Status Active PolicySat ID 15460282

Origination	01/2023	Owner	Andrew Bugajski: 4387 AVP - Research and Sponsored Studies
Last Approved	05/2024	Department	HRPP/Research
Effective	05/2024		
Next Review	05/2025		

Research: LRH Data Management- AD.0159

PURPOSE

The purpose of this policy is to provide guidelines for the management (obtaining, sending, receiving, storage, security, and destruction) of data for research studies. It is intended that this research data management policy be consistent with Food and Drug Administration federal regulations, the Common Rule, HIPAA, and good clinical practice, each as amended from time to time. Our policies guide our practices and ensure that we place people at the heart of all we do to deliver the best outcomes and safest care.

APPLICABILITY

This policy applies to Lakeland Regional Health's **Workforce** and **Research Personnel** engaged in research.

POLICY

I. Overview

  A. The HIPAA Privacy Rule requires an Institutional Review Board (**IRB**) to determine that the **Researchers** and Research Personnel will use the minimum amount of Protected Health Information (**PHI**) necessary to conduct research. Individuals performing research at Lakeland Regional Health (LRH), where the LRH IRB is the IRB of Record and/or where LRH personnel are engaged in research, will take appropriate action to send, receive, store, secure, and destroy all data obtained during the course of a research study and/or clinical trial, as permitted by this policy or as required by law.

  B. All Researchers and Research Personnel and LRH staff will use or disclose data only as permitted by this policy or as required by law.

II. Roles and Responsibilities

A. Researchers

1. Procuring **Research Data**:

   i. Research data is only collected per an IRB-approved protocol;

      a. For LRH individuals who have privileges at LRH, no other actions, outside of the approved IRB protocol, are needed regarding special permissions to access and obtain LRH data for research; and

      b. For individuals that do not have privileges at LRH, in addition to the approved IRB protocol, research data can only be obtained by completing and submitting a Lakeland Regional Health Access Request User Acknowledgement and Agreement to the IRB Administrative Office.

2. Managing Research Data: Researchers are responsible for creating and maintaining accurate data documentation and complying with approved data security and management plans. This includes:

   i. Implementing the security controls corresponding to the LRH requirements (e.g., access management, storage, and destruction);

   ii. Ensuring necessary reviews occur for **Critical Digital Information**, data exchanged pursuant to a **Data Use Agreement** (**DUA**) or sponsored award, and data subject to foreign, federal, or state regulations (e.g., export controls, Family Educational Rights and Privacy Act (FERPA), Federal Information Security Management Act (FISMA), General Data Protection Regulation (GDPR)), or intellectual property protections and recording any relevant reference number on the submission in the corresponding application;

   iii. Developing and adhering to an LRH-approved Research Data Security Plan and relevant procedures throughout the course of each project; and

   iv. Informing the Research Office, IRB and Corporate Integrity Services (Compliance) of any incidents pertaining to the research data (i.e., HIPAA violation).

3. Destroying Research Data: Research data will be destroyed in accordance to an agreed upon Research Data Security Plan in congruence with the approved IRB protocol. Unless otherwise stated in the approved IRB protocol, all patient identifiers are destroyed at the conclusion of a study (closure of the study with IRB). Research data may be retained after closure, as long as it is de-identified data.

4. IRB and Ancillary Reviews for Research Data: Researchers cannot begin procuring research data until the necessary IRB and ancillary reviews have been conducted. When applicable, ancillary reviews may include, but are

not limited to: IT, Legal, Corporate Integrity Services, Finance, etc.

5. Data Use Agreements: Researchers are responsible for initiating the DUA request and facilitating any necessary reviews. This includes:
   i. Ensuring that data protection requirements can be met and that all individuals who have access to the data have received appropriate training per relevant policies and procedures related to security and access; and
   ii. Keeping a record for any dataset(s) received pursuant to a DUA and recording any relevant reference number(s) on the submission in the corresponding IRBNet application. For example, if an LRH Researcher is leading a multi-site study where data needs to be combined/aggregated from multiple external sites, records for each dataset would need to be documented/recorded in an organized way in compliance with IRB requirements. If local data from LRH were collected, it could be named Dataset A. Then if data were received from Tampa General Hospital, it could be named Dataset B, so on and so forth.
   iii. Provision of Data will be executed per the LRH Data Use Agreement.

