LOS ANGELES COUNTY
DEPARTMENT OF MENTAL HEALTH
hope. recovery. wellbeing.

Human Subjects Research Committee
hsrc@dmh.lacounty.gov

HUMAN SUBJECTS RESEARCH APPLICATION INSTRUCTIONS

PLEASE REVIEW THE INSTRUCTIONS IN ORDER TO COMPLETE THE HSRC APPLICATION CORRECTLY AND SUBMIT THE NECESSARY FORMS AND INFORMATION.

Frequently Asked Questions (FAQs)

Does my research need Human Subjects Research Committee (HSRC) review?

1. The Los Angeles County Department of Mental Health (LACDMH) HSRC must review and approve all human subjects' research projects involving LACDMH programs, staff, and data. *Research activities cannot begin until HSRC approval is obtained.* This includes LACDMH directly-operated programs and programs with LACDMH legal entity (LE) agreements. Directly-operated clinic program sites are operated and managed with LACDMH employed staff; LE contracted providers are funded by LACDMH, but operated and managed by private organizations. Research that studies LACDMH LE contractors' staff is exempt from HSRC review.

2. Research that involves human subjects as defined by federal guidelines and LACDMH Mental Health Review Policy No. 1400.01, Section 2.2, requires HSRC review.

   Human Subjects: A living individual about whom an investigator (whether professional or student) conducting research obtains:

   a. Data through intervention or interaction with the individual
   b. Identifiable private information

   Research: A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Activities that meet this definition constitute research for purposes of this policy, whether or not they are conducted or supported under a program, which is considered research for other purposes. For example, some demonstration and service programs may include research activities.

3. The intent to develop or contribute to generalizable knowledge makes activity research. Activities designed with intent to develop or contribute to generalizable knowledge are those designed to draw general conclusions, inform policy, or generalize finding beyond a single individual or an internal program (e.g., publication), require HSRC review. Results do not have to be published or presented to qualify the activity as research.

   Publication of Research: The HSRC requires that investigators submit copies of publications resulting from their HSRC-approved research projects to the HSRC as they become available. Links to the publication (article and/or abstract) will be made available on the HSRC website.

4. HSRC review is not needed if the investigation primarily involves quality assurance activities, including program evaluations solely for internal assessments, audits and program evaluations assessing the success of established programs or processes to continuously improve the program quality or performance where it is not the intention to share the results.

5. Posting/Distribution of Recruitment Flyers: To post or distribute flyers in LACDMH LE contracted or directly-operated facilities, research studies must be approved by the HSRC.

What general criteria are necessary to apply for HSRC review?

1. The LACDMH HSRC approves research, which fits closely with its Departmental service mission, ability to allocate necessary associated resources, and responsibility to minimize to the greatest extent possible any risks to LACDMH clients or LACDMH.
2. In accordance with LACDMH policy, all LACDMH services provided as part of research activities must fully meet Departmental clinical, programmatic, privacy and security requirements, and fiscal requirements, including those related to practice parameters, policies and procedures, and medical necessity.
3. The LACDMH HSRC is not a federally registered Institutional Review Board (IRB). LACDMH requires that investigators have IRB approval from their home institution's federally registered IRB. These IRBs must include an association with a specific research institution located in Los Angeles County. Other IRBs may be considered on a case-by-case basis.

How do I apply for HSRC approval?

1. HSRC Application Process: The HSRC will only initiate its review process for applications that are complete. A complete application includes documentation of IRB approval from the investigator home institution's registered IRB, required documents, supporting letters, and applicable forms. The HSRC will schedule a meeting, at which time the principal investigator (PI) must be available by telephone to the HSRC. The HSRC will identify any specific issues pertaining to LACDMH policies, impact on services, consent, privacy and security, etc. The investigator must then resolve these issues before the application is approved.

2. Program Manager and DMH Deputy Director Approval: Investigators are to obtain one approval per site from each LACDMH program site's respective program manager and deputy director. Approval(s) are required for both LACDMH directly-operated sites, as well as LE contracted sites. Signatures indicate respective signators' intent to support the research project with the necessary resources. Attach all applicable Approval(s). For LE contracted sites, program manager's signature must have authority equivalent to a program manager/clinical manager or above, and approval from the deputy director responsible for overseeing their contracts are required. Investigators should anticipate that individuals who are responsible for programs may have other questions, or may request additional information before granting research approval.

3. Privacy Protections: All investigators are required to complete *Exhibit A - Privacy Protections*.

Please note, some questions are intentionally duplicated in Exhibits A and B. Both Exhibits request important information that is independently reviewed and approved by

the LACDMH Privacy Officer and Information Security Officer. Please complete Exhibit A in its entirety and be as detailed and thorough as possible.

