

Clinical Research Systems Data Use Attestation Form	SOP No.: CI-001
	Version No.: 8
	Issue Date: 1/1/2022
	4 Pages

Instructions

1. Please read this form carefully
2. Initial, sign and date this form to denote your acceptance and understanding of the policies outlined in this form. Please note that electronic signatures are not accepted. Please scan the signed form, save it in PDF format, then mail the PDF file to CBMISupport@uci.edu

Statement of Liability for the End Users

This document defines the responsibilities of end users who use UCI Health, Information Services, Clinical Research systems (including MyResearch/PVCE, REDCap, Cohort Discovery Tool/i2b2, ACT/SHRINE) to collect and/or store sensitive patient data (Protected Health Information = PHI) extracted from clinical systems of care or collected for research purpose under the auspices of an approved IRB protocol.

1. _____ I agree that :
Initials

- ✓ Any PHI I receive or have access to as a researcher will be pursuant to UCI IRB approval OR another IRB's Approval and UCI IRB registration.
- ✓ Any identifiable patient data containing Protected Health Information (PHI) that I receive or have access to for the purpose of the research, will be accessed with IRB Approval and the subject's consent and documented HIPAA Research Authorization, or with IRB Approval where the IRB has granted a waiver of informed consent and a waiver of HIPAA Research Authorization.
- ✓ I will not engage in any other research uses not outlined in IRB or Human Research Protections approved documentation, unless I have consulted with the IRB and acquired the appropriate waivers or protocol modification prior to proceeding with this attestation.
- ✓ If I use decedent PHI, I confirm the following:
 1. The use or disclosure is solely for research on the PHI of decedents; and
 2. The protected health information (PHI) is necessary for research purposes.
 3. If requested by the covered entity (UCI), I will be required to provide documentation of the death of the individual(s).

2. _____ I will not discuss patient data (PHI) with unauthorized persons, agencies, etc.,
Initials without the written consent of the patient.

3. _____ If I wish to export PHI from the Clinical Research systems, I will implement UC
Initials Irvine-approved protections for PHI prior to doing so; therefore, I will not store PHI outside of the Clinical Research systems on any device or system unless the device, system, or the data itself is encrypted, including emails containing PHI.

CAUTION: I must not export the datasets containing PHI delivered by the Honest Broker outside of MyResearch portal without a written approval from the Compliance Office of School of Medicine.

4. _____ Storage of PHI on local devices (workstations, laptops, USB drives, portable
Initials hard drive, etc.) is strongly discouraged. If for unavoidable reasons I must store PHI on my local device, I will protect the device that contains PHI with the following control standards where appropriate by:

- ✓ Maintaining the most current versions of anti-virus software, anti-spyware software.
- ✓ Maintaining the most current versions of operating system updates, host-based firewall software and up-to-date security patches (Note: devices supported by UCI Health IS on the UCI HS network domain will be automatically kept up-to-date) .
- ✓ Insuring the files containing PHI on the device is encrypted.
- ✓ Insuring data transmitted electronically is done so by utilizing encryption technology (sFTP, VPN, etc.).

5. _____ If I wish to export PHI from REDCap, I will export the data into my MyResearch
Initials account.

6. _____ I have completed the required tutorials by the UCI Office of Research, Human
Initials Research Protection in the last five years: CITI Human Research Protections Course and CITI Research and HIPAA Privacy Protections Course per <https://research.uci.edu/compliance/human-research-protections/researchers/training-and-education.html>

I will abide by all UCI Health policies and procedures relating to patient privacy and the protection of PHI. I recognize that my failure to do so may subject me to disciplinary action.

7. _____ I will not use PHI obtained in my role as clinician for use in research.
Initials

8. _____ I will comply with all applicable UC Irvine policies pertaining to patient
Initials confidentiality and information security, including but are limited to:

Electronic Communications

Sec. 800-15: UCI Guidelines for the UC Electronic Communications Policy

Computing and Information Systems

Sec. 714-18: Computer and Network Use Policy

Authorized and Acceptable Use of Electronic Information Sec. 650-18

9. _____ I will abide by the following safe computing practices:

Initials

- ✓ I will protect the confidentiality of my User ID and password used to access the Clinical Research systems.
- ✓ I will use strong passwords; using a password-protected screensaver.
- ✓ I will never share my computer credentials (user name and password).
- ✓ I will always log off shared workstations before leaving the workstation.

10. _____ I will comply with all federal and state laws pertaining to patient confidentiality
Initials and my failure to do so may subject me to civil penalties and/or criminal proceedings, in addition to an assessment of related University costs. I will not share credentials (user name and password). If I do, I may be responsible for costs incurred by the University as a result.

11. _____ I will file an online incident report and notify the UCI Health Privacy Office (888)
Initials 456-7006 or the Security Office (714) 456-7349 as soon as reasonably possible upon my discovery of a loss or a suspected breach of a device containing PHI, and the UC Irvine PD (949-824-5223) if a device containing this data is lost or stolen.

12. _____ Upon conclusion of the research, or conclusion of the need for PHI subject to
this attestation, I will destroy all PHI received under this attestation that resides outside of the research computing environment from which I received the data through the UCI Health authorized Honest Broker process, in accordance with NIST Standard 800-88.

13. _____ **Substance Use Disorder Patient Records**

Initials I will adhere to the following when conducting research using Part 2 patient identifying information of individuals with substance use disorder (excludes tobacco or caffeine use):

- ✓ I will comply with all federal and state laws pertaining to substance use disorder (e.g., HIPAA, CMIA, 42 CFR Part 2)

- ✓ I will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by law
- ✓ I will ensure that patient identifying information is not provided to law enforcement agencies or officials
- ✓ I will not re-disclose patient identifying information except back to the individual or UCI Health
- ✓ I understand I may only include Part 2 data in research reports in aggregate form in which patient identifying information has been rendered non-identifiable such that the information cannot be re-identified and serve as an unauthorized means to identify a patient, directly or indirectly, as having or having had a substance use disorder
- ✓ I will maintain and destroy patient identifying information in accordance with UCI Health privacy and security policies and procedures, including sanitizing hard and/or electronic copies of the information to render the patient identifying information as non-identifiable
- ✓ I will retain records in compliance with applicable federal, state, and local record retention laws.

I will contact the UCI Health Privacy Office (888-456-7006) if I have any questions on this section.

14.

Statement of Liability for Principal Investigators

Initials

If I am a Principal Investigator on any study (contract, grant, and/or IRB application), in addition to the responsibilities delineated above, I understand that I am also accountable and liable for all Clinical Research systems users associated with my study adhering to the data use and security policies outlined in this attestation agreement. If I become aware of a breach of the policies outlined in this agreement, I will report the breach to the UCI Health Privacy Office (888) 456-7006 or the Security Office (714) 456-7349 as soon as reasonably possible.

PRINT NAME

SIGNATURE

TITLE

DEPARTMENT

DATE