RESEARCH DATA SECURITY, CONFIDENTIALITY AND PRIVACY

1. POLICY

The Birmingham VA Medical Center (BVAMC) Human Research Protection Program (HRPP) is committed to protecting information about our Veterans and employees. When individuals who have served our country volunteer to participate in VA research, they entrust us to keep their personal and health information safe.

It is the policy of the BVAMC to ensure the integrity and security of patient health and personally identifiable information and data compiled during the course of doing research within this facility.

This policy establishes procedures that ensure the security of VA research data and the protection of the privacy of VA research participants. The policies and procedures described within this document do not take the place of information contained in other related BVAMC Medical Center Memorandums (MCM) such as MCM 151-04 Data and IT Security in Research. Rather, they work in conjunction with these other policies and procedures in providing guidance for BVAMC employees.

2. RESPONSIBILITIES

Every VHA employee must comply with all applicable Federal privacy and confidentiality statutes and regulations when collecting, using, sharing or disclosing individually identifiable information, which includes sensitive VA research data from the BVAMC administrative records or VA databases (national, regional, or subject specific).

All VA employees must take annual training that includes VA Privacy and Information Security and Rules of Behavior and VHA HIPAA and Privacy Training.

Anyone involved in VA research must receive annual training in data security. All individuals must be in compliance with all applicable Federal laws, regulations, policies and guidance related to privacy of research subjects, the use and disclosure of individually-identifiable information, and confidentiality, storage and security of research data. Specific requirements are found in:
• VA IT Directive 06-02, “Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations”
• MCM 151-04 Data and IT Security in Research

The BVAMC Medical Center Director has ultimate responsibility for ensuring the security and confidentiality of sensitive VA research data.

BVAMC Associate Chief of Staff for Research and Development (ACOS/R&D) must assure the Checklist for Reviewing Privacy, Confidentiality and Information Security in Research has been signed off by the facility Privacy Officer and Information Security Officer indicating all VA policies and regulations pertaining to privacy and information security have been met, as applicable. This must be completed prior to the ACOS/R&D granting approval to start the research of R&D Committee approved studies (Exempt, Non-Human and IRB approved studies).

BVAMC Research and Development (R&D) Committee must assure the security and confidentiality of sensitive VA research data, and the privacy of VA research subjects, by ensuring that all investigators and everyone else involved in research at the BVAMC are appropriately trained, credentialed and have research privileges and/or scopes of practice consistent with education, training and expertise. The R&D Committee is responsible for reviewing and evaluating all its subcommittees’ decisions, including IRB approval or exemption, before approving a research protocol.

BVAMC Institutional Review Board (IRB) is responsible for protecting the rights and welfare of subjects. The BVAMC IRB will not approve a protocol unless its data management plan includes certification from the investigator that the use, storage and security of all research information collected for, derived from, or used during the conduct of the research is in compliance with all relevant requirements. Specifically, the “Checklist for Reviewing Privacy, Confidentiality and Information Security in Research” will be submitted for review by the Privacy Officer (PO) and Information Security Officer (ISO).

If upon Continuing Review, an Amendment Request or Miscellaneous submission, the IRB Chair determines there has been a change to any aspect of Privacy, Confidentiality or Information Security of the research, the PO and ISO will be requested to review and report their findings to the IRB. The Checklist for Reviewing Privacy, Confidentiality and Information Security in Research will be completed by the PI indicating the changes in privacy and/or data security and submitted to the PO and ISO for review, recommendations (if applicable) and approval prior to final IRB approval.

Prior to releasing de-identified data outside of the VA, the PO must review the data to be released and verify, by memo, to the IRB Chair that the data is de-identified. The memo will also indicate to whom the data will be released and for what purpose. A copy of the memo will be placed in the IRB files. The protocol must indicate to whom the de-identified data will be released and for what purpose.
The IRB Chair or Administrator (upon notification from the PI) immediately reports incidents of noncompliance regarding protected health information (PHI) to the ISO, ACOS/R&D (who reports to the Director and COS) and the PO who participates in the investigation.

**Principal Investigators** are responsible for submitting the “Checklist for Reviewing Privacy, Confidentiality and Information Security in Research” that incorporates a plan to the IRB and R&D Committee for maintaining privacy of research subjects and confidentiality of sensitive VA research data that includes all applicable information (i.e. storage provisions, security measures, transportation or transmission methods, provisions for controlling access to the data, encryption methods, plans for how long identifiable information or linkages will be kept, provisions for disposition of the data at the end of the study). Additionally, for each research protocol, the principal investigator must certify that the use, storage and security of all information collected for, derived from, or used during the conduct of the research will be in compliance with all VA and VHA requirements. This will require that the PI complete the Checklist for Reviewing Privacy, Confidentiality and Information Security in Research form for each new protocol. This form must be submitted with the initial application to the IRB and a copy will be filed with the study’s regulatory documents. The protocol should indicate the Investigator’s plan to protect the participant’s individual privacy in terms of any testing, physicals, etc. that occurs during the course of the research.