4. Protection of Information and Safeguarding the Infrastructure: All investigators are required to complete *Exhibit B – Protection of Information and Safeguarding the Infrastructure*. Even if the section does not apply, please thoroughly explain why it does not apply.
   ***See Data Privacy and Security Guidelines on page 4 for further information.**

   Please note, some questions are intentionally duplicated in Exhibits A and B. Both Exhibits request important information that is independently reviewed and approved by the LACDMH Privacy Officer and Information Security Officer. Please complete Exhibit B in its entirety and be as detailed and thorough as possible.

5. Volunteer Registration: All non-DMH research staff and investigators whose work will involve a physical presence in any directly-operated LACDMH clinic for recruitment, screening, study measures, etc., are required to register as a DMH volunteer with the LACDMH Human Resources Bureau, and identify a DMH employee as a volunteer supervisor for the research project site, per DMH Policy 600.11. DMH HIPAA Training is REQUIRED for all DMH volunteers prior to starting volunteer registration. Please contact the DMH HIPAA Privacy Officer, Maurnie V. Edwards-Thomas, via email at MEdwards@dmh.lacounty.gov if you have any questions.

6. Application Submission: Send the completed application to hsrc@dmh.lacounty.gov. HSRC will review for completeness and will forward it to the DMH Privacy Officer and the CIOB Information Security Officer. You will be contacted if additional information is needed.

7. Responding to Initial Review/Time Limit: To process the application in a timely manner, the investigator should respond as quickly as possible to any questions or suggested revisions during the initial review of the application. Applications should be completed within six (6) months of initial submission; e.g., Privacy Protections, Protection of Information and Safeguarding the Infrastructure, and signed Approval(s).

8. Attachments: Complete and submit the following documents, as applicable. See page 9 list of attachments required.

   Please ensure that the information in the IRB documents is consistent with the HSRC Application. Any inconsistencies can significantly delay approval of your application.

   - Consent Document(s)
   - Recruitment Material(s)
   - Evidence of Qualifications
   - IRB Documents (IRB Application and IRB Approval Letter)*
   - Oath of Confidentiality Agreement(s)

Data Privacy and Security Guidelines

Please read this section carefully before completing Exhibits A and B.

What is de-identified data?

1. Data is considered de-identified if the LACDMH Chief Information Office Bureau (CIOB) is providing and de-identifying data or none of the 18 HIPAA identifiers are collected. If LACDMH CIOB is not providing or de-identifying the data, appropriate security measures must be taken by the investigator. All data not de-identified by CIOB which may contain identifiers (coded or not coded) are treated as Protected Health Information (PHI). The investigator's research is required to be in compliance with federal HIPAA laws and LACDMH policy.

2. The 18 HIPAA Identifiers include, but are not limited to the following:

1. Names	7. Social Security Numbers	13. Device identifiers and serial numbers
2. All geographical subdivisions smaller than a State (street address, city, zip code)	8. Medical Record Numbers	14. Web Universal Resource Locators (URLs)
3. All elements of dates (except year) for dates directly related to an individual (birth date, admission date, discharge date)	9. Health Plan Beneficiary Numbers	15. Internet Protocol (IP) address numbers
4. Telephone Numbers	10. Account Numbers	16. Biometric identifiers (finger and voice prints)
5. Fax Numbers	11. Certificate/License Numbers	17. Full face unique identifying number, characteristic, or code
6. Electronic Mail Addresses	12. Vehicle identifiers and serial numbers (license plate numbers)	18. Any other unique identifying number, characteristic, or code

How do investigators demonstrate how they will ensure security of PHI?

LACDMH requires compliance with the "Health Information Technology for Economic and Clinical Health (HITECH)" Act. HITECH Act of 2009 defines PHI as "rendered, unusable, unreadable, or indecipherable" if the data is either encrypted or destroyed by approved technology or methodologies which will satisfy the reporting requirements defined for a breach in the event the data is lost, stolen, misplaced or an attempt made to hack the data.

1. The approved encryption method for data at rest (i.e., audio or video recorded session stored temporarily on a recording device, data stored on a workstation, laptop, USB thumb drive, remote Web-Server, data that resides in databases, file systems, and other structured storage methods) are based on the National Institute of Standards and Technology (NIST) Special Publication 800-111.

