Procedure Title: Data Management and Disposition

Associated Policy:	Human Research Protection Policy (OSA Policy 1.0) Release of FERPA Protected Data Housed in the Office of Institutional Effectiveness (OIE) for Research Purposes PNWU Information and Data Protection Policy PNWU Policy for Confidentiality of Records-Students PNWU Policy for Document Retention and Destruction and Procedure: Records Retention and Disposition Schedule		
Responsible Unit:	Office of Scholarly Activity		
Created:	6/7/2017	**Executive Lead:**	Chief Research Officer
Effective:	6/7/2017	**Revision History:**	.01-7/2/18; .02-4/5/19; .03 – 6/1/2022; .04 – 1/10/2023; .05 – 8-26-2024
Approved by:	Institutional Review Board		
Procedure Number:	113.05		
Key Words:	Record Destruction; Data storage; Study Data; Shred;		
Purpose:	To meet the responsibilities for protecting human subjects as issued by the Office for Human Research Protections (OHRP) requirement for individuals involved in the conduct or review of human subjects research at institutions holding OHRP-approved Federal Wide Assurances (FWAs)		

Process:
This SOP serves to inform all agents, offices, departments, and affiliate sites of PNWU regarding the process for managing data collected from human subjects and destruction of data collected from human subjects.

Responsible Parties

The Institutional Review Board (IRB) is responsible for:

- Reviewing data management plans in study protocols including, but not limited to:
  - What data will be collected.
  - How the data will be collected.
  - Who will collect the data.
  - How the data will be stored.
  - Who will have access to the data.
  - How long will the data be stored.
  - How the data will be transferred if study personnel leave the institution or upon study closure.
  - How protected health information (PHI), personally identifiable information (PII), and Family Educational Rights and Privacy Act (FERPA) protected records will be deidentified/coded.

The Office of Scholarly Activity (OSA) is responsible for:

- Monitoring compliance with this SOP.
- Posting this SOP for the research community.
- Offering support to all investigators to ensure protected places are available to collect and store data.

The Office of Technology Services is responsible for:

- Establishing the process for password protecting computing devices (PNWU and personal property) that are used to access university data (including research data) in order to protect the university's confidential data from unauthorized access and to comply with HIPAA and FERPA.

The Facilities Department is responsible for:

- Providing PNWU Researchers with secure office space to store paper research data.

The Office of Integrate Institutional Effectiveness (OIIE) is responsible for:

- Ensuring compliance with FERPA rules when it comes to providing student records and institutional data for research.
- Meeting requirements set forth by accreditation bodies and helping to determine appropriate collection, use, and publication of institutional effectiveness practices as research.

The Investigator is responsible for:

- Being a good steward of research data generated or acquired by faculty, staff, and students through the use of University facilities and resources.
- Training and quality checking the competence of the research staff regarding carrying out their roles in the study protocol and following the data management plan, including preservation and accessibility to this data.
- Educating all study participants about how their data will be used, protected, stored, etc.

Definitions

Please reference the Glossary for complete definitions of the following terms and additional terms not listed.

- Anonymized
- Audit
- Data
- Data Confidentiality
- Data Management
- Data Safety and Monitoring Board (DSMB)
- De-Identified
- Family Education Rights and Privacy Act (FERPA)
- Health Insurance Portability and Account Act (HIPAA)
- Human Data
- Human Subject
- Personally Identifiable Information (PII)
- Principal Investigator (PI)
- Protected Health Information (PHI)
- Standard Operating Procedure

Procedure:

1. Unless superseded by specific terms of sponsorship or other agreements with PNWU (e.g., clinical affiliation agreements, reliance agreements, or memorandums of understanding), PNWU owns all research data generated or acquired by PNWU faculty, staff, and students or non-student trainees or fellows (not employed by PNWU) through research projects conducted at or under the auspices of PNWU (OSA Policy 1.0), regardless of funding source.

2. Multiple organizations or individuals may share ownership of research data, for instance, if the research data are generated or acquired through collaborative research. If data is to be shared between institutions or individuals, data use agreements must be executed. The timeline of the data sharing agreement may vary and require IRB approval.

3. The PI is the steward of the research data that are under their control. PIs are responsible for managing access to research data under their stewardship. If indicated by the IRB approved informed consent and protocol, PIs, in conjunction with OSA, may share research data. This may include placing research data in public repositories with appropriate agreements. PIs must contact OSA for supporting data use agreements in an effort to protect the PIs work, the human subjects, and PNWU intellectual property.