B. IRB

Human Subjects Research is reviewed and approved by the LRH IRB. In order for the LRH IRB to approve a research project, it must conclude that adequate provisions have been made for protecting the **Privacy** of subjects and the **Confidentiality** of personal information. Accordingly, it is the responsibility of the LRH IRB to determine the sensitivity of the data for projects involving Human Subjects Research, and to confirm that relevant confidentiality risks are addressed. The LRH IRB has the authority to review research data collected by the Researcher, to ensure that the data is in compliance with the protections of human subjects as outlined by the Common Rule, **FDA**, HIPAA, and good clinical practices.

C. **IT Security/Compliance/Informatics/Analytics**

1. IT Security/Compliance is responsible for establishing the data security needs and ensuring ongoing data security needs are being maintained. IT Security/Compliance will recommend and approve adequacy of the security applied to electronic data elements within the LRH system as derived from the Research Data Security Plan. IT Security does not have a responsibility for ensuring that the data is destroyed per the Research Data Security Plan.
2. With oversight from the Research Office, IT Informatics and the Analytics Department are responsible for coordinating data procurement from the electronic health record consistent with the approved IRB protocol. This includes: defining data elements, identifying relevant databases, ensuring data elements collected are sufficient for the intended research project,

and delivering the requested data to the Researcher.

D. Legal

All persons engaged in research by or through LRH shall comply with all LRH and IRB policies and procedures, and state and federal regulations, all as may be amended from time to time. It is the responsibility of the person conducting research to know and abide by all such polices, rules and regulations.

III. Procedures

A. Obtaining

1. Research data is only collected per an IRB-approved protocol. Research personnel must identify what PHI identifiers will be collected as part of the data collection and specify them in the research protocol. If a waiver of informed consent is requested, the principal investigator must complete and submit an Application for IRB Waiver of Authorization or Altered Authorization Under the HIPAA Privacy Rule.
2. Medical Staff Privileged/ Non-Privileged Individuals
    - i. For individuals who have privileges at LRH, no other actions, outside of the approved IRB protocol, are needed regarding permission to access and obtain LRH data for research;
    - ii. For individuals that do not have privileges at LRH, in addition to the approved IRB protocol, research data can only be obtained by completing and submitting a Lakeland Regional Health Access Request User Acknowledgement and Agreement.

B. Sending/Receiving

1. All data transferred between study personnel will be transferred by File Cloud Online (or similar approved system).
2. Paper transfer processes must be clearly documented in the protocol and approved by the LRH IRB and the Information Security Department.
3. All electronic data in transit will be protected by no less than TLS version 1.2 with a key length of at least 2048 bits.

C. Storage/Security

1. All electronic data in storage will be protected by no less than 256 AES encryption standards.
2. Any data that will be stored on a personal device of any kind must be LRH-approved. The options for data storage are:
    - i. Paper Storage
        - a. Locked file cabinet; or
        - b. Keypad-secured office.
    - ii. Electronic Storage

a. Encrypted file cloud;

b. LRH-issued laptop;

c. LRH Approved personal device (only for complete de-identified or non-critical digital information);

d. SharePoint (restricted to authorized personnel);

e. LRH Secure USB; or

f. Encrypted Database.

D. Destruction:

1. Research data and critical digital information will be destroyed in accordance to an agreed upon Research Data Security Plan in congruence with the approved IRB protocol. Unless otherwise stated in the approved IRB protocol, all patient identifiers are destroyed at the conclusion of a study (closure of the study with IRB). Research data may be retained after closure, as long as it is de-identified data. At the time of study closure, the PI is required to notify the IRB in writing that the research data has been destroyed per the protocol.

    i. The schedule for destruction/disposal shall be suspended for records involved in any open investigation, audit, or litigation until the case is resolved.

    ii. Any media scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal of the media is complete.

    iii. LRH disposes of critical digital information when no longer needed, as well as the hardware and electronic media on which it is stored, by completely and irreversibly destroying the information and preventing future access to it. All labels are removed from such data prior to disposal. See Computer Data and Media Disposal- IT.0019 and Media Reuse- IT.0024.