If a study has been deemed to meet the criteria of **Exempt** status, the Checklist will be forwarded to the R&D Committee. The PO and ISO must review the Protocol and Checklist and determine all applicable VA policies and regulations pertaining to privacy and information security have been met. An ACOS/R&D letter will not be written until such determination has been made.

If a study has been deemed **Non-Human Research**, only the ISO must review the protocol and Checklist and determine all VA policies and regulations pertaining to information security have been met. A PO review is not required. An ACOS/R&D letter will not be written until the ISO provides final determination.

*Note: If, at any point in a study, the PI determines that the security or confidentiality of data being maintained on non-VA systems or otherwise outside the VA on portable equipment does not meet VA requirements, the PI is responsible for immediately ensuring that the data are returned to reside within the VA firewall.*

All suspected and any unauthorized use, disclosure, transmission, removal, theft, loss, or destruction of VA research-related protected health information (PHI), individually identifiable private information or confidential information as defined by the HIPAA Privacy Rule, The Common Rule, the Privacy Act, or 38 U.S.C. 5701, 5705 and 7332 **MUST** be reported to the ACOS/R&D, PO and ISO within 1 hour. If the immediate notification was not in writing, the employee must also ensure written notification of the ACOS/R&D within 5 business days.

**The BVAMC Information Security Officer (ISO)** is responsible for reviewing each-proposed protocol submitted (including Exempt and Expedited studies) to the IRB to ensure the protocol meets VA guidelines for research data confidentiality and security. Additionally, the ISO reviews the Checklist for Reviewing Privacy, Confidentiality and Information Security in Research
submitted for each new study which includes the Investigator’s plans to protect, store and transmit research data. Once the checklist and protocol have been reviewed by the ISO, data security recommendations are presented to the IRB. If no recommendations are noted, the ISO approves the checklist. Checklist approval or recommendations are forwarded to the IRB Administrator for distribution to the Investigator for action and are filed with each protocol.

Note: for Exempt or Non-Human studies the ISO must submit his/her summary report to the R&D Committee Coordinator with a cc: to the ACOS, R&D and ensure the study is in compliance before the study is initiated. A copy will be maintained in the protocol file.

The ISO is responsible for approving MCM 00-ISO-05 Attachment A (memo to Request for Issuance of USB Storage Device or Attachment B (memo requesting Authorization to transport and utilize VA sensitive information outside protected environments) if an Investigator wishes to store or transmit data outside of the VA protected environment (See MCM 00-ISO-05 and MCM 151-04). The ISO ensures that access to the BV AMC computer system (including remote access) is immediately disabled for all persons involved with research no longer requiring access.

The BV AMC Privacy Officer is the authoritative source for privacy within VHA and is responsible for ensuring the facility’s overall compliance with privacy policies and requirements in research, by reviewing all proposed protocols submitted to the IRB and R&D Committee. The PO is responsible for reviewing each protocol, including the Informed Consent and approving the Checklist for Reviewing Privacy, Confidentiality and Information Security in Research as it pertains to privacy.

The PO will review the HIPAA Authorization (VA Form 10-0493) to ensure it meets VA policies and regulations and report compliance or non-compliance issues to the PI through the IRB or R&D Committee. The PO is also responsible for reviewing the protocol to ensure the Investigator indicates an adequate plan to protect each participant’s individual privacy in terms of any testing, physicians, the consenting process, etc. that occurs during the course of the research. The PO will also review and approve the Checklist for Reviewing Privacy, Confidentiality and Information Security in Research as it pertains to privacy.

Upon review of the checklist, protocol, informed consent and HIPAA Authorization (VA Form 10-0493) by the PO, privacy recommendations and/or approvals will be forwarded to the IRB Administrator for distribution to the Investigator and action and are filed with each protocol. Once stipulations to protect privacy are met by the Investigator, the PO submits a final review to the IRB Administrator/IRB.

Note: for Exempt studies the PO must submit his/her summary report to the R&D Committee Coordinator with a cc: to the ACOS/R&D and ensure the study is in compliance before the study can be initiated. A copy will be maintained in the protocol file.