4. Paper Data - Storage of paper study data, such as forms, folders, videos, consent forms, recruitment lists, screening forms, etc., must be stored in a secured, locked area or as required per the funder/sponsor.

5. Electronic Data – Storage of electronic study data such as forms, folders, videos, consent forms, recruitment lists, screening forms, etc., must be stored on computers or computer systems owned by PNWU or PNWU affiliates, and/or as required per the funder/sponsor with no less than 128-bit encryption (in transmission or at rest) with password configuration SSL/TLS authentication, authorization, and file transfer networks (e.g., PNWU SharePoint or PNWU Microsoft OneDrive). Research data owned by PNWU stored on a PNWU computer (e.g., the computer hard drive) **must** be backed up on a PNWU encrypted service such as PNWU Microsoft OneDrive or SharePoint.

6. Digital Forms and data files, such as Microsoft Excel and Access, or SPSS, must be password protected and on a password-protected computer in a secured area. Research data files with PII, PHI, and/or FERPA protected data must not be transferred electronically through email unless both the sender and receiver have an email that includes @pnwu.edu.
    - Another alternative is to have the data files encrypted and shared using methods approved by PNWU Technology Services (e.g., PNWU SharePoint or PNWU Microsoft OneDrive).

7. PNWU prohibits research data containing PII, PHI, and/or FERPA protected records to be stored on personal devices (such as but not limited to laptops, tablets, flash drives, phones, etc.) unless the owner is able to configure the device to meet the PNWU Technology Services security standards.
    - IT may only certify the security setting of the personal device while owners bring their device to the help desk.
    - IT will follow a procedure to certify the device and document such certification request.
    - This letter certifying the personal device from PNWU IT services must accompany the IRB application or amendment before allowing the personal device to be used.
    - If the owner(s) change any of the security setting afterwards, the PI will be in violation of data security and need to halt the study/data capture until re-certified.

8. PNWU prohibits research data to be stored at home or in personal vehicles.

9. Methods for de-identifying PHI or FERPA protected records must follow a recommended method such as the method recommended by the U.S. Department of Health & Human Services (e.g., Guidance on Satisfying the Safe Harbor Method).

10. PNWU has the option to take custody of primary research data to ensure appropriate access for instances such as, but not limited to, cases of an allegation of research misconduct, Single Audit (formerly known as A-133 Audit), or FDA audit.

11. PIs must retain research data for at least the minimum period required by applicable laws and regulations, sponsorship requirements, or other agreements (see references below). PIs may choose to retain the data beyond the minimum period, up to any deadline specified by laws, regulations, or other agreements. However, choosing to keep data beyond the required timeframe opens the PI and research data to any audit regardless of timeframe.

12. PIs must contact OSA to destroy the research data to ensure investigators follow the applicable process for destroying research data.

13. If a PNWU PI leaves PNWU, the original research data must remain with PNWU. The departing PI may request a copy of the research data to be transferred in conjunction with a data use agreement.

14. When the responsibilities assigned to the PI described in this SOP exceed the capacity of the PI, the PI should contact OSA to assist the PI in meeting research data management needs. If the research data management needs cannot be met by PNWU, the PI will be informed in a timely and transparent manner.

15. PIs can contact OSA to store research data during the required period. OSA uses Microsoft SharePoint to store research data that allows for a secure, user-friendly access to research data.

16. Once a study is closed and the PI and PNWU are storing data for the required period, investigators may decide to evaluate research data for secondary use. The IRB has a responsibility to protect the data repository even before the data is used. The IRB must receive and approve another protocol submission to access this data for secondary use. The IRB must determine how data will be released for secondary research use, and if additional IRB review is needed. The IRB must determine if there are consent issues, (did the subjects' consent to having the data stored for future research use and is the future use in line with the original consent document's meaning and spirit) and confidentiality (is the data being maintained in a way that protects subjects' confidentiality).

17. Research records must be maintained for a minimum of three years after the research is completed and the study is closed with the IRB. Researchers must keep records according to the longest applicable standard. Note that records generated **under a grant or contract with an industry, government, foundation, or other sponsor may require longer retention**, depending on the terms and conditions of the grant or contract. For further assistance contact OSA at research@pnwu.edu

    - **HIPAA Requirements:** Research that involves collecting identifiable health information by a covered entity or a business associate of a covered entity is subject to HIPAA requirements. As a result, there must be an accounting of disclosures and records (disclosures, HIPAA authorizations, or waivers) must be retained for a minimum of **6 years** from the date the study is closed, or from the date of the last disclosure of identifiable information from study records, whichever is later. (45 CFR 164.528).