    iv. Types of hardware and electronic media that require adequate secure disposal include, but are not limited to:

        a. Computers (desktops and laptops);

        b. Backup tapes;

        c. CD/DVD/BluRay-ROMs Media;

        d. Printers;

        e. Computer integrated medical devices;

        f. Hard drives;

        g. Flash memory; and/or

        h. Other portable storage devices.

    v. If in doubt as to what media requires disposal, contact the

Information Services Security Office (ISSO) to obtain guidance.

vi. The ISSO ensures that all critical digital information, the hardware and electronic media on which the critical digital information is stored, is logged, tracked, and disposed. This includes the following information:

   a. Date and time of disposal;

   b. Who administered the disposal;

   c. Description of the critical digital information being disposed of;

   d. Description of any hardware and electronic media being disposed of; and

   e. Description of what method was used for the disposal.

vii. LRH takes reasonable and appropriate steps to completely and permanently remove critical digital information prior to reusing any hardware or electronic media on which critical digital information has been stored. The ISSO must approve all tools to be used in this process, and workforce members must take reasonable steps to ensure that these tools are used properly.

IV. FORMS TO BE COMPLETED FOR RESEARCH-RELATED DATA

A. Research Data Security Plan

1. For all research, Researchers must complete a Research Data Security Plan. The Research Data Security Plan must be submitted to the LRH IRB and any necessary ancillary reviewers (e.g., Information Security Department) prior to approval of the study.

2. For projects involving Critical Digital Information, Researchers must receive approval from the Information Security Department prior to receiving or sharing Critical Digital Information.

B. Confidentiality Agreement for Research

For all research, Researchers must complete a Confidentiality Agreement for Research. The confidentiality agreement must be submitted to the LRH IRB and any necessary ancillary reviewers (e.g., Information Security Department) prior to approval of the study.

C. Data Use Agreements (DUAs)

1. A Data Use Agreement is needed when non-public data is made available for review or transfer between parties. The administrative review procedures for the review and approval of a DUA is similar whether LRH is the provider or recipient of the data. For additional information pertaining to the processes and procedures surrounding the DUA review process (as well as related agreements, such as non-disclosure, confidentiality, software and collaboration agreements), please reach out to the Research

Office.

2. Submission:
    i. If a Researcher requests to share LRH data with an outside person or organization, or receive data from outside LRH, the Researcher is required to submit a request for a DUA to the Research Office. In addition, Researchers who are not employees of LRH who request access to LRH data must submit a request for a DUA to the Research Office.

    ii. The Data Use Agreement will provide terms for the protection of the data, intellectual property, publication requirements and confidentiality. The Data Use Agreement will require:
        a. All data to be kept confidential and used only as permitted by the DUA, the research protocol and as required by law;
        b. The use of appropriate safeguards to prevent the unauthorized access, use or disclosure of the data;
        c. The report any unauthorized access, use or disclosure of the data; and
        d. Require that individuals granted access to the data do not use the data to contact research subjects.
3. Review: The Research Office will work with the Researcher and the LRH Information Security Department to review the security requirements of the DUA to determine whether any specific protections need to be employed. Similarly, if the project involves human subjects research, the IRB will ensure appropriate provisions are in place to protect confidentiality and privacy.
4. Approval: upon confirmation of adequacy of protections, the Research Office will provide an approved DUA to the Researcher.

V. Application for IRB Waiver of Authorization or Altered Authorization Under the HIPAA Privacy Rule

See Policy, Research: Waiver of Elements of Consent, Waiver of Documentation of Informed Consent and Waiver of Written Authorization, and Section III above for applicability.

VI. Lakeland Regional Health Access Request User Acknowledgement and Agreement

See Non-Employee Access Request Form (attached), and Section III above for applicability.

VII. Business Associate Agreement (BAA)

A BAA is required with a vendor if they are not a covered entity and are performing tasks on behalf of LRH that involve data. In order to disclose protected health information to a Researcher for research purposes, the Researcher will need to obtain either patient authorization, or obtain a waiver meeting the conditions of 45 CFR §164.512(i), or if conducting research using a limited data set, meet the requirements of 45 CFR §164.514(e). A Researcher performing research is not conducting a function or activity regulated by the Administrative Simplification Rules, such as processing payments or engaging in health care operations, or providing any of the services listed in the definition of "business associate" at 45 CFR §160.103, therefore the Researcher is not a business associate of the covered entity, and no Business Associate Agreement is required. To obtain a BAA, contact Lisa Jacklin at Lisa.Jacklin@myLRH.org.