3. DEFINITIONS

See HRPP SOP #24 – HRPP Definitions
4. **PROCEDURES**

a. **Data Security/Confidentiality and Privacy Plan for a Research Protocol**
When the principal investigator submits a research study that involves the collection, use and/or storage of sensitive information (e.g., subject identifiers or protected health information [PHI]) to the IRB and R&D Committee, his/her submission for approval must contain specific information that includes the following:

- All sites where the data will be used or stored
- Specifically who will have access to the data
- How the data will be transmitted or transported
- How the data will be secured
- If copies of the data will be placed on laptops or portable media, a discussion of the security measures
- If the data will be re-used for subsequent or future research protocols, provisions for future use in the informed consent form, and HIPAA-Compliant authorization (VA Form 10-0493)
- If relevant, provisions to ensure sponsor data storage guidelines are met and do not conflict with VA policies
- Inclusion of a description of any reasonable foreseeable privacy risks to the subject (included in the informed consent)
- Information about where and how a veteran could verify the validity of a study and authorized contacts (included in the informed consent)

b. **Restricted Access:** Access to sensitive VA research data is restricted to:

- Individuals named in the approved research protocol, on the approved research informed consent (if applicable) and the HIPAA authorization form (VA Form 10-0493) (if applicable)
- Individuals who are responsible for oversight of the research program
- VA investigators who require access “preparatory to research” if their activity meets requirements set forth in VHA policy

Persons not employed by VA are given access to medical and other VA records for R&D purposes only when necessary VA approvals have been issued that are in compliance with legal restrictions (i.e. WOC appointments, CRADO or Data Transfer Agreements).

c. **7332 PHI:** All data pertaining to 38 U.S.C 7332 (HIV, Sickle Cell Anemia, Alcohol Abuse/Treatment and Drug Abuse/Treatment) must be provided additional safeguards of protection.

d. **Privacy vs. Confidentiality:** It is important to understand the difference between privacy and confidentiality. Investigators must address each area as part of their research activity.
1) Privacy applies to the person
   a) The way potential subjects are identified and contacted
   b) The setting that potential subjects will interact with the researcher/team and
      who is present during research procedures
   c) The methods used to collect information about subjects
   d) The type of information being collected
   e) Demonstrate that access will be to the minimum amount of information
      necessary to conduct the research

2) Confidentiality applies to the data
   a) Pertains to identifiable data
   b) Data maintenance and who has access to identifiable data
   c) Procedures in place to ensure that only authorized individuals will have access
      to the information
   d) If transported, indicate how the data be protected from wrongful disclosure.

**e. Data Retention and Destruction:** VA research data must be retained in accordance with
VA, VHA, and IRB policies, protocol sponsor guidelines, or Privacy Act system of records
notice, whichever is most restrictive. At this time Records Management has established a
record of control specifically for research data. This system outlines that Research studies
may be destroyed 6 years after the closing of the study, unless a sponsor (or other source) has
requested a longer length beyond the 6 years. During the period that data are retained after a
protocol closes, the investigator must provide the same security and privacy measures as
when the protocol was active, including all physical and technical safeguards. Once the
required retention period has lapsed, the data may be destroyed using a method that will
render them unreadable, undecipherable and irretrievable following VA regulations for
destruction. See MCM 151-04 Data and IT Security in Research.

- **Notifying Veterans of Incidents Involving Compromised Personal
  Information:** Should notification letters be deemed necessary, all notification
  letters are reviewed by the facility incident response team, facility Office of
  Public and Intergovernmental Affairs, and Regional Counsel, as well as the VISN
  and National Level Incident response team, if appropriate. **NOTE: These
  notifications are NOT sent from the investigator.** BVAMC follows MCM 001-
  10 Privacy Policy, for all incidents requiring notification to Veterans.

**f. Notice of Privacy Practices (N OPP):** VHA must provide a copy of its VHA Notice of
Practice Practices to all non-BVAMC patient (Veteran or non-Veteran) research subjects
enrolled in an approved VHA research study with clinical trials or when
treatment/intervention takes place.

1) The investigator/study team must provide the VHA NOPP at the time the subject
   consents to participate in the research project.

2) The non-BVAMC patient research subject must acknowledge receipt of the VHA
   NOPP.
3) In situations where the non-BVAMC patient has a personal representative, the VHA NOPP may be given to, and the written acknowledgment obtained from, the personal representative.

4) The subject will sign and date the NOPP acknowledgement receipt and provide the original to the investigator at the time of consent.

5) A copy of the signed/dated acknowledgement will be provided to:
   a) The subject along with a copy of the NOPP.
   b) The Scanning Department of HIMS

6) The investigator will forward an encrypted e-mail to the facility Privacy Officer with the full name of the non-BVAMC patient’s last four of the social security number immediately upon the subject signing the NOPP.
   a) The PO is required to monitor receipt of acknowledgements on a quarterly basis

7) The investigator will maintain the original copy of the signed/dated acknowledgment receipt as part of the subject’s research records.

g. **Use of CDW, CMS, ViREC, Capri, VINCI, DART data for VA Research:**
   Addressed in SOP #25 Use of VA Data and Data Repositories

h. **Research Information Protection Program (RIPP) Reporting:** Immediately upon becoming aware of any situation described below, members of the VA research community are required to ensure that the situation has been reported to the ACOS for Research, the facility ISO, and the facility PO.