- **Institutional Review Board (IRB):** Records must be retained for **3 years** after study closure (45 CFR 46.115)
- **FDA Requirements:** The FDA requires that research involving drugs, devices, or biologics being tested in human subjects must have records retained for a period of **2 years** following the date a marketing application is approved for the drug for the indication for which it is being investigated or, if no application is to be filed or if the application is not approved for such indication, until **2 years** after the investigation is discontinued and the FDA is notified. Please note: this length of time can be much longer than 2 years. You should receive written confirmation from the sponsor and/or FDA granting permission to destroy the records (21 CFR 312.62c, 21 CFR 312.57, 21 CFR 812.140)
- **Federally Funded:** records must be kept for a minimum of **3 years** from the date final grant reports are submitted or the study is closed with the IRB, whichever is later. Please note: There may be additional retention requirements from the funding agency.
- **FERPA:** The Office of Enrollment Services or the Office of Institutional Effectiveness should have an accounting of FERPA disclosure at the time the disclosure was made, but if not, rectify that at study closure. Retain records for **3 years** from the date the study is closed. (34 CFR 99)
- **Health Information Abstracted from Non-Clinical Sources:** records must be retained for **3 years** from the date the study is closed.
- **Health Related Data Collected through Interaction or Intervention with Subjects:** Retain records for **3 years** from the date the study is closed.
- **Minors:** Retain records for **8 years** after the last subject contact, or until subject reaches the age of 22, whichever is later. Please note: There is no single standardized record retention schedule for consent of minors. Instead, a variety of retention requirements, including state requirements, must be reviewed to be compliant. See the table below for more information.
- **Non-Health Related Data Collected Through Interaction with Subjects (including surveys):** Retain records for **3 years** from the date the study is closed
- **OHRP Requirements** requires research records to be retained for at least **3 years** after the completion of the research (45 CFR 46).
- **Questions of data validity:** If there are allegations or questions about the validity of the study data or appropriate conduct of the research, all original research data and study documents must be retained until all litigation, claims, or audit findings involving the records have been resolved and final action has been taken.
- **Retrospective Data Abstracted from existing medical records:** records must be retained for **3 years** from the date the study is closed.
- **Sponsor Requirements:** If your study is sponsored, you must ensure that you comply with any terms for record retention detailed in the contract with the sponsor. A sponsor may require you to retain your research records for an extended period of time.

Five State Area Minor Consent Records Retention Information

There is no single standardized record retention schedule. Instead, a variety of retention requirement must be reviewed to be compliant. The IRB and all investigators must review and comply with state and federal laws when creating a record retention and disposition plan.

State	Location of Regulations	General Information
Alaska	• Statute 25.20.010 – Age of	• The age of majority in Alaska is 18. However, Alaska law

	Majority • Statute 09.55.590 – Emancipated Minors • Statute 70.41.190 – Records Retention	authorizes minors to consent for health care in numerous situations. • Alaska allows minors to consent for their own care if a parent or legal guardian cannot be contacted or is unwilling to grant or withhold consent. • Hospitals must retain records for 7 years following the discharge of the patient. • In the case of minor patient, the records must be retained for 2 years after the patient reaches the age of 19 or until 7 years following the discharge of the patient, whichever is longer.
Idaho	• Statute 32-101 – Age of Majority • Statute 39-4503 and 39-4504 – General Medical Care • Statute 39-1394 – Patient Care Records	• The age of majority in Idaho is 18. However, Idaho law authorizes minors to consent for health care in numerous situations. • Idaho Statute 39-4503 provides that any person of sufficient ordinary intelligence and awareness to comprehend the need for, the nature of, and the significant risks inherent in any hospital, medical, dental or surgical care, treatment, or procedure is competent to consent on his or her own behalf. Any health care provider may provide such health care and services in reliance upon this consent if the consenting person appears to the health care provider to possess the requisite intelligence and awareness at the time of treatment. • Intermediate Care Facilities and Skilled Nursing Records of minors must be kept for 7 years following the patient's 18th birthday. • Hospital healthcare records (X-ray, lab tests and reports) must be maintained for 5 years after the date of the text or after the age of majority, whichever is later.
Montana	• MCA 41-1-101 – Age of Majority • MCA 41-1-401, 41-1-402 & 401-1-501 – Emancipated Minors • MCA 50-16-527 – Release of Records • MAR 37.106.402 (1) and (4) – Minimum Standards for Hospital Medical Record Retention	• The age of majority in Montana is 18. However, Montana law authorizes minors to consent for health care in numerous situations. • A hospital must retain patient records for 10 years from a patient's discharge or death. • If the patient is a minor, the hospital must retain the record for 10 years after the patient reaches the age of 18 or dies if earlier.
Oregon	• OAR 109.510 – Age of Majority • OAR 127.505(1), 419B.558 – Emancipated Minor • OAR 333-505-0050(9) & (15) • OAR 109.640 – General Medical Care	• The age of majority in Oregon is 18. However, Oregon law authorizes minors to consent for health care in numerous situations. • A minor age 15 or older may consent for hospital care, medical, dental, and surgical diagnosis or treatment by a licensed physician or dentist without the consent of a parent or guardian and may consent to diagnosis or treatment by a licensed nurse practitioner without the consent of a parent or guardian. • Records for minors must be kept at least 13 years from the last date of treatment. • Hospitals are required to retain records for 10 years after the last discharge (date of treatment). • Blood bank registries are required to keep records for 20 years. • Items not otherwise included in the patient's medical record, such as Xrays, EKGs, EEGs, and isotopes must be kept for 7 years after last exam date.
Washington	• RCW 26.28.010 – Age of Majority • RCW 70.41.190 – Records Retention	• The age of majority in Washington State is 18. However, Washington law authorizes minors to consent for health care in numerous situations. • Hospitals are required to keep patient records for at least 10 years following the most recent discharge, with the exception of minors.