2. The approved encryption processes for data in motion (i.e., data that is moving through a network, including wireless transmission) are those that comply with Federal Information Processing Standards (FIPS) 140-2 and are included in NIST Special Publication 800-52, "Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations" and NIST Special Publication 800-77, "Guide to IPsec VPNs". For the transportation of sensitive information where the solution is maintained by a third-party vendor, the researcher must obtain a Business Associate (BA) contract with the vendor using language consistent with the HIPAA Final "Omnibus" Rule. The BA vendor is responsible for protecting the sensitive data from unauthorized access, including its own staff, and must comply with the Security and Breach Notification Rules.

3. The approved data destruction method is dependent on the type of media. Paper, film, and other hard copy media should be shredded or destroyed so that the PHI cannot be read or reconstructed. Electronic media should be cleared, purged or destroyed so that the PHI cannot be retrieved and be consistent with NIST Special Publication 800-88, "Guidelines for the Media Sanitation."

How does LACDMH evaluate the security of sensitive data or PHI?

1. LACDMH requires that computing devices used for the research and transportation of sensitive data meet federal (HIPAA) guidelines. The LACDMH CIOB verification process is accomplished through a risk assessment as described below:
   a. Evaluation of the computing devices used for accessing, processing or transporting sensitive data. Portable computer devices, laptops, notebooks, and tablets must be encrypted with a solution validated by NIST as meeting FIPS publication 140-2 and equipped with a strong and complex password.
   b. Ensure that all workstations, portable computing devices, and other systems that process and/or store sensitive data have a commercial third party anti-virus software solution and are updated when new anti-virus definition/software release is available. Additionally, ensure that the above-mentioned devices have current security patches applied and up-to-date.
   c. Encrypt all electronic sensitive files when the file is stored on any electronic portable devices or devices with removable media (e.g., USB thumb drives, floppies, CD/DVDs,

SD Cards, digital audio or video recorders, etc.) using a vendor product validated by NIST as FIPS 140-2 compliant or simply use devices with encrypted hardware that are compliant with FIPS 140-2 (e.g., encrypted USB thumb drives, notebooks with encrypted hard-drives, encrypted audio recorders secured by a PIN, audio or video recording using webcam and microphone, and encrypted notebook with complex password security).

d. Ensure that all emails containing sensitive information is sent via an encrypted method using a vendor product validated by NIST as FIPS 140-02 compliant.
e. Smart Phone devices used by the research staff for the project must include encryption compliant to FIPS 140-2. The device must be locked if not in use and accessed by a complex password. The web browser's caching must be disabled. The device must have remote wipe capability in an event it is misplaced or lost. Texting information that may include any of the above HIPAA identifiers is strictly prohibited. The non-sensitive texts should have a statement warning clients to never respond, forward or reply to the text and delete it once read.
f. Evaluation of the transportation method(s) for existence of adequate safeguards to secure the sensitive information from unauthorized access during transportation/transmittal. For solutions utilizing the internet/webservers, security measures such as Valid SSL Certificates, Security Protocols, Authentication Methods, Cipher strength, and FIPS Compliance will be tested and evaluated.
g. Evaluation of the data workflow determines if the path that the sensitive information travels from creation until delivery to authorized recipients includes sufficient protection to render the data unusable, unreadable or indecipherable to unauthorized access.

2. LACDMH requires that the research project investigator use role-based access controls for all user authentications, enforcing the principle of least privilege to protect the sensitive information from unauthorized persons. Only the minimum necessary amount of PHI required to perform necessary functions, as defined by HIPAA Rule, may be copied, downloaded, or exported by the research staff.

3. The research PI is expected to maintain an automated audit trail which can identify the user or a system process which initiates any level of access to PHI. The audit trail must be date and time stamped, log both successful and failed accesses, is read only, and restricted to authorized users. If PHI is stored in a database, database logging functionality must be enabled.

Principal Investigator Assurance

I, the Principal Investigator, agree to follow all applicable policies and procedures of the LACDMH, federal, state, and local laws and guidelines regarding the protection of human subjects in research, as well as professional practice standards and generally accepted, good research practice for investigators including, but not limited to, the following:

PART A: GENERAL ATTESTATION

1. Initiate the research only after HSRC approval of the Application for Research has been received.

2. Ensure that all non-DMH researchers conducting research at DMH directly-operated sites register with the LACDMH Human Resources Bureau as volunteers.
3. Perform the research as approved by the HSRC, utilizing appropriately trained and qualified personnel with adequate resources.
4. Obtain and document (unless waived) informed consent and HIPAA research authorization from human subjects (or their legally authorized representatives) prior to their involvement in the research using the HSRC-approved consent form(s) and proposed recruitment process.
5. Promptly report to the HSRC any events that represent unanticipated problems involving risks to participants or others, and/or significant new findings that may relate to the participants' willingness to continue to participate.
6. Inform the HSRC of any proposed changes in the research or informed consent process before changes are implemented, and agree that no changes will be made until approved by the HSRC (except where necessary to eliminate apparent immediate hazards to participants).
7. Complete and submit an Application for Continuing Review 45 days prior to the expiration date of the previous HSRC approval period at one-year intervals and/or as determined by the HSRC to be appropriate to the degree of risk (but not less than once per year) to avoid expiration of HSRC approval and cessation of research activities.
8. Complete and submit an Application for Continuing Review (including Part D: Final Study Review) when all research activities have ended.
9. Maintain research-related records in a manner that supports the validity of the research and integrity of the data collected, while protecting the confidentiality of the data and privacy of participants.
10. Retain research-related records for audit for a period of at least 10 years after the research has ended (or longer, according to sponsor or publication requirements).
11. Provide copies of all publications resulting from the research project.
12. Maintain current IRB renewals.
13. Adhere to County Policy 608.02, which states, "No employee is permitted to accept any gifts or other considerations from any person, firm or corporation other than the County for the performance of an act that the employee would be required or expected to render in the regular course of their County employment."
14. Inform all co-investigators, research staff, employees, and LACDMH staff assisting in the conduct of the research of their obligations in meeting this Assurance.
15. Complete HIPAA training.

PART B: DATA SECURITY ATTESTATION

1. Understand that project approval applies only to the protocol processes documented in the HSRC Application including the Privacy Protections and Protection of Information and Safeguarding the Infrastructure sections.
2. Agree that any changes in the scope, methodology or in the configuration of systems and tools to those previously approved must be reviewed and approved by LACDMH HSRC prior to implementation.
3. Report changes or be subject to possible suspension of all activities or cancelation of the project.
4. Acknowledge that LACDMH may conduct audits to validate full compliance with the LACDMH HSRC Application "Assurance" section.

Consent Instructions

All research participant consent forms must include the following elements:

1. Statement that the study involves research, explanation of the purposes of the research, expected duration of participation, description of the procedures to be followed, and identification of any procedures that are experimental.
2. Description of any reasonably foreseeable risks or discomforts to the participant.
3. Description of any benefits to the participant or to others that may reasonably be expected from the research.
4. Disclosure of appropriate alternative procedures or courses of treatment, if any, that might be advantageous to the participant.
5. Statement describing the extent, if any, to which confidentiality of records identifying the participant will be maintained.
6. Explanation of who to contact for answers to pertinent questions about the research and research participant's rights and who to contact in the event of a research-related injury to the participant.
7. All consents should include the following statement:
   "Clients served by the Los Angeles County Department of Mental Health directly-operated clinics or LE contractors with questions or concerns regarding the impact of their research activities on access to or quality of their usual care may contact the Los Angeles County Department of Mental Health Human Subjects Research Committee at hsrc@dmh.lacounty.gov."
8. Statement that participation is voluntary, and that refusal to participate will involve no penalty or loss of benefits to which the participant is otherwise entitled to, and the participant may discontinue participation at any time without penalty or loss of benefits to which the participant is otherwise entitled. The research and consent processes should not interfere with DMH services, or treatment of clients.
9. For research involving greater than minimal risk, an explanation about whether: (1) medical treatments are available if injury occurs and, if so, what they consist of or where further information can be obtained. (2) Compensation is available if injury occurs and, if so, an explanation as to what it consists of or where further information can be obtained.
10. Any additional costs to the participant that may result from participation in the research.
11. Consequences of a participant's decision to withdraw from the research and procedures for orderly termination of participation by the participant.
12. Statement that significant new findings developed during the course of the research that may relate to the participant's willingness to continue participation will be provided.

Attachments

Complete Attachments as applicable, then scan into separate and titled PDF documents and submit to hsrc@dmh.lacounty.gov.

1. **CONSENT DOCUMENTS**

2. **RECRUITMENT MATERIALS**

3. **EVIDENCE OF QUALIFICATIONS**
   Attach resume, curriculum vitae, certifications, or other evidence of qualifications of the PI. Limit to five (5) double-sided pages.

4. **INSTITUTIONAL REVIEW BOARD (IRB) DOCUMENTS**
   Attach both submitted IRB Application and IRB Approval Notification/Letter.

5. **OATH OF CONFIDENTIALITY AGREEMENT(S) – SIGNED BY ALL PARTIES**