   1) **Unauthorized Access.** Unauthorized access to VA sensitive information, (including unauthorized use, disclosure, transmission, removal, theft, or loss) related to research, including but not limited to protected health information, individually-identifiable private information (as defined in 38 CFR 16.102(f)(2)), and confidential information protected by HIPAA, or by Federal records requirements at 38 U.S.C. §§5701, 5705, and 7332.

   2) **Reportable Network Security Operations Center (NSOC) Incidents.** Any research-related incident reportable to the Office of Information and Technology (OIT) NSOC that impacts, inhibits, or compromises network or data security.

   3) **Notification of Facility Director.** The ACOS for Research must immediately notify any relevant research review committee upon discovering, receiving, or otherwise becoming aware of a credible report of a research information protection incident described in paragraphs (1) and (2) above, and must ensure that the facility ISO and facility PO have also been notified. If the relevant research review committee determines a serious problem occurred, the committee must notify the
Facility Director and the ACOS/R&D within 5 business days after its determination. The Facility Director must report the serious problem to ORO within 5 business days after receiving the notification.

4) **Written Report.** Any oral report or notification of an incident described in subparagraph (1) or (2) must be followed by a written report within 5 business days.

5) **Research Information Protection Incidents – Regular Reporting.** Independent of the reporting requirements described in (3) and (4), members of the VA research community are required to ensure that any situation described in subparagraphs (1), (2), and (3) has been reported to the ACOS for Research, the facility ISO, and the facility PO immediately of becoming aware of the situation. The ISO/PO must report to VACO/NSOC/PSETS within 1 hour of notification.

(a) **Findings of Noncompliance.** Any findings of noncompliance related to research information security/privacy or; any other deficiency that substantively compromises the effectiveness of the facility’s research information protection program by any VA/federal/state organization must be reported to ORO/RIPP. Subsequent reports to ORO/RIPP based on findings made by entities external to the facility must include a copy of the official findings.

(b) **Suspensions or Terminations.** Any suspension or termination of research (e.g., by the ACOS for Research or other facility official) related to concerns about research information protection, must be reported to ORO/RIPP. Within 5 business days of discovering, receiving a credible report of, or otherwise becoming aware of any findings of noncompliance, suspensions or terminations, as described previously must be reported by the ACOS/R&D directly (without intermediaries) to the facility Director, the R&D Committee, and any relevant research review committees, and must ensure that the facility ISO and facility PO have also been notified. The Director must report these findings within 5 business days to ORO/RIPP.

5. **REFERENCES**

- VA IT Directive 06-02, “Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations”
- The Freedom of Information Act (FOIA), 5 U.S.C. 552
- The Privacy Act (PA) of 1974, 5 U.S.C 552a
- The VA Claims Confidentiality Statute, 38 U.S.C. 5701
- Confidentiality of Drug Abuse, Alcoholism & Alcohol Abuse, Infection With the Human Immunodeficiency Virus (HIV) and Sickle Cell Anemia Medical Records, 38 U.S.C. 7332
- The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 Code of Federal Regulations Parts 160 and 164
• Confidentiality of Healthcare Quality Assurance Review Records, 38 U.S.C. 5705
• VHA Handbook 1200.05 Requirements for the Protection of Human Subjects in Research
• VHA Handbook 1058.01 Research Compliance Reporting Requirements
• VHA Handbook 1605.1 Privacy and Release of Information
• VHA Handbook 1605.04 Notice of Privacy Practices
• VHA Handbook 6500
• VHA Handbook 1200.12 Use of Data and Data Repositories in VHA Research
• MCM ISO-01 Information Systems Security and Privacy Incident Reporting
• MCM 00-ISO 04 Data and IT Security in Research
• MCM 00-ISO-05 Removable Storage
• MCM 001-10 Privacy Policy
• MCM 151-04 Data and IT Security in Research

6. ATTACHMENTS

• Medical Center Memorandum 151-04 Data and IT Security in Research
• Medical Center Memorandum 00-ISO 01 Incident Reporting
• Checklist for Reviewing Privacy, Confidentiality and Information Security in Research
• Privacy vs. Confidentiality: Main Differences

7. RESCISSIONS


8. REVIEW DATE

March 2021

Louis Dell’Italia, MD
ACOS, Research and Development