VIII. Third Party Data Banks or Repositories

Researchers may be required by data banks or repositories (any third party that accepts data deposits) to sign a contract agreeing to certain terms and conditions pertaining to the type of data, mode of transfer or security controls, among other requirements or certifications. All such contracts and related documents should be submitted to the Research Office for review.

IX. Genomic Data

Researchers intending to submit human genomic data to a National Institutes of Health (NIH)-designated data repository must first secure institutional approval that the submission of data to the repository is appropriate and consistent with the NIH Genomic Data Sharing Policy. For additional information regarding the NIH Policy and LRH's process for review of such submissions, please contact the Research Office. Researchers requesting genomic data from a third party, including the NIH, should submit a review request in IRBNet.

X. Education and Training

A. Administrators: LRH and its administrators are committed to providing helpful and effective resources to Researchers. Inherent to this is the development of training and outreach materials that promote compliance with institutional policies and processes. The LRH IRB Administrative Office maintains information available to Researchers regarding the applicable requirements and best practices concerning data privacy, confidentiality and security pursuant to the scope of IRB authority.

B. Researchers: Researchers conducting research at LRH who work with human subjects research data are required to maintain an active Collaborative Institutional Training Initiative (CITI) certificate in the ethical treatment of human subjects and animals in order to utilize LRH's resources. For more information, see Research: Investigator, Research Personnel, IRB Member, IRB Administrator, and Institutional Official Training- AD.0161.

XI. Non-Compliance

A. The LRH Research Office, Information Security Department, Analytics Department, Informatics Department, Legal Department, IRB, and other research administrators involved with the management of research data are responsible for reporting instances of non-compliance with the Research: LRH Data Management Policy, as well as the policies referenced herein, to the appropriate research oversight bodies for further review. It is also the Researcher's responsibility to report non-compliance to involved parties so that proper escalation may occur. Instances of identified non-compliance with this policy should be reported to Corporate Integrity Services at 844.468.7574.

B. Violations may impact a Researcher's access to his or her data and LRH resources. In addition, other mitigating and corrective measures may be imposed by the IRB, Chief Compliance Officer and/or Chief Information Officer, or as may be required by a data provider or sponsor.

C. Clarification/Interpretation

   Any questions regarding this policy, or a request for an exception to any of its requirements, can be directed to the administrator reviewing the relevant project. The administrator will discuss their concerns with the Researcher, and thereafter communicate the issue to the Chief Compliance Officer and Chief Information Officer for review and determination.

DEFINITIONS

Confidentiality: The treatment and management of information and materials that an individual or organization has disclosed in a relationship of trust and with the expectation that it will not be disseminated to others in ways that are inconsistent with the understanding of the original disclosure.

Critical Digital Information: LRH information that should not be publicly disclosed or accessible to unauthorized users. This information includes, but it is not limited to, (i) information related to LRH business, operations, or finances, and (ii) private information that LRH is under legal or contractual obligation to protect, such as personally identifiable information (PII), electronic protected health information (ePHI), individually identifiable health information (IIHI), and payment card industry protected information (PCI-DSS).

Data: are observations or measurements (unprocessed or processed) represented as text, numbers, or multimedia.

Dataset: a structured collection of data generally associated with a unique body of work.

Database: an organized collection of data stored as multiple datasets. Those datasets are generally stored and accessed electronically from a computer system that allows the data to be easily accessed, manipulated, and updated.

Data Manager: Coordinates data governance, data stewardship activities, oversees data management projects, and supervises data management activities.

Data Platform: A collection of software which creates a persistent, unified user-database that is accessible to users across the system. Data is pulled from multiple sources, cleaned and combined to create a single customer profile. This structured data is then made available across the system.

