


Protecting Confidential Information		
 VCU/VCU Health CLINICAL RESEARCH STANDARD OPERATING PROCEDURES		
SOP No.: CR-RE-335.3	Status: Final	Version Date: 02/11/2025 Effective Date: 03/14/2025

1. PURPOSE

The purpose of this Standard Operating Procedure is to define the standards and processes for protecting confidential information collected and maintained during the course of conducting clinical research at a VCU/VCU Health facility, affiliate, or participating site.

2. REQUIREMENTS

Protecting the safety and welfare of subjects is of the highest priority for all personnel involved in the conduct of clinical research at VCU/VCU Health. Ensuring the privacy of research subjects is a component of human subjects protection. Therefore, VCU/VCU Health will protect confidential information obtained in the course of the conduct of clinical research.

It is the responsibility of all personnel working within VCU/VCU Health, including facilities, affiliates and participating sites, to be familiar with and adhere to federal, state, and local confidentiality requirements and VCU and VCU Health policies and procedures regarding the protection of confidential information, as well as adhering to the confidentiality requirements outlined in the IRB approved protocol and consent document(s).

University faculty, staff, students, and contractors may not transmit confidential data via email and/or via email attachments unless the message and attachments are encrypted.

For transmission of email messages containing confidential data within the University's Google domain, encryption of these messages occurs with the integrated feature of Google Message Security policy-enforced TLS (Transport Layer Security). For transmission of email messages containing confidential data from the University Google domain to external recipients (i.e., over the Internet and those email addresses that are not vcu.edu), encryption of these messages can be accomplished by adding EITHER "zixmail", in lowercase, or the word "secure" in lower case, in the email subject line (without quotations). You can continue to type in the remaining text of the subject line, recipient list and

message body as needed. Review [instructions on how to send encrypted mail](#) from appsforVCU to external recipients.

For internal transmission of email messages containing confidential data within the VCU Health system (Outlook domain), encryption is automatically applied within the Outlook system. For messages containing confidential data sent from the University Google domain to external recipients (i.e., non-vcuhealth.org email addresses), Use Secure, Confidential, Encrypt or Sensitive (only one of these keywords) in the Subject Line of your message and the content is automatically encrypted once it is sent. Use Cleared or Insecure (only one of these keywords) in the Subject Line of your message and the content will bypass the encryption controls and all the transactions will be logged. Reference [How to protect your emails with Zix email encryption](#) on the VCU Health Intranet for more details.

3. DEFINITIONS

Privacy – Privacy refers to the individual. The federal regulations define ‘private information’ as “information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (e.g., a medical or education record).”

Confidentiality – Confidentiality is an extension of privacy, pertaining specifically to identifiable data. While the term ‘confidentiality’ is not formally defined in the federal regulations, the regulations make it clear that investigators have an obligation to inform research participants how their data will be used, who will have access to it, what procedures will be put in place to ensure that only authorized individuals will have access to the information, and the limitations (if any) to these confidentiality procedures.

4. PROCESS

A. Communication Involving Personal Information

- Limit discussions concerning research subjects to information directly related to the conduct of research and necessary to complete the activity at hand.
- Share confidential information with only clinical research staff and other relevant covered entities who need to know such information to do their job.
- Limit the amount of confidential information shared to the minimum necessary.

B. Information Access Control

- Limit the access to confidential information to staff members who require access to perform their jobs.
- Keep records in a secure area that is locked when not in use.
- Locate work stations in areas of limited public exposure. Instruct staff to keep counters, desks, and shelves clear and all source documents filed out of sight.
- Understand the procedures for logging on and off computer terminals.
- Control electronic records access through individual identification and authentication.

C. Transmitting Confidential Information

- Transport confidential data and documents using secure methods. Remind individuals transporting confidential information of their responsibility for the security of such information until it arrives at another secure location.
- Before faxing a document, verify the recipient's fax number. After sending, confirm delivery via telephone or review of the appropriate confirmation of fax transmittal. Check fax machines frequently for received faxes that contain confidential information.

5. REFERENCES

A. Code of Federal Regulations

- [21 CFR 56.111\(a\)\(7\) – Criteria for IRB approval of research](#)

B. Good Clinical Practice

- [ICH Harmonised Guideline Guideline For Good Clinical Practice E6\(R3\)](#)
 - Section 2 - Investigator
 - Section 2.8.10 - Informed Consent of Trial Participants

C. [Health Insurance Portability and Accountability Act](#)

D. VCU

- [Send/Receive Email from VCU Google Apps](#)
- [VCU HRPP Policies and Guidance - HRPP Toolkit](#)
 - HRP-502 Template Consent Document
 - HRP-503a Template SBS Protocol
 - HRP-503 Template Protocol
 - HRP-508 Template Site Supplement

E. [VCU Health Policies \(Policy Manager\)](#)

- Protected Health Information, Uses & Disclosures for Research
- Protected Health Information, Team Member Access

- De-Identification of Protected Health Information
- Protected Health Information, Minimum Necessary Uses and Disclosure
- Protected Health Information, Administrative, Technical, and Physical Safeguards

Review/Revision History CR-RE-335		
Version No.	Effective Date	Description
CR-RE-335.3	03-14-2025	<ul style="list-style-type: none"> ● Clarified adhering to confidentiality requirements outlined in protocol and consent ● Aligned with HRPP toolkit ● Biennial review performed ● Minor formatting edits ● Reference links updated ● Updated to ICH E6(R3)
CR-RE-335.2a	07-01-2020	<ul style="list-style-type: none"> ● Links updated
CR-RE-335.2	07-01-2020	<ul style="list-style-type: none"> ● Biennial review performed ● Minor formatting edits ● Reference links updated
CR-RE-335.1	02-03-2018	<ul style="list-style-type: none"> ● Original