving "de-identified data" are encouraged to consult with the HIPAA & Privacy Compliance Office or the IRB Office

prior to initiation of such research to ensure that their proposed data set(s) meet the Privacy Rule requirements.

To be considered "de-identified" under the Privacy Rule, EITHER: all of the following 18 identifiers of the individual, their relatives, employers, or household members must have been removed from the individual's data set by an individual that is not a member of the study team (e.g., medical records official, administrator of a database):

- Names (including the patient's name and names of other individuals connected to the patient)
- Geographic subdivisions smaller than a state (zip-code, street address, etc.…)
- All elements of a date (except year) including birth date, admission date, discharge date, date of death, and all ages over 89)
- Telephone numbers
- Fax numbers
- E-mail address
- Social security number
- Medical record number
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers including license plates
- Device identifiers and serial numbers
- Web universal resource locators (URLs)
- Internet protocol (IP) address numbers
- Biometric identifiers including fingerprints and voice prints
- Full face photographic (or comparable) images
- Any other unique identifying number, characteristic, or code unless otherwise permitted by the Privacy Rule for re-identification, **AND**

Wright State does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

OR

The data is grouped in such a way that a qualified statistician using accepted analytic techniques concludes that the risk of identification based on the information in the data set is substantially limited, and that if the information is used alone or in combination with other reasonably available information, it does not identify an individual subject

(e.g., aggregate data) [45 CFR 164.514(b)].

5.8 Limited Data Sets and Data Use Agreements

A "limited data set" is defined in the Privacy Rule as a limited set of PHI that may be disclosed to an outside party without a subject's authorization if certain conditions are met. First, the purpose of the disclosure may only be for research, public health, or health care operations. Second, the person receiving the information must sign a data use agreement with Wright State prior to being given the limited data set containing Wright State PHI.

Specifically, as it relates to the individual or his or her relatives, employers, or household members, all of the following 16 identifiers must be removed in order for health information to be considered a limited data set:

- Names (including the patient's name and names of other individuals connected to the patient)
- Street addresses (other than town, city, state and zip code)
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social Security numbers
- Medical records numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate license number
- Vehicle identifiers and serial numbers, including license plates
- Device identifiers and serial numbers
- Web universal resource locators (URLs)
- Internet protocol (IP) address numbers
- Biometric identifiers (including finger and voice prints)
- Full face photographic (or comparable) images

The identifiers that may remain in the disclosed information of a limited data set includes:

- Dates such as admission, discharge, service, date of birth, date of death
- City, state, five digit or more zip code
- Ages in years, months or days or hours

The information in the limited data set is not considered de-identified and therefore is still subject to the requirements of the Privacy Rule and human subject research regulations but does not require authorization or waiver of authorization when released via an executed data use agreement.

A data use agreement must meet the following standards specified in the Privacy Rule:

- Establish the permitted uses and disclosures of the limited data set
- Identify who may use or receive the information
- Prohibit the recipient from using or further disclosing the information, except as permitted by the agreement or as permitted by law
- Require the recipient to use appropriate safeguards to prevent a use or disclosure that is not permitted by the agreement
- Require the recipient to report to the covered entity any unauthorized use or disclosure of which it becomes aware
- Require the recipient to ensure that any agents (including a subcontractor) to whom it provides the information will agree to the same restrictions as provided in the agreement, and
- Prohibit the recipient from identifying the information or contacting the individuals whose PHI is included in the limited data set.

The limited data set provisions of the Privacy Rule also require Wright State, to take reasonable steps to cure any breach by a recipient of the data use agreement. That is, if Wright State determines that data provided to a recipient is being used in a manner not permitted by the agreement, it must work with the recipient to correct this problem. If these steps are unsuccessful, Wright State must discontinue disclosure of PHI to the recipient under the data use agreement and report the problem to the Office of Civil Rights (OCR) within the Department of Health and Human Services ("DHHS").

5.9 Research Involving External Limited Data Sets

Wright State investigators who wish to conduct research using a limited data set from an external institution (e.g., The Ohio State University) must have the external institution's Data Use Agreement reviewed and signed by a member of the Office of the Vice Provost for Research and Innovation to ensure that it meets Privacy Rule and Wright State requirements prior to receiving the data from the external/collaborating institution.

Investigators are required to submit a copy of any data use agreement to the IRB as part of a study's initial application process.

5.10 PHI Security

Investigators should develop and include a plan in the Initial Application that describes how PHI will be protected through all stages of a study utilizing tracking, recovery, and general security. A tracking system is necessary to account for how the PHI will be stored, used, and shared. A recovery plan includes how the investigator will recover

data if current records are lost to be able to meet both research and accounting of disclosures requirements.

The data security section should include measures that will prevent inadvertent disclosure, loss, or theft of PHI, for example, securing physical data in locked cabinets in locked offices/suites. Investigators should review the Data Security section of the IRB website and consult with IT professions for more information on measures to adequate secure data electronically.

5.11 International Research

The United States' Privacy Rule does not apply to studies conducted in foreign countries. Therefore, international subjects do not need to sign a HIPAA authorization to allow investigators to use and disclose their PHI. However, the DHHS and FDA requirements for protecting confidentiality and privacy for human subject research still apply. Investigators proposing international research should also determine whether there are other laws/regulations (e.g., GDPR) that apply to a subject's health information from their country of origin as part of initial study design.

5.12 Non-Compliance and Data Breaches

Any investigator who is aware of potential non-compliance with this policy must immediately report it to the IRB Chair, who will notify appropriate institutional officials (including the VPR Designee) and facilitate review of the matter under applicable institutional policy.

A privacy breach is any unauthorized access to PHI and commonly (but not always) is related to electronic files or devices that contain PHI.

Examples of breaches include, but are not limited to:

- Contacting the wrong person or sending an email, letter or fax containing PHI to the wrong address, person, or phone number.
- Losing (stolen or inadvertent loss) or improperly disposing physical records containing PHI.
- Losing unencrypted laptops, tablets, cell phones, media devices (video and audio recordings) that contain PHI.
- Losing unencrypted CDs, flash drives, memory sticks containing PHI, or
- Hacking of unprotected computer systems containing PHI.

The Privacy Rule requires that Wright State and/or applicable covered entity review and address any potential privacy breach within 60 days of any Workforce Member discovering the breach. Therefore, prompt reporting of any Privacy Rule compliance

issues is essential to meet this requirement.

6.0 Records

Signed authorizations must be retained by the investigator (or Wright State in absence of investigator) for six years from the date of signature or when it was last in effect, whichever is later. Records documenting the PHI that was disclosed for research via a waiver of authorization must also be maintained for six years.

7.0 References

- 45 CFR 160
- 45 CFR 164
- 45 CFR 162