		Consent records for minors must be retained for ten (10) years following the most recent discharge/treatment OR no less than 3 years following attainment of age of majority. • If a minor patient is incompetent the records must be retained indefinitely.

References:

1. Food and Drug Administration (FDA) Federal Regulations (21 CFR 50, 54, 56, 312, 314, 600, 601, 812 and 814) http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm
2. Department of Health and Human Services (DHHS) Regulations (45 CFR 46 Subparts A, B, C, and D) http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.html
3. Minor Consent to Medical Treatment Laws https://www.guttmacher.org/state-policy/explore/overview-minors-consent-law
4. An Overview of Minors' Consent Law. https://www.guttmacher.org/state-policy/explore/overview-minors-consent-law
5. PNWU Information and Data Protection Policy. https://www.pnwu.edu/about/policy-library/information-and-data-protection-policy/
6. PNWU Document Retention and Destruction Policy. https://www.pnwu.edu/about/policy-library/records-retention-and-disposition-policy/
7. The U.S. Department of Health & Human Services Guidance on Satisfying the Safe Harbor Method. https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html PNWU Data Use Agreement.
8. U.S. Department of Health and Human Services Guidance for Industry - Computerized Systems Used in Clinical Investigations (May 2007) and U.S. Department of Health and Human Services Guidance for Industry - Part 11, Electronic Records; Electronic Signatures – Scope and Application, August 28, 2003.
9. U.S. Department of Education, Family Educational Rights and Privacy Act (FERPA) https://www.ecfr.gov/current/title-34/subtitle-A/part-99?toc=1Office of Human Research Protections (OHRP), Investigator Responsibilities Frequently Asked Questions, What records should investigators keep and for how long https://www.hhs.gov/ohrp/regulations-and-policy/guidance/faq/investigator-responsibilities/index.html

Appendices:

PNWU Disposition of Records Form.

Version/ Effective Date	Author	Section Changed & Reason for Revision
.00 / 6-7-2017	M. McCarroll	Original SOP
.01 / 10-25-2017	M. McCarroll	Section 6 renumbered and minor modifications to section 6.2 for clarification
.02 / 4-5-2019	M. McCarroll	Put into new SOP format
.03 / 6-9-2022	C. Case	Deleted definitions not used in this SOP; Added additional definitions that are used in this SOP; added information about personally identifiable information; added recommendation to back up research data stored on PNWU hard drives to PNWU encrypted shared sites such as One Drive; replaced Sharefile with SharePoint throughout the document; deleted research record storage table and added bulleted list instead; updated

		PNWU policy reference links; added a reference and link for FERPA and OHRP.
.04 / 1-18-2023	C. Case	Per recommendation by Bob Roach, compliance consultant, The language in item 5 above regarding storage of research data has been updated to require investigators to back up research data on a secure PNWU service such as OneDrive or SharePoint when research data is stored on PNWU devices (e.g., personal computer hard drive). Corrected minor grammatical and punctuation errors.
.05 / 8-26-2024	J. Simmons	Fixed instances where "PHI" and "HIPAA protected data" are both mentioned. They mean the same thing. Edits to OIIE responsibilities to reflect current workflow. Replaced "A-133 audit" with "Single Audit (formerly known as A-133 audit)" Minor grammar/punctuation edits. Verbiage/phrasing edits in places to improve clarity.