Data Use Agreement (DUA): A binding contract governing access to and treatment of nonpublic data provided by one party (a "Provider") to another party (a "Recipient"). DUAs are often required by external parties before they permit data to be received by LRH and may also be necessary for LRH data to be disclosed to another organization. DUA terms and conditions vary depending on the laws and regulations governing the specific type of data to be shared, as well as the policies and/or requirements of the Provider and Recipient.

FDA: Food and Drug Administration.

Human Subjects Research: As defined in relevant federal regulations.

IRB: Institutional Review Board.

Metadata: A structured, machine-readable file that provides basic information about data (who, what, when, where, why, and how) that is essential to promote scientific collaboration; enable discovery, interpretation, and effective use of the data; and document its nature and quality.

Privacy: Control over the extent, timing, and circumstances of sharing information and materials about oneself with others.

Protected Health Information (PHI): Any personal health information, medical records, etc. protected under the HIPAA Privacy Rule.

Registry: A registry is a collection of information about individuals, usually focused around a specific diagnosis or condition. Many registries collect information about people who have a specific disease or condition, while others seek participants of varying health status who may be willing to participate in research about a particular disease. Depending on the nature/use of the registry, patient data may be entered automatically if the patient meets the needs/requirements of the registry (trauma, stroke, etc.) or individuals may provide the information on a voluntary basis. Registries can be sponsored by a government agency, nonprofit organization, health care facility, or private company.

Research Data and Materials ("Research Data" or "Data"): include recorded, tangible, or intangible research information, regardless of form or the media on which it may be recorded, that is created or collected in the process of performing research. Research Data and Materials include, but are not limited to, computer software (computer programs, computer databases, and documentation thereof), materials such as unmodified and modified biological specimens, new or modified chemical entities, laboratory notebooks, notes of any type, materials submitted to and/or approved by IRB, IACUC, or other research oversight committees (e.g., applications, outreach/advertising materials, consent forms, survey routines/questionnaires and debriefing scripts), photographs, films, audio recordings, digital images, original or modified biological and environmental samples, gels, spectra, cell lines, reagents, protocols, algorithms, graphs, charts, numerical raw experimental results, instrumental outputs, other deliverables under sponsored agreements; intangible data such as statistics, findings, conclusions, other deliverables under sponsored agreement; and any other records of, or in any form that could be used for, reconstruction and evaluation of reported or otherwise published results of research.

Researchers/Research Personnel: All individuals designing or directing research, serving as a principal or co-investigator, enrolling research subjects (including obtaining subjects' informed consent or screening potential subjects), or making decisions related to eligibility to participate in research, analyzing or reporting research data, analyzing or reporting adverse events, or submitting manuscripts concerning the research publication.

Workforce: All LRH employees, volunteers, trainees/students, contractors, and medical staff.

REFERENCES

Harvard University: https://vpr.harvard.edu/pages/harvard-research-data-security-policy

FORMS/ATTACHMENTS

I. Research Data Security Plan

II. Confidentiality Agreement

III. LRH Data Use Agreement

IV. Application for IRB Waiver of Authorization or Altered Authorization Under the HIPAA Privacy Rule

V. Lakeland Regional Health Access Request User Acknowledgement and Agreement

VI. Business Associate Agreement – Contact Lisa Jacklin for a BAA (Lisa.Jacklin@myLRH.org)

Attachments

📎 Non-Employee - Access Request Form v5-2022.pdf

Approval Signatures

Step Description	Approver	Date
	Danielle Drummond: 0001 President & Chief Executive Officer - LRHS	05/2024
	Jonn Hoppe: 1011 Executive VP, Chief Legal Officer-General Cou	05/2024
	Timothy Regan: 0009 President - LRMC/Chief Medical Officer	04/2024
	Renee Reed: 4064 Senior Attorney	04/2024
	Deana Nelson: 4080 SVP - Administration and Corporate Initiative	04/2024

Michael Spake: 0057 SVP - External Affairs/Chief Compliance	04/2024
Ana Kalman: 4713 SVP - LRHS CIO Chief Applications Officer and	04/2024
Lisa Jacklin: 4118 Privacy Officer	03/2024
Georgia Ann Keriazes: 0729 QI/ Due Pharmacist	03/2024
Andrew Bugajski: 4387 AVP - Research and Sponsored Studies	03/2024